Was ist eine Signatur

Mit Signaturen kann geprüft werden, ob ein signiertes Dokument - etwa ein E-Mail -

- unversehrt und unverändert ist,
- ob es wirklich vom angegebenen Absender stammt.

Durch Signatur können die Urheberschaft und Unverfälschtheit eines E-Mails sichergestellt werden.

Elektronische Signaturen werden unter Anwendung kryptographischer Funktionen erstellt. Die Signatur eines E-Mails ist wie ein Attachment an das E-Mail angehängt.

Zur Erstellung der Signatur bedient man sich eines kryptographischen Schlüsselpaares - dieses besteht aus:

- einem **öffentlichen Schlüssel** (Public Key), öffentlich zugänglich - in einem so genannten Zertifikat enthalten
- und einem **privaten Schlüssel** (Private Key) unter Kontrolle des Signators.

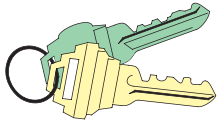
Der Signator signiert das E-Mail mit seinem privaten Schlüssel, den nur er besitzt.

Die Prüfung der Signatur erfolgt mit dem öffentlichen Schlüssel bzw. mit dem Zertifikat, das den öffentlichen Schlüssel enthält.

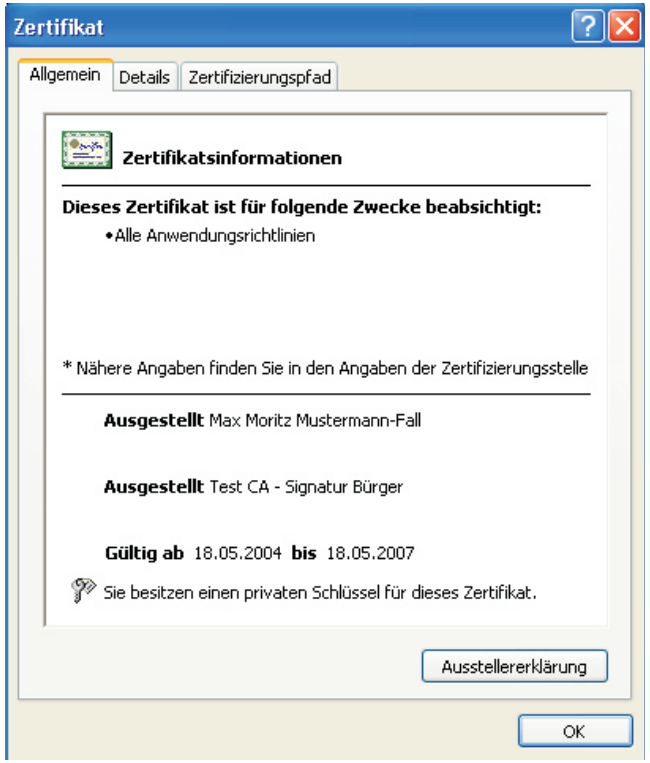
Was ist ein Zertifikat

Um die Urheberschaft feststellen zu können, muss das Schlüsselpaar einer Person zugeordnet werden. Dabei werden Zertifikate eingesetzt, mit denen vertrauenswürdige Stellen diese Zuordnung bestätigen.

Zertifikate werden von Zertifizierungsdiensteanbietern ausgestellt. Dabei wird die Identität des Signators an den öffentlichen Schlüssel der Signatur gebunden.



Das Schlüsselpaar bzw. das Zertifikat wird auch als digitale ID bezeichnet.



Signieren von E-Mails

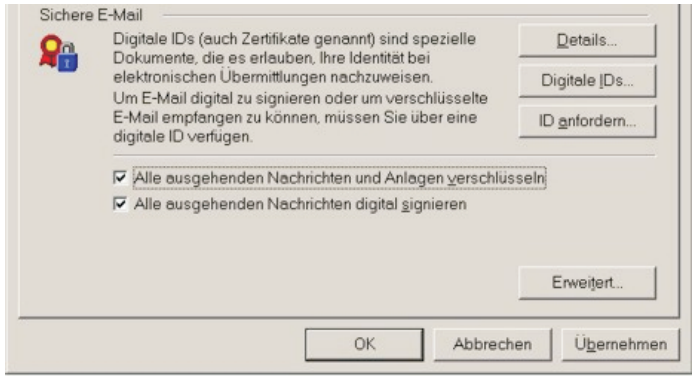
Gängige E-Mail-Programme bieten bereits integrierte Signaturfunktionen nach gängigen Standards. Vornehmlich wird der Standard S/MIME eingesetzt.

Das Zertifikat mit dem privaten Schlüssel muss in Ihr E-Mail-Programm bzw. in die Signatursoftware importiert werden. Im Allgemeinen wird das Zertifikat mit dem öffentlichen Schlüssel den signierten E-Mails angehängt.

Um signieren zu können, müssen Sie im Besitz eines **privaten Schlüssels samt Zertifikat** sein. Diese sind in das Signatur- oder E-Mail-Programm zu importieren.

In gängigen E-Mail-Programmen kann über die Einstellungen die Signatur automatisch allen E-Mails beim Versenden angebracht werden. Alternativ können Sie bei jedem E-Mail einzeln entscheiden, dieses zu signieren.

Über Schlüsselpaare und Zertifikate können vertrauliche E-Mails auch verschlüsselt werden.



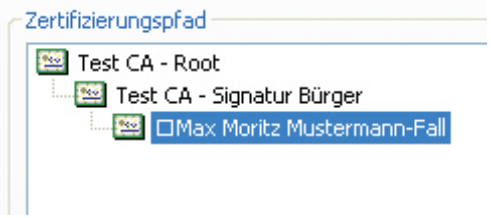
Prüfung von signierten E-Mails

Die Signaturprüfung besteht aus:

- der **kryptographischen Prüfung der Signatur** mit dem öffentlichen Schlüssel des Signators
- der **Prüfung des Zertifikates des Signators**, ob dieses von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde und ob es noch gültig ist.

Zur Prüfung der Signatur muss der/die Empfänger/in das Zertifikat mit dem öffentlichen Schlüssel des Signators besitzen. Dieses ist typisch dem signierten E-Mail angehängt.

Der/die Empfänger/in muss auch die Zertifikate der ausstellenden Zertifizierungsstelle - das sind das Wurzelzertifikat und allfällige Zwischenzertifikate - besitzen und diese als vertrauenswürdig einstufen. So kann die gesamte Zertifikatskette - vom Zertifikat der Zertifizierungsstelle bis zum Zertifikat des Signators - geprüft werden.



Wenn ein Root-Zertifikat noch nicht als vertrauenswürdig eingestuft ist, so erscheint beim Empfang eines signierten E-Mails eine entsprechende Warnung. In diesem Fall prüfen Sie die Herkunft des E-Mails und dann können Sie das Root-Zertifikat oder auch nur das Benutzerzertifikat des Senders als vertrauenswürdig festlegen.

Vorsicht im Umgang mit Vertrauen.
Stufen Sie nur jene Zertifikate als vertrauenswürdig ein, denen Sie auch wirklich vertrauen wollen.

Gängige E-Mail-Programme prüfen eingehende signierte E-Mails bereits automatisch.

E-Mail-Signatur mit der Bürgerkarte

Auch mit Ihrer Bürgerkarte können E-Mails signiert werden. Dazu benötigen Sie ein Programm, das die auf der Bürgerkarte befindlichen Zertifikate und Schlüssel einer Signatursoftware bzw. dem E-Mail-Programm zugänglich macht.

Für die von der Zertifizierungsstelle a.trust ausgestellten Bürgerkarten ist das Programm a.sign client frei beziehbar.
Damit kann die Bürgerkarte zur Signatur von E-Mails mit MS Outlook, MS Outlook Express, Mozilla Thunderbird, etc. verwendet werden.

Auf gleiche Weise können auch andere Signaturkarten zur Signatur von E-Mails verwendet werden.

Informieren Sie sich bei Ihrem Zertifizierungsdiensteanbieter, wie Ihre Signaturkarte zum Signieren von E-Mails verwendet werden kann.

Beachten Sie, dass gängige E-Mail-Clients die von der e-card verwendeten elliptischen Kurven noch nicht unterstützen.

Fragen

Senden Sie ein E-Mail an: technology@a-sit.at

Zentrum für sichere Informationstechnologie - Austria
A-SIT
Secure Information Technology Center - Austria

Elektronische Signatur und E-Mail

E-Government Flyer Nr.204

DIGITALES ÖSTERREICH

Signatur von E-Mails zur Sicherstellung des Ursprungs und der Unveränderheit

- Was ist eine Signatur
- Was ist ein Zertifikat
- Signieren von E-Mails
- Prüfung von signierten E-Mails
- E-Mail Signatur mit der Bürgerkarte