

## Wie funktioniert Kryptographie & Co.?

# Kryptographie

### Etwas Theorie für Interessierte\*

Rein technisch gesehen, basieren sichere Mail-Lösungen auf modernen Verschlüsselungstechniken. Diese kryptographischen Verfahren verunmöglichen den Zugriff durch Unbefugte auf Ihre Daten. Sie garantieren die Echtheit des Absenders und die Ursprünglichkeit der Daten, d.h., dass diese «unterwegs» nicht verändert worden sind.



#### **Symmetrische Verschlüsselung (Shared-Key-Lösung)**

Grundsätzlich unterscheidet man zwei Verschlüsselungstechniken: die symmetrische und die asymmetrische. Symmetrische Verschlüsselungsverfahren verwenden nur einen Schlüssel, im Gegensatz zum asymmetrischen Verfahren mit einem Schlüsselpaar.

Im Ein-Schlüssel-Verfahren ver- und entschlüsselt derselbe Schlüssel die Nachricht. Damit zeigt sich bereits der Nachteil der Lösung: Will der Adressat die Nachricht entschlüsseln, muss ihm auch der Schlüssel übermittelt werden. Aber nicht per Mail, da dies ja noch nicht geschützt ist, sondern über einen sicheren Weg, also über Telefon, SMS oder bei einem Treffen.

Für Spezialanwendungen hat dieser Weg seine Berechtigung, für Mailkommunikation eignet er sich nicht. Denn hier bilden Sender und Empfänger jeweils ein Paar mit einem Schlüssel, der nur diesen beiden bekannt ist. Schicken sich 4 Teilnehmer gegenseitig Mails, braucht es 6 Schlüssel, bei 10 Teilnehmern sind es bereits 45 Schlüssel, und hochgerechnet auf 100 Teilnehmer 4950 Schlüssel. Mit der Formel  $(n-1)/2 * n$  lässt sich schnell ausrechnen, was das für ein Unternehmen bedeutet.

#### **Asymmetrische Verschlüsselung (Public-Key-Lösungen)**

Dieses Verfahren arbeitet mit je einem Schlüssel zur Verschlüsselung und zur

Entschlüsselung der Nachricht. Jeder Schlüssel ist anders, aber jeder ist Teil eines zueinander passenden Schlüsselpaares. Der erste Schlüssel ist als Public Key öffentlich und allen zugänglich. Sein Gegenstück, der Private Key, ist geheim und nur dem Anwender bekannt.

Mailen Sie nun eine vertrauliche Nachricht, verschlüsseln Sie sie mit dem öffentlich zugänglichen Schlüssel des Adressaten, dem Public Encryption Key. Entschlüsselt werden kann die Nachricht einzig und allein vom Besitzer des dazu passenden Private Key. Damit ist sichergestellt, dass die Nachricht nur vom richtigen Empfänger gelesen werden kann.

#### **Digitale Signatur**

Spricht man von asymmetrischer Verschlüsselung, kommt man fast automatisch zur digitalen Signatur, die vergleichbar mit einer Unterschrift ist.

Wenn Sie eine Mail signieren, garantieren Sie,

- a) dass die Mail von Ihnen stammt, d.h. eine Mail mit Ihrer Signatur kann von niemandem sonst kommen (Authentifizierung).
- b) dass der Mailinhalt unterwegs nicht verändert wurde (Integrität).

Um Mails digital zu signieren, verwendet man den Persönlichen Schlüssel (Privat Signing Key). Er verschlüsselt eine aus dem Mailinhalt generierte Prüfsumme zur

## Wie funktioniert Kryptographie & Co.?

# Kryptographie

eigentlichen Signatur. Der Text selber kann dabei unverschlüsselt, also lesbar, bleiben. Der Empfänger kann die Signatur mit dem Öffentlichen Schlüssel (Public Key) des Senders überprüfen und sieht sofort, ob auch nur ein einziges Zeichen manipuliert worden ist.

Zur rechtlichen Verbindlichkeit einer digitalen Signatur sei auf das Signaturgesetz (ZertES) verwiesen, das seit dem 1. Januar 2005 in Kraft ist. Dieses Gesetz regelt klar, in welchen Fällen und unter welchen Bedingungen eine digitale Signatur rechtlich einer manuellen Unterschrift gleichgestellt wird.

### Digitale Zertifikate

Alles bisher Gesagte zeigt klar, welche zentrale Rolle die nachweisbare Identität eines Schlüsselpaar-Besitzers spielt: Als Empfänger müssen Sie absolut sicher sein, wer hinter der Senderadresse steht. Der Schlüssel allein garantiert noch nicht, dass es sich um die richtige Person handelt.

Erst ein digitales Zertifikat verbindet die Schlüssel und ihre Besitzer eindeutig. Ähnlich einem amtlichen Ausweis stellt es als elektronische Identitätskarte eine eindeutige Verbindung zwischen kryptographischem Schlüssel und Besitzer her – über eine externe vertrauenswürdige Stelle (Trust Center), die eben dieses Zertifikat erzeugt und so den öffentlichen Schlüssel beglaubigt. Das Trust Center verwaltet diese Zertifikate (ungültig erklären, erneuern, ändern) und publiziert die öffentlichen Schlüssel wie in einem Telefonbuch.

### Schweizer Zertifizierungsgesetz ZertES

Beim Thema Gleichstellung von elektronischer und eigenhändiger Unterschrift sind wir ein gutes Stück weiter: Das Gesetz über die digitale Unterschrift ist von den Eidgenössischen Räten beschlossen worden und seit Januar 2005 in Kraft. Damit werden digitale und handschriftliche Unterschriften gleichgesetzt, sofern

sie gesetzeskonform sind und die definierten Zertifikate beinhalten. Entsprechende Zertifikate stellen verschiedene Schweizer Zertifizierungsstellen heute zur Verfügung.

In der Schweiz gilt die «Formfreiheit» für Verträge. Sie wird durch ZertES nicht berührt, erlaubt aber auch unabhängig den Gebrauch von digitalen Unterschriften für verbindliche Belange. Derartige Rechtsgeschäfte werden «elektronisch», mit und ohne digitale Signatur abgewickelt. Solange keine Probleme auftauchen, ist dies ein einfacher, schneller und gangbarer Weg für die moderne Wirtschaft. Im Streitfall entscheidet allerdings der Richter, ob und wie elektronische Dokumente zur Beweisführung zugelassen werden.

Mit ZertES können neu auch Rechtsgeschäfte elektronisch abgewickelt werden, für die das Gesetz die Schriftform verlangt (mit wenigen Ausnahmen).

---

*\*Hier gehts wirklich nur um Theorie am Rande. Wenn Sie ein «technischer Insider» sind und jetzt voreilig denken, mit unserem theoretischen Wissen sei es nicht weit her, dann sei Ihnen versichert: Wir können das Ganze auch hoch wissenschaftlich-technisch erklären. Allerdings wäre das nur für Insider interessant, den Anwendern von Secure Mail wäre es wohl des Guten zu viel. Wir glauben, eine optimale Secure-Mail-Lösung muss immer anwenderfreundlich sein – auch wenn es um das Verständnis geht.*

### SwissSecure AG

Haldenstrasse 34, 8955 Oetwil a.d.L., Switzerland  
Phone +41 1 77 55 111, Fax +41 1 77 55 101  
E-Mail [info@swisssecure.ch](mailto:info@swisssecure.ch), [www.swisssecure.ch](http://www.swisssecure.ch)