INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Newsletter 2.03 : Sichere E-Mails

In diesem Newsletter finden Sie Antworten zu den folgenden Fragen:

:: Wie funktioniert der E-Mail-Transport?

:: Welche Risiken nehme ich in Kauf?

:: Wie mache ich E-Mails sicher?
- PGP
- Zertifikate (X.509)

Dies ist eine kostenlose Dienstleistung von der GO OUT Production GmbH.

Inhaltsverzeichnis

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Sichere E-Mails

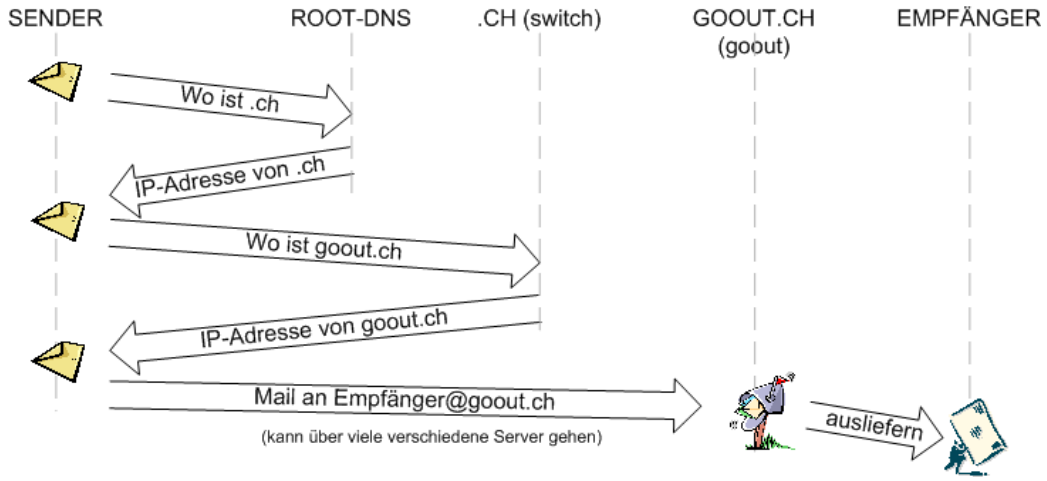
E-Mails sind aus der heutigen Zeit nicht mehr wegzudenken. Schnell einen Termin festlegen, diesen bestätigen, eine Bestellung durch-führen oder einfach ein kurzes Lebenszeichen an eine bekannte Person versenden, E-Mails sind nicht nur schnell, sie sind auch sehr zuverlässig.

2 Wie funktioniert der E-Mail-Transport?

Beim Versand von E-Mails verhalten sich Zieladressen ähnlich einer persönlichen Anschrift. Sie bestehen aus einem Namen und einer durch das Sonderzeichen «@» abgetrennte Hausanschrift. Beides zusammen ergibt dies die weltweit einmalige Anschrift.

Beispiel:
empfaenger@goout.ch

Diese Adresse wird von hinten her gelesen. Zuerst wird '.ch' von einem der 13 Root (Mutter) DNS Server beantwortet. Mit '.ch' weiss das E-Mail-Programm nun, dass diese elektronische Post in die Schweiz gesandt werden muss. Dort wird nachgefragt, wo 'goout.ch' «liegt». Die Antwort erhält das Mailprogramm von der Firma Switch, welche in der Schweiz die Domainnamen verwaltet. Damit ist die E-Mail vor unserer Haustür angelangt und das Mail-Programm teilt dem Mailserver mit, dass die Post für „Empfaenger" bestimmt ist. Der Mailserver nimmt die E-Mail entgegen und legt sie in die Box – den Briefkasten - von „Empfaenger".



goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3 Welche Risiken nehme ich in Kauf?

Die Kommunikation mit E-Mails basiert grundsätzlich auf lesbaren Daten, d.h. alle Benutzernamen, alle Informationen und Passworte werden ungeschützt über das Internet an die entsprechenden Rechner geschickt. Dabei sind einige Schwachpunkte vorhanden:

1. Die Absenderadresse ist beliebig wählbar
Ein Mail-Empfänger kann sich nicht darauf verlassen, dass die Person, deren Namen in der „von"-Zeile einer E-Mail erscheint, auch die Person ist, die die E-Mail wirklich versandt hat. So wird zum Beispiel dubiose Werbung mit falschen Absenderangaben getarnt, um die wirklichen Absender zu verbergen. Und wenn der richtige Absender nicht bekannt ist, kann man sich bei dieser Art von - meist lästiger - Werbung auch nicht beschweren. Oder es werden als Anhang Viren mit gefälschten Adressangaben verschickt, um eine Rückverfolgung zu erschweren.

2. Ungeschützte Übertragung
Auf dem Weg durchs Internet – vom eigenen Computer über diverse Mailserver zum Empfänger – sind ohne vorsorgliche Massnahmen alle Informationen im Klartext unterwegs. An jedem Computer, der zwischen Absender und Zielrechner liegt, können die Daten mitgelesen oder verändert werden. Im privaten Bereich ist dieser Um-stand zwar vielleicht nur unangenehm. Betriebliche Geheimnisse ungeschützt per E-Mail zu verschicken, kann jedoch für Unternehmen eine ganz andere Tragweite aufweisen.

Da sind zum Beispiel Fälle von Offerten bekannt, die mittels unverschlüsselter E-Mail übertragen und von der Konkurrenz abgefangen werden konnten. Kein Wunder, erhielt die Gegenofferte den Vorzug…

3. Ungeschützte Lagerung der elektronischen Post
Elektronische Post wird zuerst auf einem Mailserver zwischengespeichert, bevor sie dem Rechner zu-gestellt wird, auf den die adressierte Person Zugriff hat. Auch auf diesen zwischenlagernden Systemen haben deren Verwalter meist die Möglichkeit, die elektronische Post zu lesen und - in der Regel - auch Kopien davon anzufertigen.

4. Passwort wird unverschlüsselt übertragen
Werden E-Mails vom Mailserver heruntergeladen, werden meist das Passwort und die Daten ungeschützt mit übertragen. Dies bedeutet, dass alle Personen zwischen Adressat und Mailserver diese Daten ausspähen und in späteren Versuchen missbräuchlich verwenden könnten (E-Mails lesen oder schreiben).

5. Gefahr durch Viren
E-Mail-Programme bieten die Möglichkeit, als Anhang weitere Daten zu versenden. Diese Dateien können Bilder, Textdokumente oder auch ausführbare Programme sein. Ob ein angehängtes Textdokument oder eine ausführbare Datei einen Virus enthält, kann jedoch nur ein Virendetektor erkennen. Daher ist im Umgang mit Datenanhängen grundsätzlich Vorsicht angebracht.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

6. Mailverluste
Meist werden gesendete wie empfangene E-Mails gespeichert, um auch nachträglich noch Zugriff darauf zu haben. Ärgerlich ist, wenn diese Daten durch Rechner-Abstürze oder Umkonfiguration plötzlich verschwunden sind.

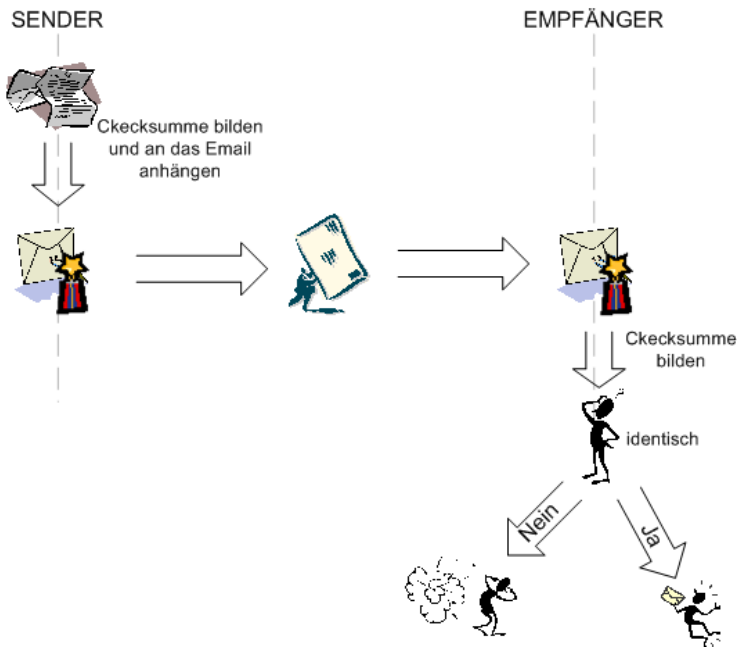
4 Wie werden E-Mails sicher?

Die grössten Gefahren gehen bei E-Mails von der Veränderung des Inhalts bzw. der Absenderadresse aus. Dabei gibt es zwei Arten, diesen Gefahren entgegenzutreten und E-Mails sicher zu übermitteln:
A. Die E-Mail wird mit einer digitalen Unterschrift versehen
B. Die E-Mail wird als ganzes komplett verschlüsselt.

A. Die digitale Unterschrift
Die digitale Unterschrift bildet eine Checksumme über die gesamte E-Mail. Diese Zahl wird zum Abschluss der E-Mail angehängt. Nach Empfang wird die Checksumme erneut berechnet. Sind nun beide Checksummen identisch, wurde die E-Mail nicht verändert. Tritt eine Abweichung auf, ist klar, dass der Inhalt (inkl. einem möglichen angehängten Dokument) verändert wurde.

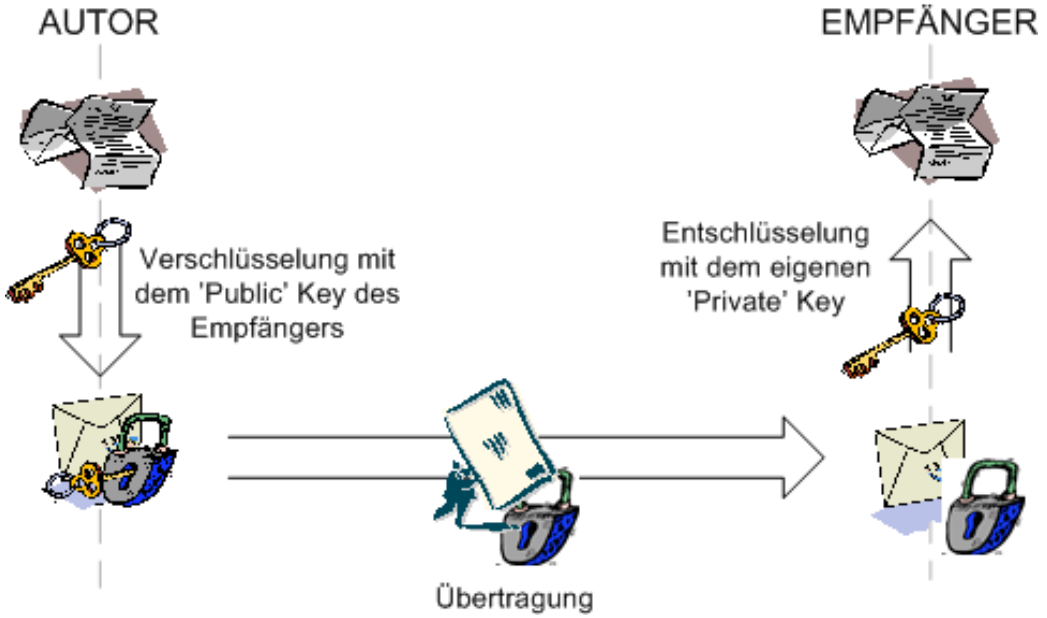
Die digitale Unterschrift ist persönlich und kann zum heutigen Zeit-punkt nicht verändert werden. Hauptsächlich werden zwei Techniken angewandt:
MD5 - Message Digest #5, Ron Rivest, RSA (128 Bit Verschlüsselung)

SHA - Secure Hash Algorithm, NIST / NSA (160 Bit Verschlüsselung)
E-Mails, welche mit einer digitalen Unterschrift versehen sind, können unterwegs jedoch weiterhin von allen Personen gelesen werden. Sobald vertrauliche Nachrichten übermittelt werden, empfiehlt sich also die verschlüsselte Übertragung.



B. Verschlüsselung
Bei der verschlüsselten Übertragung muss der öffentliche Teil des Schlüssels, der so genannte Public Key des Empfängers, bekannt sein. Dieser kann via E-Mail übertragen werden, muss aber anschliessend per Telefon überprüft werden (die Checksumme des Schlüssels reicht). Mit diesem öffentlichen Schlüssel des Empfängers wird die E-Mail nun auf dem Rechner des Senders codiert, bevor sie abgeschickt wird. Unterwegs ist die E-Mail für alle Zwischenstationen unlesbar. Erst am Ziel wird sie durch den privaten Teil des Schlüssels, dem Privat Key, wieder „lesbar" gemacht.

Sollte die E-Mail verändert werden, was jedoch keinen Sinn macht, da sie nur aus verwirrlichen Zahlen und Buchstabenfolgen besteht, ist sie auf der Empfängerseite nicht mehr lesbar, da nicht mehr entschlüsselbar.
Heute bieten sich zwei Möglichkeiten der Verschlüsselung an:
- **PGP**, eine Software, die auf dem Prinzip des Web of Trust agiert
- **X.509** Zertifikate



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

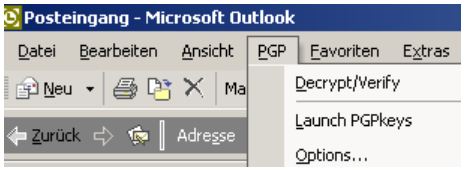
Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

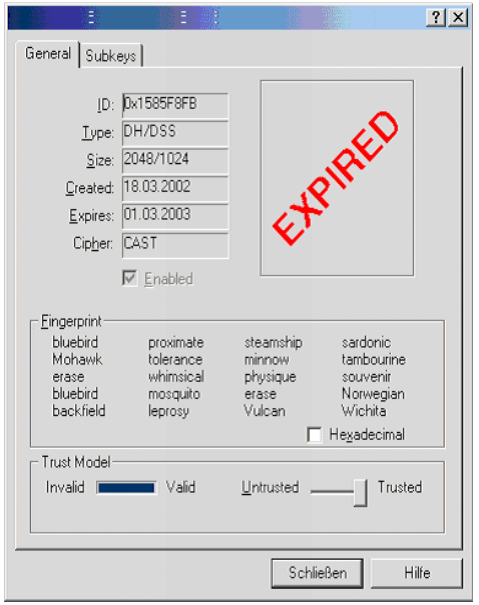
Telefon 052 320 91 20
Fax 052 320 91 21

PGP

PGP ist ein beliebtes und verbreitetes Programm. Es bietet einfache Möglichkeiten, E-Mail direkt zu verschlüsseln oder digital zu signieren. Heute ist es mit Hilfe von PGP auch möglich, direkt in MS Outlook E-Mail zu verschlüsseln. Ein zusätzlicher Menupunkt öffnet die notwendigen Funktionen.



Nachteilig wirkt sich jedoch das Web of Trust aus. Die E-Mail ist zwar verschlüsselt, es ist aber nicht sicher, ob der Sender wirklich auch der Sender ist. Die Identität des öffentlichen Schlüssels (Public Key) muss daher bei jedem neuen Sender kontrolliert werden.



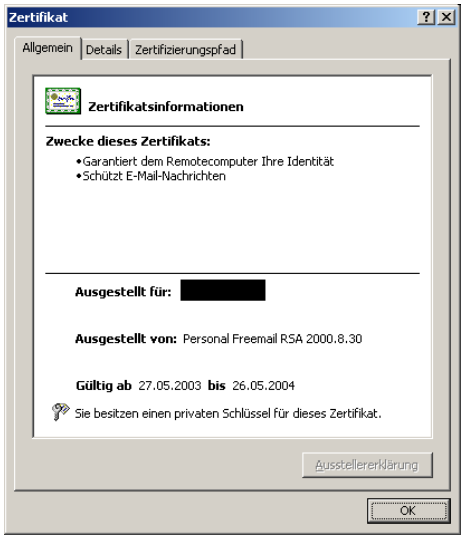
Obenstehendes Zertifikat wurde manuell auf „trusted“ gesetzt. Das bedeutet, der Schlüssel wurde als vertrauenswürdig eingestuft. Inzwischen ist jedoch der oben abgebildete Schlüssel abgelaufen und sollte nicht mehr verwendet werden.

X.509 Zertifikate

Zertifikate werden von einer zentralen Stelle aus vergeben. In der Schweiz gibt es zur Zeit keine solche solche mehr, nachdem die Firma „Swisskey“ ihren Betrieb eingestellt hat. Um diese Aufgaben buhlen momentan einige Firmen, hier sei stellvertretend für alle eine genannt: Thawte.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Thawte stellt kostenlos Zertifikate aus, die in praktisch allen E-Mail-Programmen verwendbar sind. Diese können auf der Homepage „bestellt“ und sofort verwendet werden.
Das erhaltene Zertifikat hat aber nur einen begrenzten Schutz. Zuerst muss die Glaubwürdigkeit des Zertifikatsinhabers bestätigt werden. Da Thawte den Geschäftssitz in Südafrika hat, ist es kaum möglich, dort persönlich vorbeizugehen. Aus diesem Grund gibt es in der Schweiz verschiedenen Notare, die diese Glaubwürdigkeit bestätigen können. Die GO OUT Production GmbH gehört dazu. Persönliche Vorstellung mit Pass oder ID ist Bedingung. Sobald man eine gewisse Anzahl an „Punkte“ hat, ist das Zertifikat nicht mehr „unpersönlich“, sondern lautet auf den Namen des Senders.

Allen genannten Problemen zum Trotz ist es heute möglich, sichere E-Mail zu versenden. Diese einfachen Möglichkeiten sollten unbedingt genutzt werden. Für weitergehende Fragen stehen wir gerne zur Verfügung. Kontaktieren Sie uns unverbindlich, wir helfen gerne weiter!

ISP-Partner:

Nützliche Links:
PGP: http://www.pgpi.org
Thawte: http://www.thawte.com