

Quickstart

Das Wichtigste in Kürze

- 1. Worum geht es überhaupt?** Mit dem WEB.DE-TrustCenter und einem geeigneten Mailprogramm können Sie E-Mails verschlüsseln und digital unterschreiben. *Siehe Seite 4*
- 2. Wozu das ganze?** Nur verschlüsselte E-Mails wahren das Briefgeheimnis, und digital unterschriebene Mails haben mehr Beweiskraft als unsignierte. *Siehe Seite 5*
- 3. Überlegen Sie sich, wie viel Sicherheit Sie brauchen.** Die voreingestellten Sicherheitsstufen reichen nämlich oft nicht für wirklich sensible Bereiche. Wie Sie die Sicherheit erhöhen können, lesen Sie für *Netscape auf Seite ###3* und für *Microsoft auf Seite 6*.
- 4. Wenn der Hersteller Ihres Browsers oder E-Mailprogramms das WEB.DE-TrustCenter noch nicht anerkannt hat, müssen Sie das nachholen.** Technisch tun Sie das, indem Sie die Zertifikate des Trustcenters installieren. Wir arbeiten daran, diesen Schritt überflüssig zu machen. Vorerst müssen Sie sich aber noch häufig selbst darum kümmern.
Netscape siehe Seite 16, Microsoft Seite 27
- 5. Ein Zertifikat besteht aus einem beglaubigten Schlüsselsatz zum Chiffrieren und Signieren.** Sie beantragen Ihr Zertifikat bei Trust.web.de, indem Sie die Anmeldeformulare online ausfüllen. Sie erhalten sofort ein vorübergehendes Zertifikat. *Netscape siehe Seite 18, Microsoft Seite 28*
- 6. WICHTIG: Sichern sie Ihr Zertifikat, am besten doppelt auf zwei verschiedenen Disketten.** Behandeln sie das Zertifikat mit der gleichen Sorgfalt wie Ihren Wohnungsschlüssel.
Netscape siehe Seite 21, Microsoft Seite 30
- 7. Ihr Zertifikat enthält zwei Schlüssel, die sich gegenseitig ergänzen.** Der eine ist öffentlich, der andere privat und geheim. Mit dem privaten Schlüssel können Sie ab sofort Mails digital unterschreiben. *Netscape siehe Seite 22, Microsoft Seite 32*
- 8. Die anderen können mit Ihrem öffentlichen Schlüssel Mails an Sie chiffrieren.** Diese Mails können nur Sie mit dem privaten Schlüssel lesen.
Netscape siehe Seite 24, Microsoft Seite 37
- 9. Wenn Ihre Mailpartner ebenfalls Zertifikate haben, können Sie beides kombinieren:** Verschlüsselung und Unterschrift. Jetzt sind Ihre Mails wirklich sicher.
Netscape siehe Seite 23, Microsoft Seite 34
- 10. Inzwischen prüft das Trustcenter Ihre Identität, um aus Ihrem vierwöchigen Zertifikat ein einjähriges zu machen.** Dazu bekommen Sie einen Brief mit dem Activator Key, der das vollgültige Zertifikat freischaltet. Es kann gut sein, dass Sie diese Anleitung zusammen mit dem Activator Key bekommen haben. *Siehe Seite 43*
- 11. Wenn das einjährige Zertifikat abläuft, müssen Sie es erneuern.** *Siehe Seite 43*
- 12. Wenn sich Ihre Hausadresse oder die E-Mail-Adresse ändert, müssen Sie Ihr Zertifikat widerrufen und ein neues beantragen,** denn das Zertifikat ist mit Ihren Daten digital fest verbunden.
Siehe Seite 43
- 13. Ihnen ist das alles zu kompliziert?** Kein Problem, es geht auch viel einfacher: Mit FreeMail, unserem kostenlosen Web-basierten E-Mail-Dienst. In FreeMail haben wir nämlich das TrustCenter schon eingebaut. Mit FreeMail verschlüsseln und signieren Sie Mails mit einem einzigen Mausklick. Keine komplizierten Einstellungen, keine Installation. *Siehe Seite 41*

Inhaltsverzeichnis

THEMA	SEITE
1. Warum Verschlüsselung?	4
.....Zehn Argumente für die Verschlüsselung	5
.....Ist das wirklich sicher?	6
2. Was brauche ich dazu?	7
.....Mit welchen Programmen geht das?	7
.....Warum ist das nicht gleich eingebaut?	7
3. Was ist das: Verschlüsselung, Unterschrift, Zertifikat?	8
4. Warum S/MIME und nicht PGP?	12
5. Wie bekomme ich das Nötige von WEB.DE?	13
6. Schritt für Schritt	15
Netscape	16
.....a) Festlegen der Sicherheitsstufe für Netscape	16
.....b) WEB.DE-Zertifikate installieren mit Netscape	16
.....c) Eigene Zertifikat beantragen mit Netscape	18
.....d) Zertifikate exportieren, importieren und sichern mit Netscape	21
.....e) Digitale Unterschrift mit Netscape Messenger	22
.....f) Verschlüsseln mit Netscape Messenger	23
.....g) Wie sieht eine an mich verschlüsselte E-Mail aus	24
.....h) Zertifikate verwalten mit Netscape Messenger	24
Microsoft	27
.....a) Erhöhen der Sicherheitsstufe für den Internet Explorer	27
.....b) WEB.DE-Zertifikate installieren im Internet Explorer	27
.....c) Eigene Zertifikate beantragen mit Internet Explorer	28
.....d) Zertifikate exportieren, importieren und sichern mit Internet Explorer	30
.....e) Digitale Unterschrift mit Outlook	32
.....f) Verschlüsseln mit Outlook	34
.....g) Wie sieht eine verschlüsselte Mail an mich aus?	37
.....h) Zertifikate verwalten mit Microsoft	38
7. Ganz einfach: FreeMail	41
8. Zertifikate erneuern und widerrufen	43
.....Das vorläufige Testzertifikat erneuern	43
.....Das 1 Jahr gültige WEB.DE Zertifikat erneuern	43
.....Zertifikate widerrufen	43
9. Hotline: Fragen und Antworten aus unserer Benutzerberatung	44
10. Ausblick	48
Anhang	
I Die Fingerprints des WEB.DE Trustcenters	50
II Allgemeine Geschäftsbedingungen für das TrustCenter von WEB.DE	51
III Zertifizierungsrichtlinien des WEB.DE-TrustCenters	55
IV Die Zertifikathierarchie des WEB.DE-TrustCenters	59
V Glossar	61
Impressum	63

1. Warum Verschlüsselung?

E-Mail-Verschlüsselung? Das ist doch alles viel zu kompliziert! Oder?

Nein – lassen Sie sich nichts erzählen! Verschlüsselung ist kein Tummelplatz für selbsternannte Internet-Experten. Sichere E-Mail ist auch kein Privileg für gestandene Internet-Nutzer mit mindestens zwei Jahren Surferfahrung und Internetführschein. Jeder kann es.

Was auf den ersten Blick so komplex und kompliziert aussieht ist mit dem TrustCenter (<http://trust.web.de>) von WEB.DE ganz einfach. Versprochen. Lassen Sie sich auf keinen Fall abschrecken und gehen Sie die einfachen Schritt für Schritt-Anleitung durch. Schon nach kurzer Zeit werden Sie Ihre erste E-Mail verschlüsselt und unterschrieben verschicken können. Ob Netscape oder Internet Explorer – die nötigen Bordwerkzeuge für sichere Kommunikation mit Ihrer E-Mail-Adresse sind integriert. Damit Ihre elektronische Post bleibt, was sie ist: Privatsache!

Kryptografie für Faule und Unterwegs

FreeMail (<http://freemail.web.de>) von Web.de richtet sich an den „faulen User“ und an alle, die unterwegs auf Ihre E-Mail zugreifen wollen oder müssen. Alles was für sichere



Armin Gellweiler, Chefredakteur WEB.DE

Kommunikation gebraucht wird ist bereits eingebaut. FreeMail übernimmt die gesamte technische Seite – Sie müssen lediglich zwei Kästchen anklicken und die Nachricht abschicken. Sie werden sich fragen, warum wir nicht gleich alles über FreeMail abwickeln? Diese besonders elegante Methode für sichere E-Mails können wir nur für eine kostenlose E-Mail-Adresse@web.de anbieten. Für alle anderen E-Mail-Adressen wie zum Beispiel @t-online.de oder @meinefirma.de ist das WEB.DE TrustCenter Ihr Ansprechpartner. Mehr zu FreeMail lesen Sie ab Seite 41.

Zehn Argumente für die Verschlüsselung

1. Nehmen Sie Ihr Grundrecht auf Briefgeheimnis wahr!

Das Grundgesetz garantiert in Artikel 10 das Briefgeheimnis. Da man elektronische Post nicht in Umschläge stecken kann, kann dieses Grundrecht hier nur durch Verschlüsselung gewahrt werden. http://www.bundestag.de/gesetze/gg/gg_10.htm

2. Unverschlüsselte Mails sind unsicherer gegen Lauscher als Postkarten.

Postkarten werden manchmal von neugierigen Postboten gelesen. E-Mails können von viel mehr Leuten gelesen werden.

3. „Ich habe doch nichts zu verbergen“ – Irrtum.

Jeder hat eine Privatsphäre. Beispiel Gesundheit: Würden Sie einen Arzt per Internet zum Beispiel wegen Hämorrhoiden um Rat fragen? Verschlüsselt können Sie auch vertrauliche Themen in E-Mails behandeln.

4. Der Lauschangriff läuft längst.

E-Mails werden längst im großen Stil abgehört und ausgewertet. Unter dem Codenamen Echelon filtern Superrechner heute schon einen großen Teil aller E-Mails nach Inhalten, die für Geheimdienste interessant sein könnten.

5. Die Bösen verschlüsseln sowieso.

Gegen Verschlüsselung wird oft eingewendet, dass diese Techniken Verbrechern das Leben zu leicht machen. Das Gegenteil ist der Fall. Wer einen Raub verabreden will, tut das ohnehin nur verschlüsselt. Wenn Sie aber ein größeres Bargeschäft unverschlüsselt vereinbaren, laden Sie die Räuber geradezu ein.

6. Sie wissen zuviel.

Ihre Daten sind wertvoller als Sie denken. Adressenlisten zum Beispiel sind bares Geld. Rechnungen, Angebote, beiläufige Bemerkungen in Mails können die Konkurrenz mit wertvollen Informationen versorgen. Klar sind die Mitbewerber meistens ehrlich. Aber deshalb lassen Sie die Eingangstür zu Ihrer Firma doch auch nicht offen stehen, oder?

7. Online Shopping 1

Egal, ob Sie online kaufen oder verkaufen wollen: Kreditkarten-Nummern und ähnliche Informationen sollten stets verschlüsselt werden.

8. Online Shopping 2

Die digitale Signatur stellt sicher, dass Käufer und Verkäufer wirklich die sind, für die sie sich ausgeben. Angebote oder Bestellungen unter falschem Namen sind ausgeschlossen.

9. Beispiel Jobsuche

Lassen Sie nie Bewerbungsunterlagen auf dem Kopierer Ihrer Firma liegen. Und E-Mails zu dem Thema sollten grundsätzlich verschlüsselt werden.

10. Verschlüsseln Sie besser alles.

Wenn Sie gerade dabei sind, verschlüsseln Sie alle oder möglichst viele Ihrer Mails. Denn wenn Sie nur vereinzelt chiffrieren, fallen die verschlüsselten Mails auf. Wenn Sie eine einzelne verschlüsselte Mail von Ihrem Arbeitsplatz aus an eine Konkurrenzfirma schicken, dann sollten Sie sich nicht erwischen lassen. Was könnte so eine Mail enthalten außer einer Bewerbung?

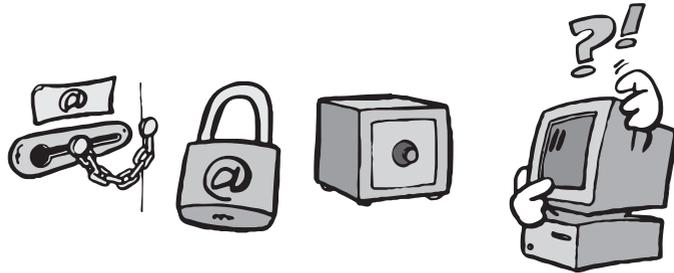
Ist das wirklich sicher?

Ja. Die Methoden, mit denen verschlüsselt wird, sind öffentlich bekannt und werden von Experten weltweit untersucht, diskutiert und immer wieder auf die Probe gestellt. Es ist bekannt, dass die digitalen Schlösser funktionieren und wie sie funktionieren. Jetzt kommt es auf die Schlüssel an, vor allem auf Ihren privaten Schlüssel. Hüten Sie diesen Schlüssel wie Ihren Augapfel. Wenn Sie mit Ihren Schlüsseln sorgsam umgehen, dann ist die Verschlüsselung wirklich sicher.

Und noch etwas: Sie sollten Ihr Mailprogramm auf starke Verschlüsselung einstellen, um sicher zu gehen. Dabei wird die Schlüssellänge erhöht. Wie das geht, lesen Sie für *Netscape* auf Seite 16 und für *Microsoft* auf Seite 27.

Es ist nämlich theoretisch ganz leicht, die Verschlüsselung zu knacken. Die Methode dazu nennt man „Brute Force“, „Rohe Gewalt“. Man muss nur alle möglichen Schlüssel durchprobieren. Deshalb hängt die Sicherheit grundsätzlich von der Schlüssellänge ab. Wenn Sie einen 40-Bit-Schlüssel verwenden, muss ein Code-Knacker 2^{40} Schlüssel ausprobieren, um Ihren zu finden, das sind 1.099.511.627.776 Schlüssel. Bei einem 128-Bit-Schlüssel müssen 2^{128} Schlüssel durchprobiert werden. Das sind ungefähr 340.282.366.920.900.000.000.000.000.000.000.000.000.000 Schlüssel. Bis die alle durchprobiert sind, lebt keiner mehr, der sich für das Ergebnis interessiert.

Die Sicherheit, die Verschlüsselung bietet, ist immer eine Sicherheit auf Zeit. Absolute Sicherheit gibt es nicht, übrigens auch sonst nirgendwo. Beim Verschlüsseln von Daten kommt es darauf an, die Zeit, die jemand zum Brechen des Codes braucht, in astronomische Höhen zu treiben. Und es sind tatsächlich astronomische Zeitspannen, die zum Brechen hinreichend langer Schlüssel gebraucht würden. Schlüssel von 40 Bit Länge sind schon geknackt worden, auch die Sicherheit von 56-Bit-Schlüsseln ist zweifelhaft.



Ein 56-Bit-Schlüssel ist im Januar 1999 mit Hilfe von fast 100.000 PCs innerhalb eines Tages geknackt worden. Details dazu finden Sie unter <http://www.rsa.com/pressbox/html/990119-1.html>. Ein 40-Bit-Schlüssel hätte dieser Rechenpower nicht viel länger als eine Sekunde standgehalten.

Mit einem 128-Bit-Schlüssel dagegen würden die Computer immer noch rechnen, denn bei gleicher Rechenleistung müsste man 10.000.000.000.000.000.000 Jahre veranschlagen, um den Schlüssel zu knacken. Das liegt daran, dass sich der Rechenaufwand zum Knacken des Codes mit jedem Bit verdoppelt. Merke: ein Bit mehr = doppelte Sicherheit. Selbst wenn die verfügbare Rechenleistung sich jedes Jahr verdoppeln würde, würde es noch 72 Jahre dauern, bis ein 128-Bit-Schlüssel zu knacken wäre.

2. Was brauche ich dazu?

Mit welchen Programmen geht das?

Das WEB.DE-TrustCenter benutzt die Methode S/MIME zum Verschlüsseln und Unterschreiben. Zur Zeit funktioniert das WEB.DE-TrustCenter reibungslos mit den Internet-Programmen von Netscape und Microsoft. Weitere Programme werden dazukommen.

Sie können das Trustcenter aber auch mit nahezu beliebigen Internet-Browsern benutzen, wenn Sie auf den Web-basierten E-Mail-Dienst FreeMail zugreifen. (Internet-Browser heißt das Programm, mit dem Sie Internet-Seiten anschauen.) Sie finden FreeMail unter <http://freemail.web.de>. Wie das Trustcenter mit FreeMail funktioniert, lesen Sie auf Seite 41.

Die Verschlüsselung hängt nicht vom Betriebssystem ab. Wenn es für Ihr Betriebssystem eine Netscape-Variante gibt, können Sie am Trustcenter teilnehmen.

Wenn Sie in einem Netzwerk arbeiten, kann es sein, dass Sie einzelne Details mit Ihrem Systembetreuer absprechen müssen, bevor Sie das TrustCenter benutzen können.

Warum ist das nicht gleich eingebaut?

Ihren Haustürschlüssel geben Sie nicht aus der Hand, es sei denn an besonders vertrauenswürdige Personen. Tatsächlich haben aber schon mehrere Leute Ihren Schlüssel in der Hand gehabt, die Sie gar nicht kennen. Wer das war? Es waren die Schlosser, die den Schlüssel hergestellt haben und die Händler und Spediteure, die Schloss und Schlüssel transportiert haben. Natürlich sind diese Leute vertrauenswürdig (hoffentlich).

Aber viel praktischer wäre es doch, wenn Sie Ihren Schlüssel selbst herstellen könnten. Dann könnten Sie sicherstellen, dass niemals jemand den Schlüssel in die Hand bekommt, auch nicht bevor Sie ihn einsetzen. Bei digitalen Schlüsseln ist das tatsächlich möglich, und es wird auch so gemacht. E-Mail-Programme werden ohne Schlüssel ausgeliefert. Stattdessen enthalten die Programme eine Funktion, mit der Sie selbst auf Ihrem eigenen Computer Ihre Schlüssel herstellen können.

Die Schlüssel, die Sie auf diese Weise erzeugen, bestehen immer aus zwei Teilen, einem privaten und einem öffentlichen (*siehe Seite 8*). Ihr Mailprogramm erzeugt beide Teile völlig selbständig. Auch wenn Sie dabei mit unserem Server per Internet verbunden sind, verlässt Ihr privater Schlüssel nie Ihren Rechner. Das ist einer der Gründe, weshalb Sie unbedingt Sicherheitskopien Ihrer Schlüssel anfertigen sollten: Es gibt sonst nur ein einziges Exemplar! Und sollte dieses Exemplar durch irgendeine Panne verloren gehen, bekommen Sie nirgends einen Nachschlüssel. Es ist beim derzeitigen Stand der Technik keine Methode bekannt, Nachschlüssel für verlorene digitale Privatschlüssel zu einem bezahlbaren Preis innerhalb einer erlebbaren Zeit anzufertigen. (*siehe vorige Seite*)

Bleibt eine Frage: Wenn Sie Ihre Schlüssel selbst herstellen, wozu brauchen Sie dann das Trustcenter? Die Antwort finden Sie im nächsten Abschnitt.

3. Was ist das: Verschlüsselung, Unter- schrift, Zertifikat?

Die Sicherheit von E-Mails beruht wesentlich auf den drei Elementen Verschlüsselung, Unterschrift und Zertifikat. Die Verschlüsselung schützt vor Lauschern, die Unterschrift vor Fälschern und das Zertifikat vor Betrügern. Technisch beruhen alle drei auf dem selben Prinzip, dem der asymmetrischen Schlüssel.

Asymmetrische Schlüssel

Wenn Sie Ihre Wohnung betreten, schließen Sie sie mit einem Schlüssel auf. Wenn Sie von innen abschließen, benutzen Sie denselben Schlüssel. Es gibt aber auch Mechanismen, die nur in einer Richtung funktionieren, zum Beispiel ganz normale Briefkästen. Wenn Sie einen Brief einwerfen, benutzen Sie die Klappe am Briefkasten. Das kann jeder. Der Brief fällt rein, kann aber nicht mehr entnommen werden. Um den Briefkasten zu leeren, muss man aber den Schlüssel dazu haben. Und den hat nur der Besitzer. Genau so funktionieren asymmetrische Schlüssel. Der öffentliche Schlüssel wirkt wie die Briefkastenklappe: Hier kann jeder eine Mail einwerfen, d.h. verschlüsseln, so dass keiner mehr dran kommt. Der private Schlüssel ist der, mit dem man den Briefkasten leert. Nur mit ihm sind die verschlüsselten Mails noch zugänglich.

Verschlüsselung

Die Verschlüsselung ist das erste und wichtigste Glied in der Sicherheitskette. Ohne Verschlüsselung ist bei E-Mails so gut wie nichts sicher. Sie können nicht wissen, ob eine Mail wirklich von dem Absender stammt, der drauf steht. Niemand weiß, ob

Ihre Mails wirklich beim Empfänger ankommen. Lauscher und Fälscher können sich irgendwo im Dickicht des Internet verstecken und Ihre Mails abfangen und manipulieren.

Wenn Sie ein S/MIME-Schlüsselpaar haben, können Sie damit Ihr Ende des Mail-Weges absichern. Andere können sicherstellen, dass Mails für Sie wirklich nur bei Ihnen ankommen. Dazu müssen sie die Mails an Sie mit Ihrem öffentlichen Schlüssel chiffrieren. Und wenn Sie einen Text mit Ihrem privaten Schlüssel signieren, kann jeder mit Ihrem

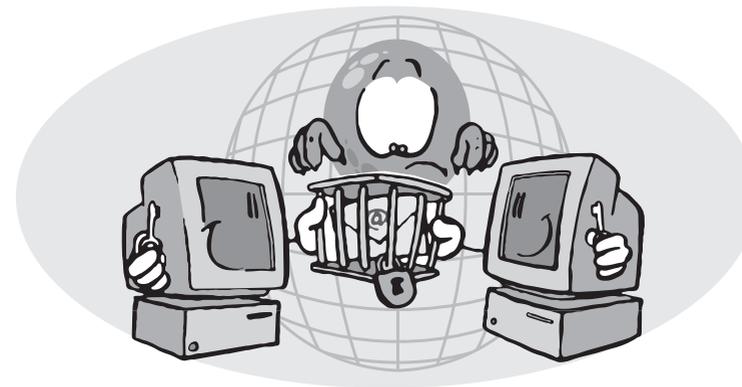


öffentlichen Schlüssel überprüfen, ob der Text von Ihnen stammt. Damit ist sichergestellt, dass Sie wirklich der Urheber des Textes sind.

Damit die Sache wirklich sicher wird, muss auch die andere Seite der Mailverbindung abgesichert werden. Darum muss sich Ihr Mailpartner selbst kümmern, denn den eigenen Schlüssel stellt ja jeder selbst her (siehe Seite 7).

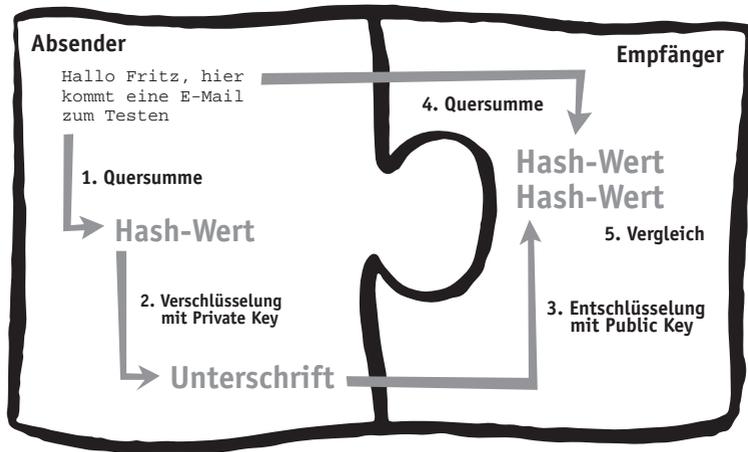
Nehmen wir an, Ihre Mailpartnerin heißt Milly und hat ebenfalls ein Schlüsselpaar. Dann können sie einen Brief an Milly mit Millies öffentlichem Schlüssel kodieren, so dass nur Milly ihn mit ihrem privaten Schlüssel lesen kann. So ist sicher, dass der Brief wirklich nur bei Milly ankommt.

Jetzt sind beide Seiten abgesichert, Sie können sich auf die E-Mail-Verbindung verlassen. Ihre Mails an Milly unterschreiben Sie mit Ihrem Privatschlüssel und verschlüsseln sie mit Millies öffentlichem Schlüssel. So können Sie sichergehen, dass niemand außer Milly die Mail liest und Milly kann sich darauf verlassen, dass die Mail wirklich von Ihnen ist.



Und wie funktioniert eigentlich die Signatur?

Die digitale Signatur erfüllt die gleiche Funktion wie eine Unterschrift auf Papier. Sie könnten auch den Text mit Ihrem privaten Schlüssel chiffrieren - aber dann müsste man ihn erst dekodieren um ihn zu lesen. Ein signierter Text bleibt klar lesbar. Erst wenn die Echtheit überprüft werden soll, kommt die Technik ins Spiel. Und so funktioniert das ganze:



1. Aus dem Text Ihrer Mail wird nach einem mathematischen Verfahren eine Art Quersumme gebildet, der sogenannte Hash-Wert. (sprich „Häsch-Wert“)
2. Dieser Hash-Wert wird mit Ihrem privaten Schlüssel chiffriert. Das Ergebnis ist Ihre digitale Unterschrift für genau diesen einen Text.
3. Der Text kann weiterhin gelesen werden. Jetzt soll die Echtheit überprüft werden. Der Empfänger entschlüsselt Ihre digitale Signatur. Das Ergebnis ist die Quersumme der Original-Mail, die Sie abgeschickt haben.
4. Er bildet die Quersumme der Mail, die ihm vorliegt.
5. Der Vergleich der beiden Werte bringt den Beweis. Übereinstimmung: Die Mail ist echt, sie stimmt Bit für Bit mit dem Original überein. Unterschiede: Die Mail ist gefälscht.

In der Praxis laufen diese Vorgänge automatisch ab.

Zertifikat

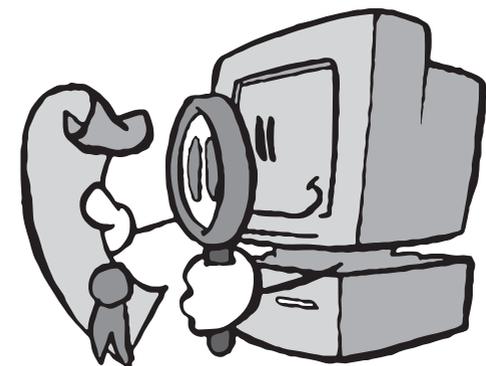
Die Sache hat einen Haken. Stellen Sie sich vor, Sie bekommen per E-Mail eine Einladung von Gerhard Schröder, und zwar verschlüsselt und signiert. Würden Sie der Mail glauben? Wahrscheinlich nicht, und Sie hätten Recht mit Ihrem Misstrauen. Die Mail kann nämlich trotz Verschlüsselung und Unterschrift von einem Betrüger stammen. Dieser könnte sich eine E-Mail-Adresse auf den Namen Gerhard Schröder besorgen. Das ist kein Problem und kostet noch nicht einmal Geld. Dann erstellt er sich ein Schlüssel-paar, das geht mit jedem Browser. So kann er Mails im Namen des Kanzlers schreiben, verschlüsseln und signieren. „Dagegen muss doch was getan werden!“ sagen Sie jetzt vielleicht. Richtig. Wir tun gerade was dagegen.

An dieser Stelle kommen Trustcenter ins Spiel. Trustcenter überprüfen die Identität von Schlüsselinhabern. Wir von WEB.DE schicken zu diesem Zweck einen Brief mit einem zusätzlichen Schlüssel, dem Freischaltcode, an die Adresse, die Sie bei der Anmeldung angeben. Wenn dieser Brief ankommt, kann können Sie mit diesem Freischaltcode und Ihrem persönlichen Passwort Ihr Zertifikat aktivieren. Wir wissen dann, dass die angegebene Adresse stimmt, und bestätigen das gegenüber anderen Benutzern.

Sollte sich tatsächlich jemand als Bundeskanzler bei uns anmelden, dann werden wir den Freischaltsschlüssel an das Bundeskanzleramt schicken. War die Anmeldung das Werk eines Witzboldes, läuft das Zertifikat nach vier Wochen aus. Gleichzeitig erfährt Gerhard Schröder durch unseren Brief, dass jemand mit seinem Namen Schabernack treiben wollte.

Nur wenn der Kanzler wirklich selbst hinter der Anmeldung steckt, kann er das Zertifikat freischalten. Um das Zertifikat freizuschalten, muss er sich zunächst mit seinem persönlichen Passwort bei unserem Server anmelden. Das persönliche Passwort hat er sich bei der Anmeldung selbst ausgedacht. Erst wenn er dieses Passwort eingegeben hat, kann er den Freischaltsschlüssel benutzen. Betrüger haben keine Chance.

(Es sei denn, der Betrüger hätte die gleiche Postadresse wie Sie, würde unter Ihrem Namen mailen und Ihre Post abfangen. In dem Fall sollten Sie sich überlegen, mit wem Sie da zusammen wohnen oder arbeiten.)



5. Wie bekomme ich das Nötige von WEB.DE?

Zuerst melden Sie sich an

Sie können das WEB.DE-TrustCenter bequem in Ihrem Browserfenster benutzen. Sie melden sich an, füllen die Formulare aus und erhalten ein vorläufiges Zertifikat, das Sie sofort benutzen können. Dann warten Sie auf Post von uns. Wenn Sie per Briefpost Ihren Freischaltcode erhalten, können Sie Ihr endgültiges Zertifikat aktivieren. (Es kann gut sein, dass Sie diese Gebrauchsanweisung zusammen mit Ihrem Freischaltsschlüssel erhalten haben.)

Damit Ihr E-Mail-Programm mit Zertifikaten von WEB.DE arbeiten kann, muss zuerst das Zertifikat von WEB.DE selbst installiert sein. Es kann sein, dass das schon der Fall ist. Dann hat der Hersteller Ihres Mailprogramms uns schon als Vertrauensinstanz akzeptiert.

Wenn nicht, müssen Sie zunächst Ihr Einverständnis erklären, dass Sie das WEB.DE-TrustCenter als Vertrauensinstanz akzeptieren. Technisch passiert das dadurch, dass Sie die Zertifikate des Trustcenters in Ihrem Browser installieren. Die Identität des Trustcenters wird genauso durch ein Zertifikat beglaubigt wie später Ihre eigene. Allerdings haben wir dieses Zertifikat nicht von einem übergeordneten Trustcenter erhalten, sondern selbst angefertigt. Deshalb gibt es eine andere Methode, unsere Zertifikate zu überprüfen: Sie können uns anrufen, und sich fernmündlich die Zertifikate bestätigen lassen. Dazu brauchen Sie den sogenannten „Fingerprint“ auf Seite 50. Vergleichen Sie die abgedruckten Fingerprints mit denen, die Sie online erhalten und dem, den Sie telefonisch von uns erfragen. Die Werte sollten niemals voneinander abweichen.

Um Ihr eigenes Zertifikat zu bekommen, müssen Sie ein paar Dialogfenster beantworten. Wir haben Anleitungen für Sie vorbereitet, die diesen Vorgang Schritt für Schritt zeigen. (*Netscape siehe Seite 18, Microsoft siehe Seite 28*)

Was passiert mit diesen Daten, wie schützt WEB.DE die Daten?

Die Daten des TrustCenters sind bei WEB.DE auf einem einzelnen Computer gespeichert, der nicht mit dem Firmennetz von WEB.DE verbunden ist. Dieser Rechner verwaltet ausschließlich die Daten des Trustcenters und sonst nichts. Er ist besonders gesichert. Unbefugte Zugriffe werden durch spezielle Sicherheitshard- und -software unterbunden.

Die Sicherheitskopie des privaten Schlüssels ist in drei Teile aufgeteilt worden, die an drei verschiedenen sicheren Orten hinterlegt sind. Drei unserer Mitarbeiter sind je für eins dieser Teile verantwortlich. Niemand kennt den Aufbewahrungsort aller drei Teile. Eine Sicherheitskopie der geheimen Schlüssel als Ganzes existiert nicht. Ein Missbrauch dieser Schlüssel ist damit unmöglich. Das Original des geheimen Schlüssels ist durch eine Krypto-Karte und komplexe Passwörter gesichert. Die Passwörter sind nur den Administratoren des TrustCenters bekannt und werden von diesen geheimgehalten. Die

4. Warum S/MIME und nicht PGP?

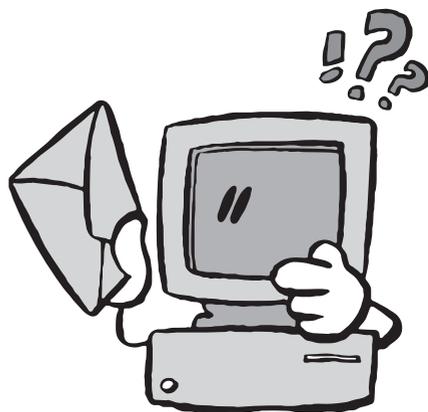
Wenn Sie zu den alten Hasen im Internet gehören, dann fragen Sie sich jetzt vielleicht, weshalb wir nicht PGP unterstützen. Dafür gibt es zwei Gründe.

Erstens beschäftigen wir uns, seit es die Firma WEB.DE gibt, mit dem World Wide Web. Die Lösung, die wir anbieten, hängt eng mit dem Web zusammen, weil sie mit den E-Mail-Komponenten wichtiger Browser funktioniert. PGP ist bisher nicht in Browser integriert.

Zweitens funktioniert PGP etwas anders als das Protokoll S/MIME, das wir verwenden. Beide Protokolle sind als offizieller Internet-Standard in der Diskussion. Welches sich durchsetzen wird, muss sich noch zeigen. Allerdings brauchen Sie für PGP eigentlich gar kein Trustcenter. PGP verwendet an Stelle zentraler Vertrauensinstanzen das sogenannte „Netz des Vertrauens“. Dieses Netz funktioniert nach dem Motto: „Ich kenne einen, der einen kennt, der einen kennt, der den Absender dieser Mail kennt. Also vertraue ich dem in einem gewissen Maß.“ Technisch funktioniert das so, dass man im Bekanntenkreis gegenseitig die PGP-Schlüssel signiert. Das Modell funktioniert tatsächlich. Trustcenter und das Netz des Vertrauens haben beide Vor- und Nachteile. Aber wenn man für PGP kein Trustcenter braucht, warum sollten wir dann eins einrichten?

PGP

PGP ist die Abkürzung für „Pretty good Privacy“, zu deutsch etwa: „Ziemlich gute Privatsphäre“. PGP ist ein Verschlüsselungsprogramm, das ähnlich arbeitet wie S/MIME. Es verwendet die gleichen Verschlüsselungstechniken. Wenn Sie mehr darüber wissen wollen: <http://www.pgpi.com/>



6. Schritt für Schritt

Im Folgenden zeigen wir Ihnen anhand der E-Mail-Programme von Microsoft und Netscape Schritt für Schritt, wie das TrustCenter funktioniert. Der grundsätzliche Ablauf ist derselbe, es sind aber nicht immer alle Schritte notwendig. Erledigen Sie am besten die Schritte 1 bis 4 in einer Sitzung. Erfahrungsgemäß schleichen sich hin und wieder Fehler ein, wenn man den Vorgang unterbricht und später fortsetzt.

a) Festlegen der Sicherheitsstufe

Überlegen Sie sich zuallererst, welche Sicherheitsstufe Sie brauchen. Wenn Ihnen die voreingestellte Schlüssellänge von 56 Bit nicht ausreicht, dann verlängern Sie die Schlüssel auf 128 Bit. Damit sind Sie auf der sicheren Seite (für die Bedeutung der Schlüssellängen *vergleiche Seite 6*). Wie sicher Ihr Browser verschlüsselt, können Sie auf folgenden Test-Seiten herausfinden:

<https://www.karlsruhe.de/cgi-bin/seccheck.pl>

<https://www.fortify.net/sslcheck.html>

b) Installation der Root-Zertifikate

Ein Mail-Programm, das mit Trustcentern zusammenarbeitet, enthält eine Liste von Trustcentern, denen vertraut werden kann. Üblicherweise trägt der Hersteller des Mail-Programms hier schon ausgewählte Trustcenter ein. Sollte das WEB.DE-TrustCenter in dieser Liste noch nicht eingetragen sein, dann müssen Sie das nachholen. Praktisch geschieht das dadurch, dass Sie unsere Zertifikate in Ihrem Mail-Programm installieren.

c) Zertifikat beantragen

Ihr eigenes Zertifikat erhalten Sie, indem Sie einige Online-Formulare bei uns ausfüllen. Dabei wird Ihr Schlüsselpaar auf Ihrem PC von Ihrem E-Mail-Programm erstellt. Wenn die Schlüssel fertig sind, wird der öffentliche Schlüssel zu unserem Server übertragen. Der Datensatz aus Ihrer Postadresse, E-Mail-Adresse und dem öffentlichen Schlüssel wird von unserem Server signiert und stellt das Zertifikat dar.

d) Zertifikate sichern, exportieren und importieren

Wenn Sie Ihr eigenes Zertifikat bekommen haben, sollten Sie es sofort sichern, am besten auf zwei verschiedenen Disketten. Denn von Ihrem privaten Schlüssel gibt es sonst keine Kopie, auch nicht auf unserem Server. Wenn Sie Zertifikate in Dateien kopieren, können Sie sie auch zwischen verschiedenen E-Mail-Programmen austauschen.

e) Digital unterschreiben

Sobald Sie ein Zertifikat haben, können Sie Mails digital unterschreiben.

f) Verschlüsseln

Verschlüsseln können Sie dagegen nur, wenn der Adressat Ihrer Mail Ihnen sein Zertifikat zugeschickt hat, indem er eine Mail an Sie digital unterschrieben hat.

g) Verschlüsselte Mails empfangen

Dafür können andere aber schon Mails an Sie verschlüsseln.

h) Zertifikate verwalten

Hier erfahren Sie, wie Sie herausfinden, welche Zertifikate auf Ihrem Rechner installiert sind. Falls Sie mehrere Zertifikate haben, ein Zertifikat löschen oder prüfen wollen, finden Sie ebenfalls Anleitungen.

Passwörter werden niemals im Klartext gespeichert, gesendet oder irgendwo notiert. Passwörter und Krypto-Karte werden nur für diesen einen Zweck benutzt und nicht auf anderen Systemen eingesetzt.

Ihr eigener privater Schlüssel wird direkt auf Ihrem Rechner erzeugt und ist uns noch nicht einmal bekannt.

Wo bekomme ich weitere Hilfe?

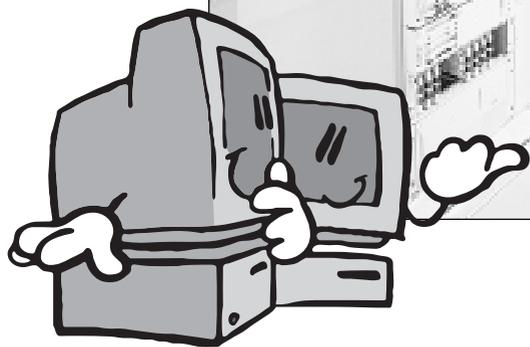
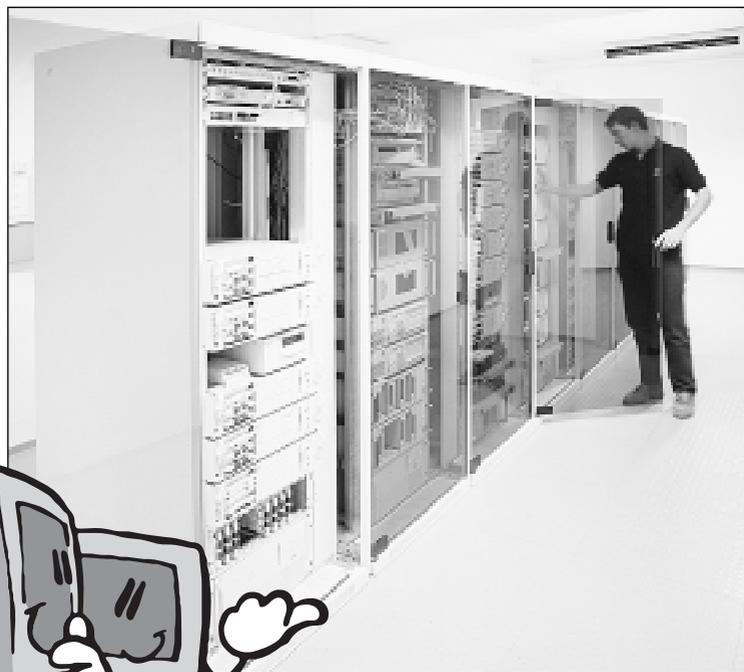
Wenn Sie noch Fragen haben, helfen wir Ihnen gerne weiter.

E-Mail: trust@web.de

Telefon: 0721/94329-36

Telefax: 0721/94329-22

Wie sieht ein TrustCenter aus?

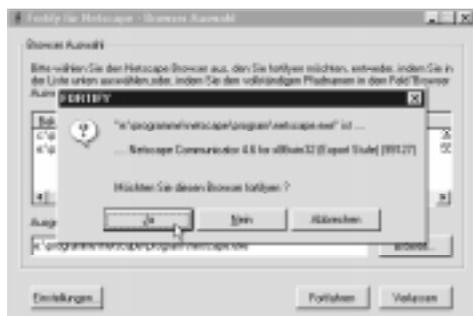


Netscape

a) Festlegen der Sicherheitsstufe für Netscape

Netscape unterliegt den amerikanischen Exportbestimmungen und erlaubt daher nur eine Schlüssellänge von 56 Bit. Sie können jedoch mit Hilfe des Programms Fortify die Schlüssellänge auf 128 Bit erhöhen. Das geht ganz einfach:

1. Laden Sie Sie Fortify von <http://www.fortifyfy.net> herunter. Der private Gebrauch ist kostenlos, Firmen müssen einen Obolus entrichten.
2. Installieren Sie das Programm und starten Sie es. Im Begrüßungsfenster klicken Sie auf „Starten“.



3. Fortify sucht nach installierten Netscape-Browsern. Wenn Sie eine oder mehrere Versionen von Netscape korrekt installiert haben, zeigt Fortify eine Liste dieser Browser an. Wählen Sie einen davon und klicken Sie auf „Fortfahren“.

4. Fortify nimmt Änderungen am Programmcode von Netscape vor. Falls Sie der Sache nicht trauen, können Sie Fortify automatisch eine Sicherheitskopie der Netscape-Programmdatei anfertigen lassen. Und nach der Abfrage für die Sicherheitskopie folgt schon die Erfolgsmeldung.

Wenn Sie zusammen mit ihrem Netscape-Browser das Programm Fortify benutzen, dann kann es bei der Installation ihres Zertifikates zu Unregelmäßigkeiten kommen: Mitunter zeigt der Browser bei der Installation von Zertifikaten nicht die üblichen Meldungen und Dialogfenster an. Das Zertifikat wird aber trotzdem korrekt installiert.

Weitere Informationen können Sie der mitgelieferten Dokumentation von Fortify entnehmen. Dort sind auch Methoden beschrieben, wie Sie die Sicherheit Ihres Netscape-Browsers testen können.

b) WEB.DE-Zertifikate installieren mit Netscape

Bevor Sie eigene Zertifikate mit Netscape beantragen können, müssen die WEB.DE-Zertifikate in Ihrem Browser installiert sein. Diese Zertifikate werden benötigt, um die digitalen Unterschriften von WEB.DE-TrustCenter- und FreeMail-Anwendern zu überprüfen. So installieren Sie die Zertifikate in Netscape:



Auf der Homepage des Trustcenters (<https://trust.web.de/>) finden Sie einen Link „WEB.DE-Root-Zertifikat installieren“.

Klicken Sie diesen Link an.

Es erscheint die Seite <https://trust.web.de/ooot.sql>. Hier finden Sie eine ähnliche Anleitung wie diese hier und vor allem die Links, mit denen Sie die Zertifikate installieren können.

Klicken Sie die WEB.DE-Zertifikate nacheinander an, um sie zu installieren.

Nach dem Mausklick auf „WEB.DE-Root-Zertifikat installieren“ öffnet sich das Fenster „Neuer Zertifikatsaussteller – Netscape“.

Klicken Sie auf .

Es folgt ein Fenster mit einer kurzen Hintergrundinformation.

Klicken Sie erneut auf .

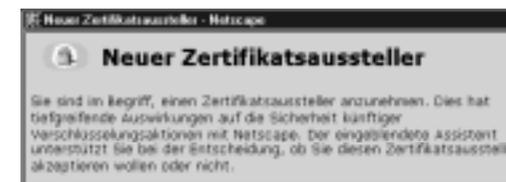
Im nächsten Schritt können Sie sehen von wem das Zertifikat für wen ausgestellt wurde. Im Bild sehen Sie die Informationen zum WEB.DE-Zertifikat, das von WEB.DE selbst ausgestellt wurde.

Wenn Sie auf „Mehr Info“ klicken, erscheint ein Fenster, in dem Sie den Fingerabdruck des Zertifikates überprüfen können. Den Fingerabdruck, den Sie in diesem Fenster sehen, können Sie mit dem auf Seite 50 abgedruckten vergleichen.

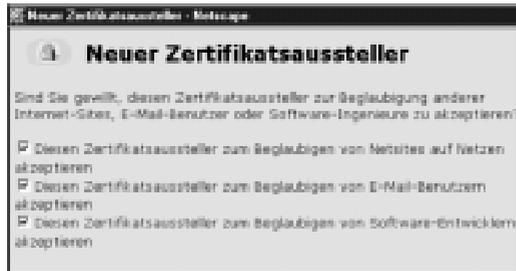
Sie können zur Überprüfung der Fingerprints auch gerne bei uns anrufen. Sie erreichen uns unter Tel. 0721/9432936. Dieses Telefon ist Montag bis Freitag zwischen 9.00 und 17.00 Uhr besetzt.

Schließen Sie das Fenster mit einem Klick auf OK.

Bezeichnung	MD5 Fingerprint
WEB.DE Root-Zertifikat installieren	8D D4 F5 1A 7D 70 46 5D D8 6F 4D 6B 41 83 99 93
WEB.DE CA-Zertifikat installieren	09 B2 B0 51 3C 0C 6B 5B 7C 3D D1 2D BD 63 A3 04
WEB.DE Trust-Zertifikat installieren	0B D6 22 68 4C 74 77 61 87 6F AD 0B 00 2D 14 70
WEB.DE-Zertifikat installieren (Classic Mediatechnik GmbH)	5F E4 D3 A6 7A A6 0F E7 5D AC AC 10 AC 2E 58 13



Im nächsten Schritt werden Ihnen 3 Optionen angeboten, von denen Sie unbedingt das erste und zweite Feld von oben durch einen Mausklick in das Kästchen aktivieren müssen. Sie müssen das Zertifikat für das Beglaubigen von Netsites akzeptieren, weil das



WEB.DE-TrustCenter selbst auf diese Weise als vertrauenswürdig eingestuft wird. Dass Sie das Beglaubigen von E-Mail-Benutzern akzeptieren müssen, versteht sich fast von selbst, denn das ist ja schließlich der Sinn der ganzen Übung. Das Beglaubigen von Software-Herstellern spielt zur Zeit noch keine Rolle. In Zukunft soll mit solchen Zertifikaten die Produkthaftung und Herstellergarantie bei Software sichergestellt werden, auch wenn Sie diese irgendwo aus dem Internet herunterladen.

Klicken Sie dann auf **Weiter**

Tragen Sie einen Namen für das Zertifikat ein. Der Name, mit dem das Zertifikat auch bei uns geführt wird, bietet sich an. Es ist der, den Sie vorher angeklickt haben, um

die Installationsprozedur zu starten. Ein abschließender Mausklick auf **Weiter** installiert das Zertifikat sicher in Ihrem Net-scape-Browser.

Diese Prozedur müssen Sie für alle vier WEB.DE-Zertifikate wiederholen: Root, CA, Trial und Cinetic. Wir haben vier verschiedene Zertifikate, weil das WEB.DE-Trust-Center Benutzerzertifikate in mehreren verschiedenen Sicherheitsstufen vergibt.

E-Mail verschlüsseln mit Netscape & Outlook

Mails im Internet werden in der Regel im Klartext verschickt. Privater, Techniker, Hacker - an vielen Stellen kann Ihre Post gelesen werden.

Machen Sie damit Schluss!

Vorpassen Sie Ihrer E-Mail Adresse Schutz und Regel.

... und dafür gibt's vom WEB.DE TrustCenter:

- **Kostenlose Zertifikate** für das digitale Unterschriften und Verschlüsseln Ihrer E-Mails mit Netscape and Outlook
- **Online-Check** für alle WEB.DE Zertifikate für RealTime Security

... gleich loslegen ?

E-Mail-Adresse **Zertifikat holen**

c) Eigene Zertifikate beantragen mit Netscape

Wenn die Zertifikate für das WEB.DE-TrustCenter in Ihrem Netscape-Browser installiert sind, können Sie Zertifikate für eigene E-Mail-Adressen beantragen. Dazu müssen Sie sich zunächst als Benutzer bei WEB.DE registrieren. Wenn Sie schon eine FreeMail-Adresse haben, können Sie mit Ihrem Benutzernamen und Passwort von FreeMail auf das Trustcenter zugreifen. Auf die Registrierungsformulare gehen wir hier nicht näher ein, da sie sich selbst erklären. Achten Sie darauf, Ihre Adresse sorgfältig einzugeben, denn an diese Adresse wird der Activator-Key geschickt, mit dem Sie Ihr Zertifikat dann dauerhaft aktivieren. Bei der Registrierung geben Sie sich selbst ein Passwort. Die-

ses Passwort brauchen Sie später wieder, um mit Ihrem Activator Key Ihr Zertifikat freischalten zu können.

Den Zertifikats-Antrag erreichen Sie auf verschiedene Arten, zum Beispiel, indem Sie auf der Homepage des Trustcenters unten rechts Ihre E-Mail-Adresse eintragen und auf „Zertifikat holen“ klicken.

Auf der nächsten Seite müssen Sie Benutzername und Passwort eingeben, und dann erscheint der Online-Antrag für ein Zertifikat.

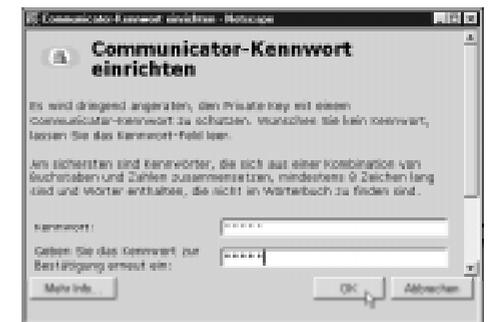
Beachten Sie die verfügbare Schlüssellänge. 768 und 1024 Bit stehen nur zur Verfügung, wenn Sie Ihren Net-scape-Browser mit Fortify vorbereitet haben. Sind nur 512 Bit verfügbar, dann können Sie entweder auf dieser Sicherheitsstufe weitermachen, oder den Vorgang abbrechen, um Netscape zunächst mit Fortify auf längere Schlüssel vorzubereiten (siehe Seite 16).

Sobald Sie auf „Weiter“ klicken, wird die Schlüssel-Erzeugung in Netscape gestartet. Netscape zeigt das mit einem Hinweisfenster an. Bestätigen Sie diesen Hinweis, indem Sie auf „OK“ klicken.

Wenn Sie das erste Mal einen privaten Schlüssel erstellen, fordert Netscape Sie auf, ein Passwort zum Schutz ihrer Privatschlüssel einzurichten. Denken Sie sich ein sicheres Passwort aus, das nicht in einem Wörterbuch vorkommt, Sonderzeichen und Zahlen enthält und mindestens acht Zeichen lang ist. Haben Sie schon früher ein Passwort für die Zertifikate vergeben, so werden Sie jetzt nach diesem Passwort gefragt. Falls Sie dieses Passwort vergessen haben, hilft nur eins: Netscape komplett deinstallieren und neu installieren.

Nachdem Sie das Passwortfenster mit OK bestätigt haben, verschwinden die Fenster, der Cursor wird zur Sanduhr, und kurz darauf taucht eine neue Meldung unseres Servers in Ihrem Browserfenster auf:

In der Zwischenzeit ist eine Menge geschehen. Netscape hat intern Ihr Schlüsselpaar erzeugt und den öffentlichen Schlüssel dieses Paares an unseren Server geschickt. Der TrustCenter-Ser-



1 Zertifikat beantragen 2 Mail abrufen 3 Zertifikat installieren

Vielen Dank für Ihren Zertifikatsantrag!

Sie werden in den nächsten Minuten von uns per E-Mail benachrichtigt.

ver hat den Schlüssel in Empfang genommen, zusammen mit Ihren persönlichen Daten signiert und damit Ihr Zertifikat erzeugt. Das Zertifikat liegt nun zur Abholung bereit. Sie können das Zertifikat noch nicht sofort benutzen, weil erst Ihre E-Mail-Adresse überprüft werden muss. Das geschieht, indem unser Server eine Mail an genau diese Adresse schickt. Nur wenn Sie diese Mail erhalten, können Sie Ihr Zertifikat abholen. So ist sichergestellt, dass zertifizierte E-Mail-Adressen stets korrekt sind. Und das ist ja schließlich der Sinn der Sache.

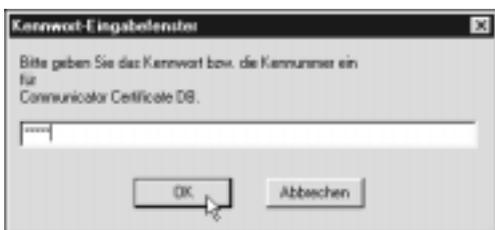
Sie müssen jetzt Ihre Mail mit dem Activator Key abholen. Bei hoher Netzauslastung kann es einige Minuten dauern, bis die Mail bei Ihnen ankommt. Sie brauchen den

Activator Key nicht abzutippen oder aus der Mail herauszukopieren, weil er bereits in der angegebenen URL enthalten ist. Es reicht, die URL anzuklicken. Der Activator-Key wird damit wieder zu unserem Server geschickt. Damit wir sicher

gehen können, dass der Key nach dieser Rundreise tatsächlich von Ihnen kommt, wird jetzt noch einmal Ihr persönliches Passwort abgefragt.

Sobald Sie sich mit Ihrem Passwort autorisiert haben, sendet unser Server Ihr Zertifikat an Ihren Computer. Netscape nimmt das Zertifikat in Empfang und installiert es in seiner Zertifikats-Datenbank. Dabei werden Sie noch einmal nach dem Kennwort gefragt, mit dem Sie die Zertifikate in Netscape schützen (Es sei denn, Sie haben auf den Kennwortschutz für Zertifikate in Netscape verzichtet).

Nach diesem Klick wird Ihr Zertifikat installiert. Fertig! Nach dieser ganzen Prozedur können Sie erst mal eine Pause machen. Aber dann wäre ein guter Zeitpunkt, die Früchte Ihrer Arbeit zu sichern. Denn Ihr privater Schlüssel existiert nur ein einziges Mal. Es gibt keine Sicherheitskopie. Also sollten Sie eine anfertigen (oder zwei). Wie das geht, lesen Sie auf den nächsten Seiten.



d) Zertifikate exportieren/importieren und sichern mit Netscape

Wofür ist das gut?

Sie können das Zertifikat exportieren um es zum Beispiel neben dem Netscape Messenger auch in Outlook 98 oder Outlook Express einzusetzen. Eine Sicherheitskopie ist sehr nützlich, falls Ihre Festplatte beschädigt oder die Zertifikats-Daten versehentlich gelöscht werden. Wenn Sie eine Kopie Ihres Zertifikates auf einer Diskette abspeichern, sind Sie jederzeit in der Lage, dieses Zertifikat erneut zu installieren. Wenn Sie Ihr Zertifikat verlieren und es nicht gesichert haben, sind alle Nachrichten verloren, die mit diesem Zertifikat verschlüsselt wurden. Wichtig: Sie können das Zertifikat auch nicht von unserem Server neu installieren, weil dieser nur Ihren öffentlichen Schlüssel gespeichert hat, nicht aber den privaten.

So speichern Sie eine Kopie Ihres Zertifikates



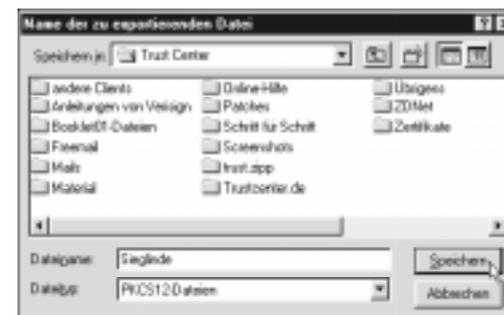
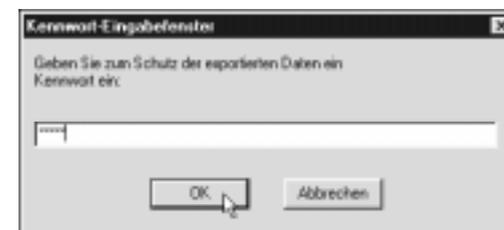
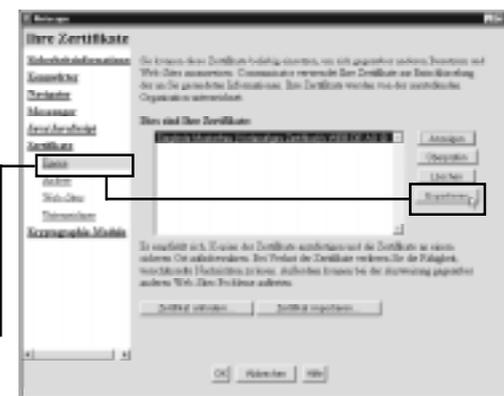
Klicken Sie auf das Sicherheitssymbol in der Navigationssymbolleiste („Sicherheitsinformationen anzeigen“).

Klicken Sie auf „Eigene“ unter „Zertifikate“ in der linken Menüleiste. Wählen Sie das gewünschte Zertifikat aus und klicken anschließend auf den „Exportieren“-Button.

Netscape fragt Sie dann zwei- bis dreimal nach einem Passwort. Wenn Sie die Zertifikatsdatenbank mit einem Passwort geschützt haben, müssen Sie zunächst dieses eingeben. Danach bestimmen Sie ein Passwort, mit dem die Export-Datei geschützt wird, und geben dieses zur Bestätigung ein zweites Mal ein. Dieses Passwort brauchen Sie später, um Ihr Zertifikat neu zu importieren.

Wählen Sie anschließend Speicherort und Dateiname aus, unter dem Sie Ihr Zertifikat abspeichern wollen, zum Beispiel auf einer Diskette unter dem Namen „Mein Zertifikat“.

Lagern Sie die Diskette an einem sichern Ort. Wenn Sie ganz sicher gehen wollen, kopieren Sie die Datei auf eine zweite Diskette und lagern Sie die an einer anderen Stelle.

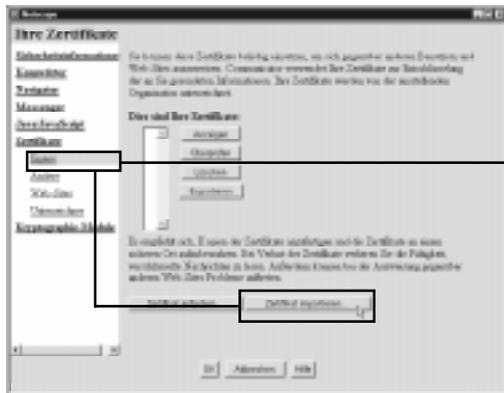


Wie importiere ich ein Zertifikat oder die Sicherheitskopie meines Zertifikates?

Als ersten Schritt müssen Sie Ihr Zertifikat auf eine Diskette oder einen anderen Datenträger sichern (siehe vorigen Abschnitt). Wenn Sie Ihr Zertifikat erfolgreich gesichert haben, können Sie es erneut installieren oder es auf einen anderen Rechner übertragen.



Klicken Sie auf das Sicherheitssymbol in der Navigationssymbolleiste („Sicherheitinformationen anzeigen“).



Klicken Sie auf „Eigene“ unter „Zertifikate“ in der linken Menüleiste. Klicken Sie auf den „Zertifikat importieren“-Button am unteren Ende der Seite.

Geben Sie auf Anforderung Ihr Sicherheits-Passwort für die Zertifikatsdaten-bank an. Im folgenden Dateidialog wählen Sie die Zertifikatsdatei aus. Sie sollte das Dateiformat *.pfx oder *.p12 haben. Klicken Sie auf „Öffnen“. Geben Sie Ihr Kopie-Passwort an und klicken auf „OK“. Netscape meldet den erfolgreichen Import und zeigt das Zertifikat in der Liste der Zertifikate an. Wenn das importierte Zertifikat aus einem anderen Programm als Netscape stammt, kann es sein, dass das Zertifikat nicht im Klartext, sondern als unverständliche Ziffernfolge angezeigt wird. Die Zertifikate sind aber nicht beschädigt.



e) Digitale Unterschrift mit Netscape Messenger

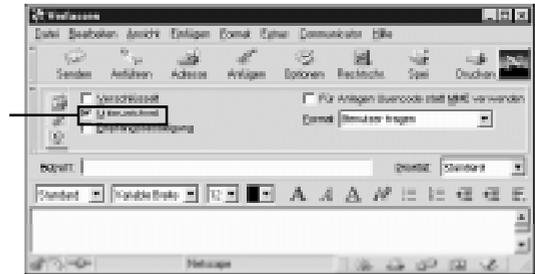


Die digitale Unterschrift stellt sicher, dass die elektronische Nachricht tatsächlich vom angegebenen Absender stammt und dass sie auf dem Weg vom Absender zum Empfänger nicht verändert wurde. Der Inhalt der Nachricht ist aber für jeden lesbar. Erst die Verschlüsselung sorgt dafür, dass Ihre Post von Unbefugten nicht gelesen werden kann. Das „Unterzeichnet“-Symbol in einer geöffneten E-Mail zeigt an, wenn sie digital unterschrieben ist. Das Zertifikat des Absenders, das in der digitalen Unterschrift enthalten ist, wird automatisch abgespeichert, so dass sie zukünftig verschlüsselte Nachrichten an ihn senden können.

Sie können einzelne E-Mails digital unterschreiben oder den Communicator so konfigurieren, dass automatisch alle ausgehenden E-Mails digital unterschrieben werden.

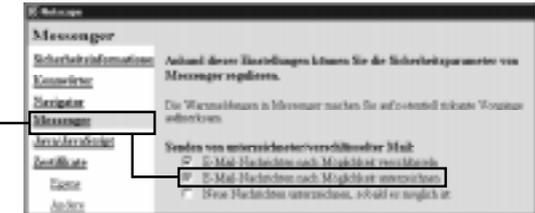
Einzelne E-Mails digital unterschreiben

Klicken Sie beim Verfassen einer neuen Nachricht auf „Sendeoptionen für Nachrichten“ und aktivieren Sie die Checkbox „Untertezeichnet“.



Automatisch alle ausgehenden E-Mails digital unterschreiben

Klicken Sie auf das Schloß-Symbol („Sicherheit“) in der Navigations-Leiste des Communicators oder wählen Sie die „Sicherheitseinstellungen“ im Menü „Communicator/Extras“. Wählen Sie unter den Sicherheitseinstellungen den Punkt „Messenger“ aus und aktivieren Sie die Checkbox „E-Mail-Nachrichten nach Möglichkeit unterschreiben“. Schließen Sie das Fenster mit OK.



f) Verschlüsseln mit Netscape Messenger

Die Verschlüsselung von E-Mails sorgt dafür, dass Ihre elektronische Post von Unbefugten weder gelesen noch verändert werden kann. Um aber eine Nachricht verschlüsseln zu können, benötigen Sie das Zertifikat des Empfängers. Sollten Sie vom Empfänger Ihrer Nachricht schon einmal eine digital unterschriebene Nachricht erhalten haben, so ist sein Zertifikat schon automatisch im Adressbuch gespeichert.

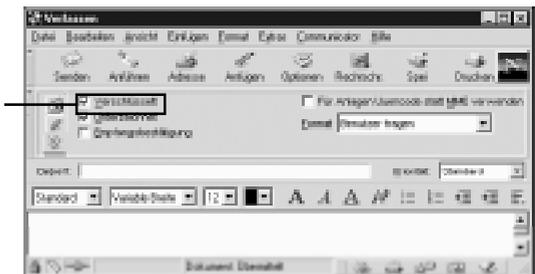
Enthält Ihr Adressbuch das Zertifikat des Empfängers nicht, so bitten Sie ihn um eine digital unterschriebene Nachricht.

Verschlüsselte E-Mails, die Sie selber erhalten, werden automatisch entschlüsselt. Beim Lesen der Nachricht zeigt ein Symbol an, dass die Nachricht verschlüsselt war.

Sie können einzelne E-Mails verschlüsseln oder den Communicator so konfigurieren, dass automatisch alle E-Mails verschlüsselt werden. Es können nur an diejenigen Empfänger verschlüsselte E-Mails verschickt werden, deren Zertifikate in Ihrem Adressbuch stehen.

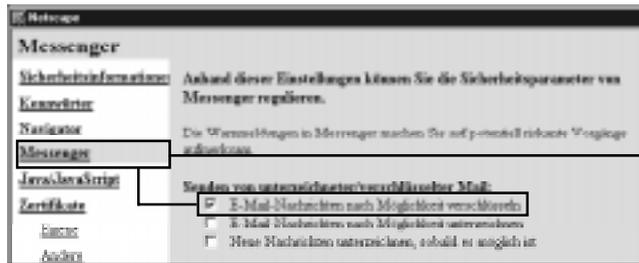
Einzelne E-Mail verschlüsseln

Klicken Sie beim Verfassen einer neuen Nachricht auf „Sendeoptionen für Nachrichten“ und aktivieren Sie die Checkbox „Verschlüsselt“.



Automatisch alle ausgehenden E-Mails verschlüsseln

Klicken Sie auf das Schloss-Symbol („Sicherheit“) in der Navigations-Leiste oder wählen Sie die „Sicherheit“ im Menü „Communicator/Extras“.



Wählen Sie unter den Sicherheitseinstellungen den Punkt „Messenger“ aus und aktivieren Sie die Checkbox „E-Mail-Nachrichten nach Möglichkeit verschlüsseln“.

g) Wie sieht eine an mich verschlüsselte E-Mail aus?

Wenn Ihnen jemand eine digital unterschriebene und verschlüsselte E-Mail geschickt hat, dann sieht sie so aus:



Ihr Browser hat die ganze Arbeit des Entschlüsselns für Sie bereits erledigt. In der rechten oberen Ecke sehen Sie ein Symbol, das wie eine Briefmarke aussieht. Diese „Briefmarke“ zeigt an, dass die E-Mail an Sie verschlüsselt wurde. Weitere Informationen zum Verschlüsselungsgrad erhalten Sie, wenn Sie auf dieses Symbol klicken.

h) Zertifikate verwalten mit Netscape Messenger

In den letzten Abschnitten haben Sie gelernt, wie Sie die grundlegenden Funktionen des TrustCenters mit Netscape nutzen können. Im folgenden lernen Sie, was Sie tun müssen, wenn Sie mehrere Zertifikate besitzen, wie Sie die vorhandenen Zertifikate einsehen und überprüfen können und wie Sie ein Zertifikat aus Netscape löschen.

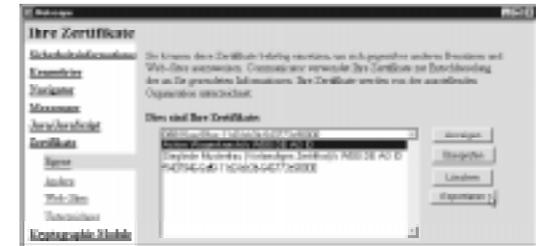
Gespeicherte Zertifikate ansehen und bearbeiten

Wenn Sie eine verschlüsselte E-Mail verschicken wollen, dann benötigen Sie das Zertifikat des Empfängers in ihrem Adressbuch. Der Communicator speichert automatisch das Zertifikat eines Absenders ab, wenn Sie eine digital unterschriebene Nachricht erhalten. Haben Sie das Zertifikat eines Empfängers noch nicht gespeichert, so bitten Sie ihn doch einfach um eine digital unterschriebene E-Mail. Welche Zertifikate auf Ihrem Computer gespeichert sind, sehen Sie wie folgt:

Klicken Sie auf das Schloss-Symbol („Sicherheit“) in der Navigations-Leiste des Communicators oder wählen Sie die „Sicherheit“ im Menü „Communicator/Extras“.

Wählen Sie unter den Sicherheitseinstellungen den Punkt „Eigene“ oder „Andere“ in der Zertifikate-Kategorie aus.

Wählen Sie das Zertifikat mit einem Klick aus, das Sie bearbeiten, überprüfen oder löschen wollen.



Welches Zertifikat soll's denn sein?

Besitzen Sie mehrere Zertifikate, so müssen Sie im Communicator festlegen, welches Ihrer Zertifikate Sie für die digitale Unterschrift nutzen wollen:

Klicken Sie auf das Schloss-Symbol („Sicherheit“) in der Navigations-Leiste des Communicators oder wählen Sie die „Sicherheit“ im Menü „Communicator/Extras“.

Wählen Sie unter den Sicherheitseinstellungen den Punkt „Messenger“ aus. Wählen Sie im Pulldownmenü unter dem Punkt „Zertifikat für Ihre unterzeichneten und verschlüsselten Nachrichten“ das Zertifikat aus, das Sie für Ihre E-Mails verwenden möchten.

Zertifikat aus Netscape löschen

Klicken Sie im Netscape-Menü auf den Punkt Sicherheit.

Klicken Sie in der linken Spalte unter „Zertifikate“ auf „Eigene“.

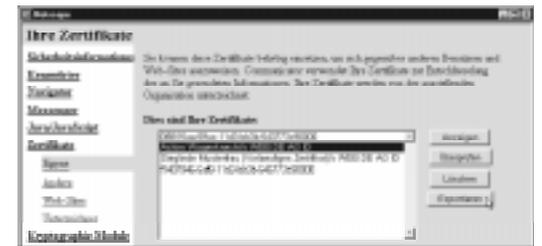
Wählen Sie das zu löschende Zertifikat per Mausklick aus und klicken Sie in der Spalte rechts auf „Löschen“.

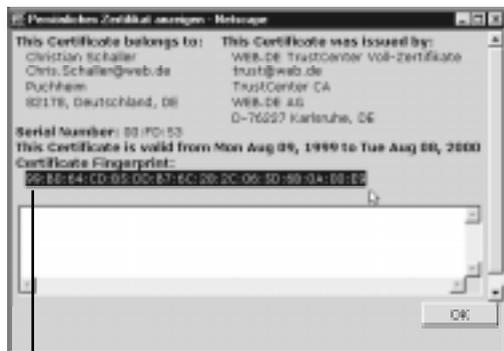
Lesen Sie die folgenden Sicherheitshinweise aufmerksam durch und bestätigen Sie das endgültige Löschen des Zertifikats.

Prüfen, ob ein Zertifikat gültig ist

Auf der TrustCenter-Homepage finden Sie die Funktion „Online-Check“. Hier kann jede und jeder anhand von Seriennummer oder Fingerprint ein Zertifikat des WED.DE TrustCenters überprüfen. Und So wird's gemacht:

Klicken Sie im Menü „Sicherheit“ und anschließend in der Navigationsleiste links im Unterpunkt „Zertifikate“ auf „Andere“.





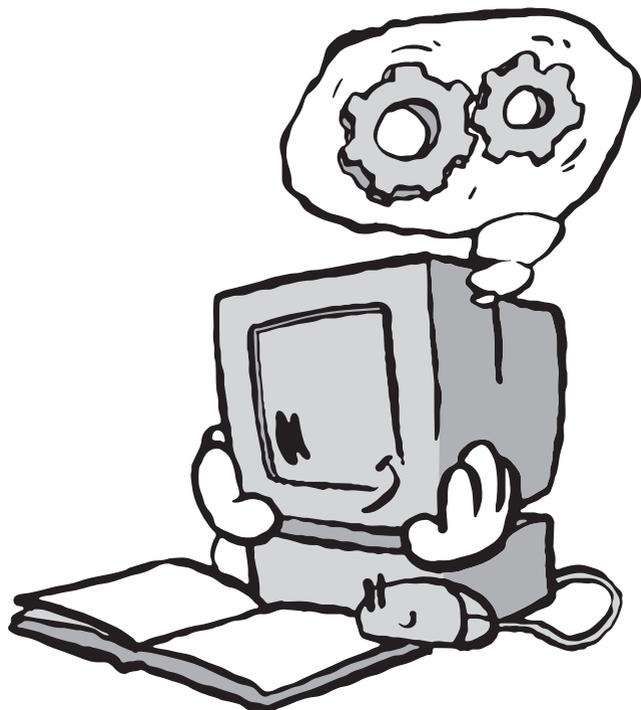
Mit Tastenkombination
»Strg-C«
kopieren!

Wählen Sie das zu prüfende Zertifikat aus der Liste im mittleren Fenster. Klicken Sie anschließend auf „Anzeigen/Bearbeiten“. Wichtig für den Online-Test: Kopieren Sie entweder die Seriennummer oder den Fingerprint in die Zwischenablage. (Setzen Sie den Mauszeiger an die erste Stelle der Seriennummer und ziehen Sie anschließend den Mauszeiger bei gedrückter linken Maustaste bis an die letzte Stelle der Seriennummer. Mit der Tastenkombination „STRG + C“ können Sie den Zahlenwust in die Zwischenablage kopieren.)

Schließen Sie alle Fenster mit einem Klick auf „OK“.

Setzen Sie die Seriennummer/Fingerprint durch die Tastenkombination „STRG + V“ in das entsprechende Feld auf der TrustCenter-Homepage ein und klicken Sie auf „Weiter“.

Das Zertifikat wird auf die Gültigkeit geprüft.



Microsoft

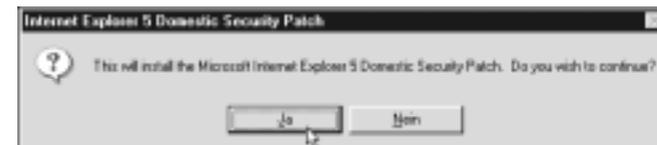
a) Erhöhen der Sicherheitsstufe für den Internet Explorer

Wenn Sie mit der Standard-Sicherheitsstufe zufrieden sind, können Sie diesen Schritt überspringen. Wenn Sie mehr Sicherheit wollen, können Sie die Schlüssellängen im Internet Explorer wie folgt erhöhen:

1. Laden Sie den 128-Bit-Security Patch für den Internet Explorer aus dem Internet (Adresse siehe Kasten).

2. Starten Sie die Datei Msie_5.0_win95_98_128.exe.

Bestätigen Sie die Nachfrage mit Ja. Das Programm schaltet die höheren Verschlüsselungsstufen im Internet Explorer frei und verlangt dann nach einem Neustart. Starten Sie Ihren Rechner neu. Von nun an können Sie auch mit dem Internet Explorer und Outlook starke Verschlüsselung nutzen.



Sicherheits-Patches

Internet Explorer 5

ftp://ftp.fu-berlin.de/unix/security/replay-mirror/browsers/128bit/MS-IEexplorer-v50/Msie_5.0_win95_98_128.exe

Internet Explorer 4.0

<ftp://ftp.fu-berlin.de/unix/security/replay-mirror/browsers/128bit/MS-IEexplorer-v40/msie40-128.exe>

Weitere Patches für andere Versionen und andere Programme

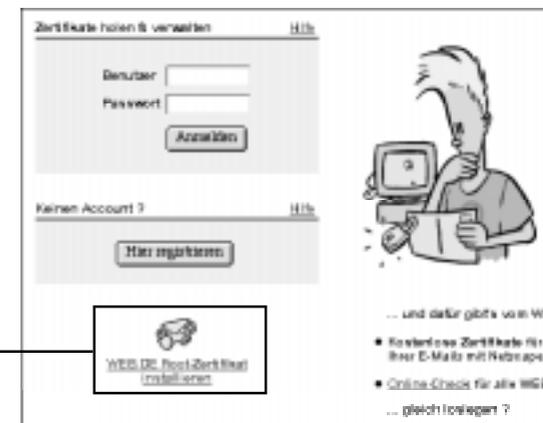
<ftp://ftp.fu-berlin.de/unix/security/replay-mirror/browsers/128bit/>

b) WEB.DE-Zertifikate

installieren im Internet Explorer

Bevor Sie eigene Zertifikate mit dem Internet Explorer beantragen können, müssen die WEB.DE-Zertifikate in Ihrem Browser installiert sein. Diese Zertifikate werden benötigt, um die digitalen Unterschriften von WEB.DE-TrustCenter- und FreeMail-Anwendern zu überprüfen. So installieren Sie die Zertifikate im Internet Explorer:

Auf der Homepage des Trustcenters (<https://trust.web.de/>) finden Sie einen Link „WEB.DE-Root-Zertifikat installieren“.

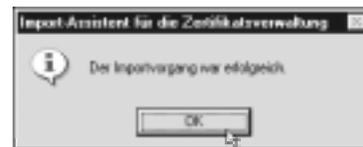




Es erscheint die Seite https://trust.web.de/oot.sql. Hier finden Sie eine ähnliche Anleitung wie diese hier und vor allem den Link, mit dem Sie die Zertifikate installieren können. Klicken Sie diesen Link an.

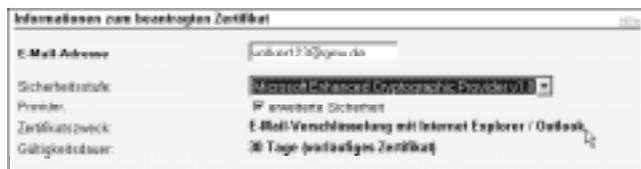
Es erscheint der irreführende Hinweis, es werde jetzt ein Datei heruntergeladen. Lassen Sie sich davon nicht irritieren. Markieren Sie die Option „Die Datei von ihrem aktuellen Ort öffnen“ und klicken Sie auf OK.

Als nächstes meldet sich der „Import-Assistent für die Zertifikatsverwaltung“. Die drei aufeinanderfolgenden Dialogfelder dieses Assistenten können sie alle mit „Weiter“ oder „Fertigstellen“ bestätigen. Zuletzt erhalten Sie die Erfolgsmeldung:



c) Eigene Zertifikate beantragen mit Internet Explorer

Melden Sie sich beim TrustCenter an und wählen Sie die Seite „Zertifikat beantragen“. Der „Microsoft Enhanced Cryptographic Provider“ und die erweiterte Sicherheit stehen nur zur Verfügung, wenn Sie den SecurityPatch installiert haben. Wenn Sie die Installa-

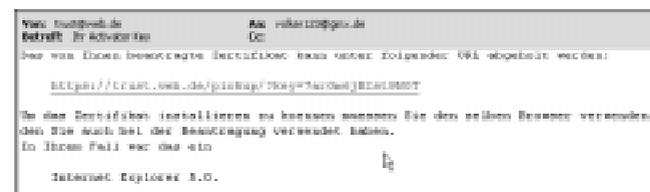


tion jetzt nachholen möchten, brechen Sie den Vorgang ab, installieren Sie den Patch und starten Sie den Zertifikats-Antrag dann neu (siehe Seite 27).

Sobald Sie auf klicken, meldet sich der „Container des privaten Schlüssels“ mit der Meldung „Creating a new RSA exchange key!“. Bestätigen Sie das Fenster mit OK. Es erscheint das gleiche Fenster, jetzt mit der Meldung „Signing data with your private exchange key!“ Bestätigen Sie wiederum mit OK.

Als nächstes taucht eine neue Meldung unseres Servers in Ihrem Browserfenster auf. In der Zwischenzeit ist eine Menge geschehen. Der Internet Explorer hat intern Ihr Schlüsselpaar erzeugt und den öffentlichen Schlüssel dieses Paares an unseren Server geschickt. Der TrustCenter-Server hat den öffentlichen Schlüssel in Empfang genommen, zusammen mit Ihren persönlichen Daten signiert und damit Ihr Zertifikat erzeugt. Das Zertifikat liegt nun zur Abholung bereit. Sie können das Zertifikat noch nicht sofort benutzen, weil erst Ihre E-Mail-Adresse überprüft werden muss. Das geschieht, indem unser Server eine Mail an genau diese Adresse schickt. Nur wenn Sie diese Mail erhalten, können Sie Ihr Zertifikat abholen. So ist sichergestellt, dass zertifizierte E-Mail-Adressen stets korrekt sind. Und das ist ja schließlich der Sinn der Sache.

Sie müssen jetzt Ihre Mail mit dem Activator Key abholen. Bei hoher Netzauslastung kann es einige Minuten dauern, bis die Mail bei Ihnen ankommt. Sie brauchen den Activator



Key nicht abzutippen oder aus der Mail herauszukopieren, weil er bereits in der angegebenen URL enthalten ist. Es reicht, die URL anzuklicken. Der Activator-Key wird damit wieder zu unserem Server geschickt. Damit wir sichergehen können, dass der Key nach dieser Rundreise tatsächlich von Ihnen kommt, wird jetzt noch einmal Ihr persönliches Passwort abgefragt.



Auf der folgenden Seite klicken Sie auf  und der Internet Explorer fügt das neue Zertifikat in seine Zertifikatsdatenbank ein. In der Version 5 des Internet Explorers funktioniert das ohne weitere Abfragen. Sollten doch noch Dialogfenster auftauchen, achten Sie auf die Meldungen und bestätigen Sie die Abfragen. Zuletzt erhalten Sie die Erfolgsmeldung.



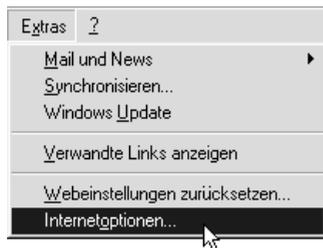
d) Zertifikate exportieren/importieren und sichern mit Internet Explorer

Wofür ist das gut?

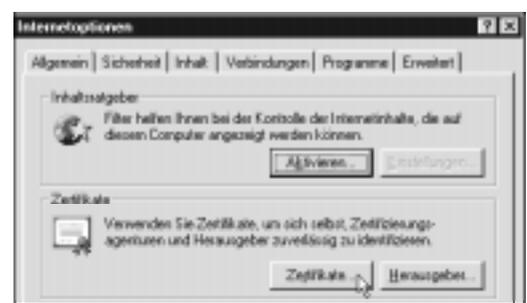
Sie können das Zertifikat exportieren um es zum Beispiel neben den Microsoft-Programmen auch Netscape einzusetzen. Eine Sicherheitskopie ist sehr nützlich, falls Ihre Festplatte beschädigt oder die Zertifikats-Daten versehentlich gelöscht werden. Wenn Sie eine Kopie Ihres Zertifikates auf einer Diskette abspeichern, sind Sie jederzeit in der Lage, dieses Zertifikat erneut zu installieren. Wenn Sie Ihr Zertifikat verlieren und es nicht gesichert haben, sind alle Nachrichten verloren, die mit diesem Zertifikat verschlüsselt wurden. Wichtig: Sie können das Zertifikat auch nicht von unserem Server neu installieren, weil dieser nur Ihren öffentlichen Schlüssel gespeichert hat, nicht aber den privaten.

So speichern Sie eine Kopie Ihres Zertifikates

Wählen Sie aus dem Hauptmenü unter „Extras“ (im IE 4 unter „Ansicht“) den Menüpunkt „Internetoptionen aus.“



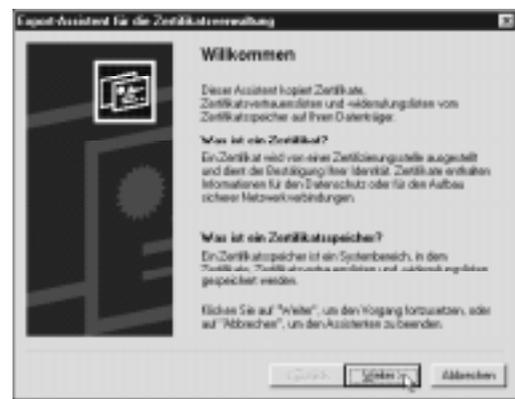
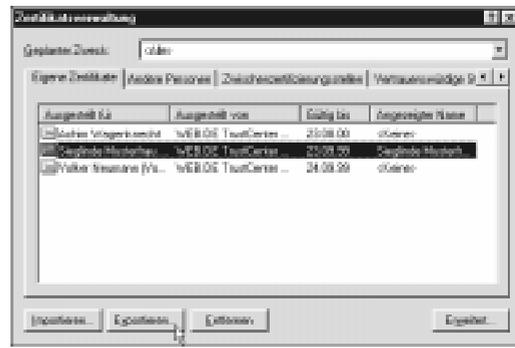
Wählen Sie den Reiter „Inhalt“ und klicken anschließend auf den Button „Zertifikate“ (im IE 4 Button „Eigene ...“) unter dem Menüpunkt „Zertifikate“.



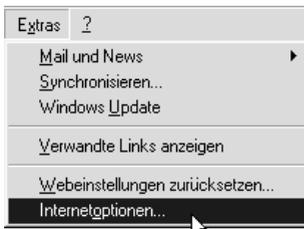
Wählen Sie aus der Liste „Eigene Zertifikate“ das gewünschte Zertifikat aus und klicken auf „Exportieren“.

Es meldet sich der „Export-Assistent für die Zertifikatsverwaltung“. Dieser Assistent führt Sie mit mehreren Dialogfenstern durch den Exportvorgang. Klicken Sie auf „Weiter“.

Im nächsten Schritt werden Sie gefragt, ob Sie das Zertifikat einschließlich des privaten Schlüssels exportieren wollen. Bejahen Sie diese Frage, indem Sie das entsprechende Feld anklicken. Ohne den privaten Schlüssel können Sie das exportierte Zertifikat weder als Sicherheitskopie verwenden noch es in ein anderes Programm importieren. Im nächsten Fenster wird das Dateiformat festgelegt. Lassen Sie die Voreinstellungen unverändert und klicken Sie auf „Weiter“. Weil die Exportdatei auch den privaten Schlüssel enthält, wird sie durch ein Passwort geschützt. Das Passwort vergeben Sie im nächsten Fenster. Im folgenden Fenster legen Sie fest, wo und unter welchem Namen das Zertifikat gespeichert wird. (Klicken Sie auf „Durchsuchen“, um den Speicherort zu bestimmen.) Schließlich zeigt der Assistent eine Zusammenfassung an und speichert Ihr Zertifikat.



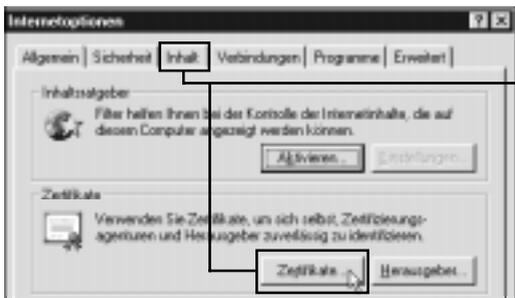
Daß das gespeicherte Zertifikat auch Ihren privaten Schlüssel enthält, stellt Windows im Symbol der Zertifikatsdatei anschaulich dar. Kopieren Sie die Datei ein- oder zweimal auf Diskette und lagern Sie diese an einem sichern Ort.



So importieren Sie ein Zertifikat

Als ersten Schritt müssen Sie Ihr Zertifikat auf eine Diskette oder einen anderen Datenträger sichern (siehe vorigen Abschnitt). Wenn Sie Ihr Zertifikat erfolgreich gesichert haben, können Sie es erneut installieren oder es auf einen anderen Rechner oder ein anderes Programm übertragen.

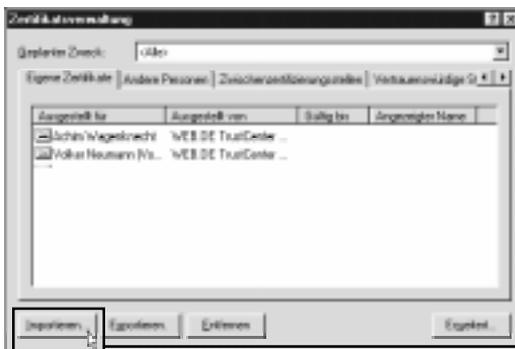
Wählen Sie aus dem Menü „Extras/Internet-Optionen“ (im IE 4 unter „Ansicht“).



Im Fenster „Internet-Optionen“ klicken Sie auf die Registerkarte „Inhalt“ und dort auf den Button „Zertifikate“.

In der Zertifikatsverwaltung klicken Sie auf „Importieren“.

Es meldet sich der „Import-Assistent für die Zertifikatsverwaltung“. Bestätigen Sie das Willkommensfenster des Assistenten mit einem Klick auf „Weiter“ und wählen Sie im nächsten Fenster die Datei, die Sie importieren wollen, indem Sie auf „Durchsuchen“ klicken.



Möglicherweise müssen Sie den Dateityp im Dateidialog auf „Alle Dateien“ schalten, um Zertifikate aus Netscape zu importieren. Im nächsten Fenster wird das Kennwort der Zertifikatsdatei abgefragt. Außerdem können Sie bestimmen, ob der private Schlüssel wiederum exportierbar sein soll und ob die erweiterte Sicherheitseinstellungen des Internet Explorers angewendet werden sollen. Kreuzen Sie beide Optionen an und klicken Sie auf „Weiter“. Die folgenden Fenster können Sie einfach bestätigen, bis der Import abgeschlossen ist.



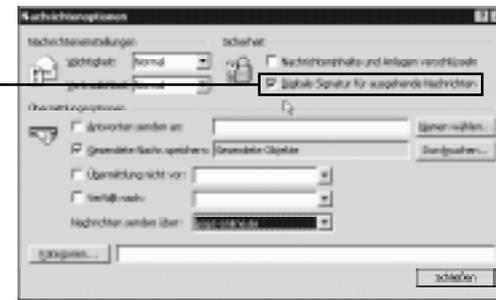
e) Digitale Unterschrift mit Outlook

Die digitale Unterschrift stellt sicher, dass die elektronische Nachricht tatsächlich vom angegebenen Absender stammt und dass sie auf dem Weg vom Absender zum Empfänger nicht verändert wurde. Der Inhalt der Nachricht ist aber für jeden lesbar. Erst die Verschlüsselung sorgt dafür, dass Ihre Post von Unbefugten nicht gelesen werden kann.

Das Zertifikat, das im Microsoft Internet Explorer 4.0 (oder höher) installiert ist, kann in Outlook genutzt werden, um ausgehende Nachrichten digital zu unterschreiben. Sie können einzelne E-Mails digital unterschreiben oder Outlook so konfigurieren, dass automatisch alle ausgehenden E-Mails digital unterschrieben werden.

Einzelne E-Mail digital unterschreiben

Klicken Sie in der neuen Nachricht auf „Optionen“ und aktivieren Sie die Checkbox „Digitale Signatur für ausgehende Nachrichten“.



In Outlook Express müssen Sie zunächst festlegen, welches Zertifikat Sie für die digitale Unterschrift nutzen wollen, selbst wenn Sie nur ein einziges haben. Vorher können Sie keine Mails digital unterschreiben.

Gehen Sie im Menü „Extras“ auf den Menüpunkt „Konten“ und wählen Sie den Reiter „E-Mail“. Markieren Sie die Adresse Ihres Mailservers und klicken Sie auf den „Eigenschaften“-Button.



Wählen Sie den Reiter „Sicherheit“. Aktivieren Sie die Checkbox „Digitale ID verwenden“ und klicken Sie auf den Button „Digitale ID...“

Achtung: Das funktioniert nur, wenn die WEB.DE-Root-Zertifikate installiert sind.

Im nächsten Fenster markieren Sie ein Zertifikat und bestätigen Sie mit „OK“-Button.

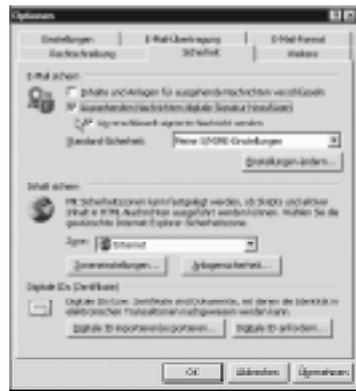
Nachdem Sie das Zertifikat auf diese Weise zum Unterschreiben aktiviert haben, können Sie Mails digital signieren. Klicken Sie in der neuen Nachricht auf „Signieren“

Das Siegel-Symbol zeigt an, dass die Nachricht digital unterschrieben wird.



Automatisch alle ausgehenden E-Mails digital unterschreiben

Gehen Sie in den Menüpunkt „Extras/Optionen“ und wählen Sie den Reiter „Sicherheit“. Aktivieren Sie die Checkbox „Ausgehenden Nachrichten digitale Signatur hinzufügen“.



Outlook Express

In Outlook Express sieht dieses Fenster geringfügig anders aus. Sie finden die gleiche Option zum Ankreuzen, müssen dafür nur ein bisschen weiter unten klicken.

f) Verschlüsseln mit Outlook

Die Verschlüsselung von E-Mails sorgt dafür, dass Ihre elektronische Post von Unbefugten weder gelesen noch verändert werden kann. Um aber eine Nachricht verschlüsseln zu können, benötigen Sie das Zertifikat des Empfängers. Deshalb sollten Sie, wenn Sie eine digital unterschriebene E-Mail erhalten, das darin enthaltene Zertifikat des jeweiligen Absenders in ihrem Kontaktverzeichnis speichern, um es später zum Verschlüsseln zur Verfügung zu haben.

Enthält Ihr Adressbuch das Zertifikat des Empfängers nicht, so bitten Sie den Empfänger am besten um eine digital unterschriebene Nachricht. Diese enthält dann automatisch das Zertifikat.



Das Zertifikat in das Kontaktverzeichnis aufnehmen

Öffnen Sie die unterschriebene Nachricht. Sie erkennen unterschriebene Nachrichten an dem Symbol

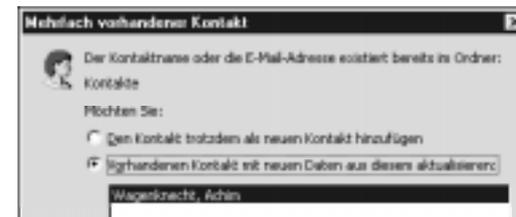
Klicken Sie mit der rechten Maustaste auf den Namen im Feld „Von“, und klicken Sie anschließend im Kontextmenü auf „Zu den Kontakten hinzufügen“.

Falls sich in Ihrer Kontaktliste bereits ein Eintrag für diese Person befindet, klicken Sie auf „Vorhandenen Kontakt aktualisieren“.

Das Zertifikat wird damit zusammen mit dem Kontakteintrag für diesen Empfänger gespeichert. Sie können nun verschlüsselte E-Mail-Nachrichten an diese Person senden.

Zum Anzeigen der Zertifikate für einen Kontakt doppelklicken Sie auf den Namen der Person und klicken anschließend auf die Registerkarte „Zertifikate“.

Wenn Sie selber eine verschlüsselte E-Mail erhalten, so wird sie von Outlook automatisch entschlüsselt. Ein Schloss-Symbol zeigt an, dass die Nachricht verschlüsselt war.



Outlook Express

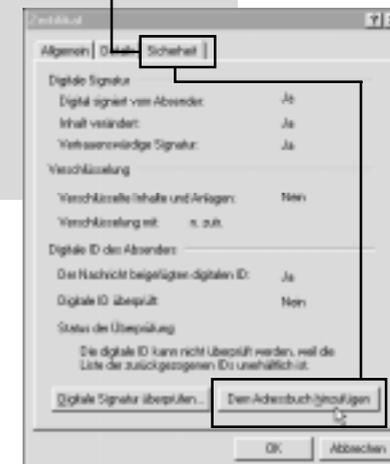
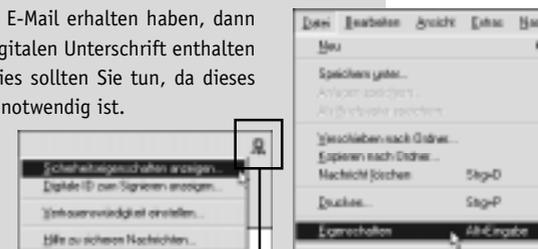
Wenn Sie eine digital unterschriebene E-Mail erhalten haben, dann können Sie das Zertifikat, das in der digitalen Unterschrift enthalten ist, in Ihrem Adressbuch speichern. Dies sollten Sie tun, da dieses zum Versenden verschlüsselter E-Mails notwendig ist.

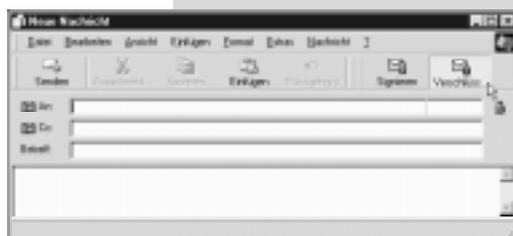
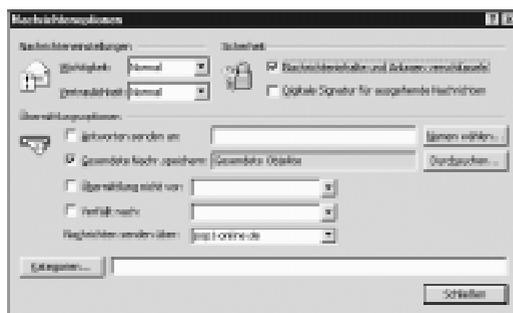
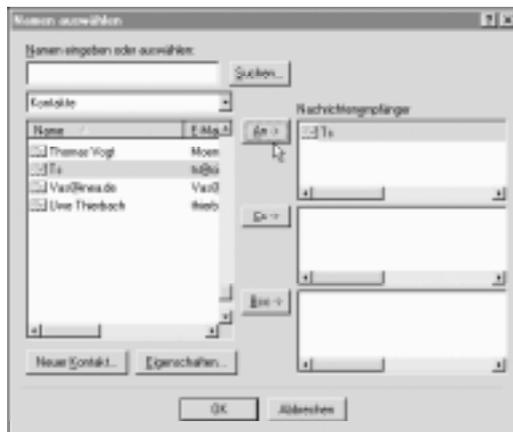
Öffnen Sie die digital unterschriebene Nachricht und gehen Sie in den Menüpunkt „Datei/Eigenschaften“.

oder

Öffnen Sie die digital unterschriebene Nachricht und klicken Sie auf das Siegel-Symbol. Wählen Sie im aufklappenden Kontextmenü den Menüpunkt „Sicherheits-eigenschaften anzeigen“.

Wählen Sie den Reiter „Sicherheit“ und klicken Sie auf „Dem Adressbuch hinzufügen“.





Einzelne E-Mail verschlüsseln

Sie können einzelne E-Mails verschlüsseln oder Outlook so konfigurieren, dass automatisch alle ausgehenden E-Mails verschlüsselt werden. Es können nur an diejenigen Empfänger verschlüsselte E-Mails verschickt werden, deren Zertifikate in Ihrer Kontaktliste stehen.

Klicken Sie auf „Neue Mail schreiben“. Um die Empfängeradresse auszuwählen, klicken Sie auf „An“.

Wählen Sie den gewünschten Empfänger aus. Wenn der gewünschte Kontakt mit einem Symbol für ein Zertifikat gekennzeichnet ist, können Sie Mails an diese Adresse verschlüsseln.

Klicken Sie in der neuen Nachricht auf „Optionen“ und aktivieren Sie die Checkbox „Nachrichteninhalte und Anlagen verschlüsseln“.

Outlook Express

In Outlook Express geht das etwas einfacher. Sie brauchen nur in der neuen Nachricht auf „Verschlüsseln“ zu klicken.

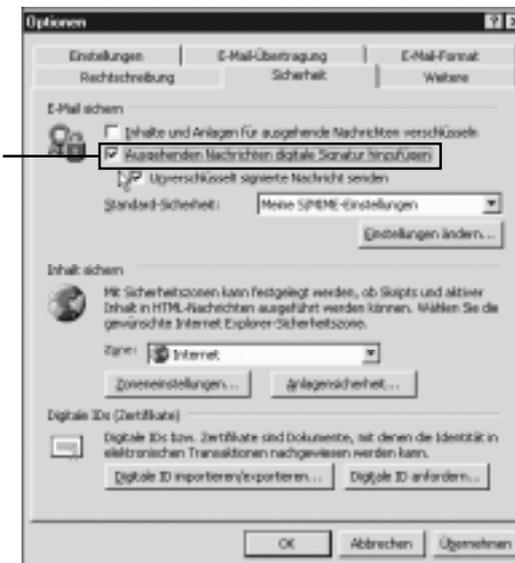
Ein Schloss-Symbol rechts neben dem Adressfeld zeigt an, dass die Nachricht verschlüsselt wird.

Automatisch alle ausgehenden E-Mails verschlüsseln

Gehen Sie in den Menüpunkt „Extras/Optionen“ und wählen Sie den Reiter „Sicherheit“. Aktivieren Sie die Checkbox „Inhalte und Anlagen für ausgehende Nachrichten verschlüsseln“. Aktivieren Sie die Checkbox „Ausgehenden Nachrichten: digitale Signatur hinzufügen“.

Outlook Express

In Outlook Express finden Sie die gleiche Option im gleichen Dialogfenster, nur ein bisschen tiefer.



g) Wie sieht eine verschlüsselte Mail an mich aus?

Wenn Ihnen jemand eine verschlüsselte E-Mail geschickt hat, dann sieht sie so aus:

Ihr Browser hat die ganze Arbeit des Entschlüsselns für Sie bereits erledigt. Rechts über dem Mailtext sehen Sie ein kleines, symbolisiertes Schloss .

Dieses Schloss zeigt an, dass die E-Mail an Sie verschlüsselt wurde.

Weitere Informationen zum Verschlüsselungsgrad erhalten Sie, wenn Sie in Outlook auf das Schloss klicken.

Outlook Express

In Outlook Express sieht das fast genauso aus. Verschlüsselung und Signatur werden an der gleichen Stelle durch die gleichen Symbole angezeigt.



h) Zertifikate verwalten mit Microsoft

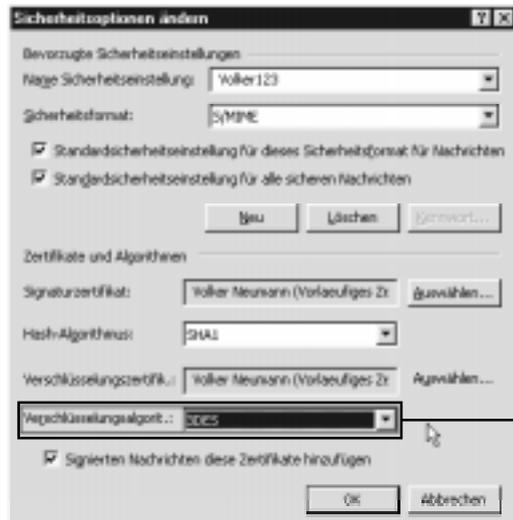
In den letzten Abschnitten haben Sie gelernt, wie Sie die grundlegenden Funktionen des TrustCenters mit Microsoft-Programmen nutzen können. Im folgenden lernen Sie, was Sie tun müssen, wenn Sie mehrere Zertifikate besitzen, wie Sie die vorhandenen Zertifikate einsehen und überprüfen können und wie Sie ein Zertifikat aus dem Speicher löschen.

Welches Zertifikat soll's denn sein?

Besitzen Sie mehrere Zertifikate, so müssen Sie in Outlook festlegen, welches Ihrer Zertifikate Sie für die digitale Unterschrift nutzen wollen. Wählen Sie im Menü „Extras“

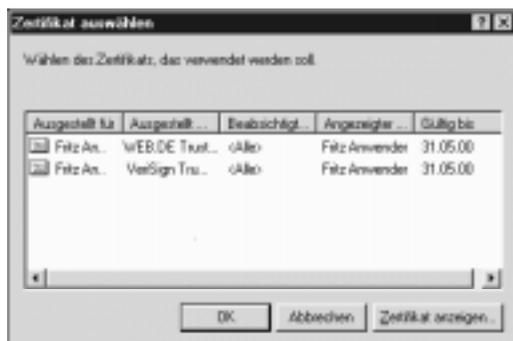
den Menüpunkt „Optionen“ und dann den Reiter „Sicherheit“ und klicken Sie auf den Button „Einstellungen ändern“.

Geben Sie Ihren „Sicherheitseinstellungen“ einen Namen Ihrer Wahl. Wählen Sie als „Sicheres Nachrichtenformat“ S/MIME aus. Klicken Sie unter „Signaturzertifikat“ auf den Button „Auswählen...“



TIP: Im Feld „Verschlüsselungsalgorithmus“ können Sie sehen, ob starke Verschlüsselung (3DES oder RC2-128 Bit) zur Verfügung steht oder nicht.)

Markieren Sie ein Zertifikat und bestätigen Sie mit „OK“-Button. Wiederholen Sie das für das Verschlüsselungszertifikat.



Outlook Express

In Outlook Express müssen Sie zwingend ein Zertifikat auswählen, bevor Sie die erste Mail digital unterschreiben können, selbst wenn Sie nur ein einziges Zertifikat haben. Daher finden Sie die Anleitung dazu beim Punkt „Digitale Unterschrift mit Outlook“ auf Seite 32.

Zertifikat ins Adressbuch importieren

Ein Zertifikat, das Sie als Datei erhalten haben, muss erst in das Adressbuch importiert werden, bevor Sie damit E-Mails verschlüsseln können.

Klicken Sie dazu auf das Buch-Symbol („Adressen“) in der Navigations-Leiste oder wählen Sie den Menüpunkt „Extras/Adressbuch“.

Öffnen Sie einen Adressbucheintrag durch einen Doppelklick auf eine Adresse oder klicken Sie auf den „Eigenschaften“-Button in der Navigations-Leiste (Menüpunkt „Datei/Eigenschaften“), nachdem Sie eine Adresse im Adressbuch markiert haben. Wenn Sie eine neue Adresse eingeben wollen, klicken Sie auf „Neu“.

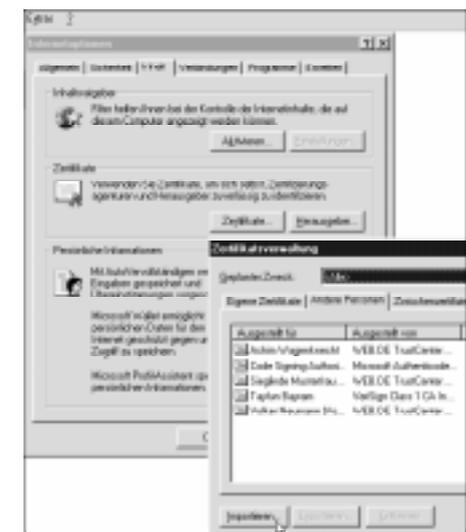
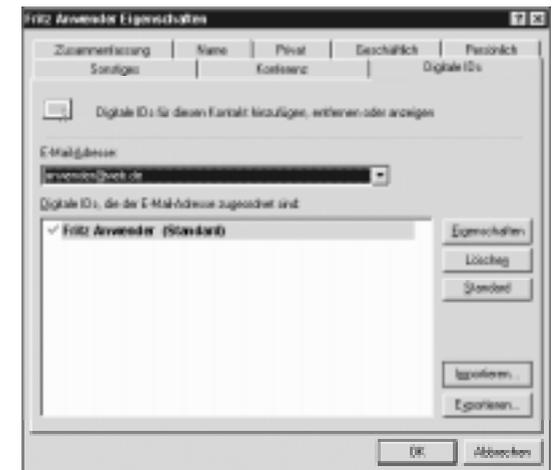
Wählen Sie den Reiter „Digitale IDs“. Klicken Sie auf „Importieren...“. Es kann vorkommen, dass das Format der Zertifikatsdatei nicht erkannt wird. In dem Fall müssen Sie sich vom Inhaber des Zertifikats eine digital unterschriebene Mail zuschicken lassen und das Zertifikat dieser Mail entnehmen (siehe Seite 34).

Outlook Express

Alternativ dazu können Sie in Outlook Express den Menüpunkt „Extras/Optionen“ aufrufen. Wählen Sie dann den Reiter „Sicherheit“ und klicken Sie auf „Digitale IDs“. Wählen Sie „Andere Personen“ und klicken Sie auf „Importieren...“

Sie können Zertifikate auch über die Zertifikatsverwaltung im Internet Explorer (ab Version 5) importieren. Gehen Sie in den Menüpunkt „Extras/Internetoptionen“. Wählen Sie den Reiter „Inhalt“ und klicken Sie auf „Zertifikate“. Wählen Sie „Andere Personen“ und klicken Sie auf „Importieren...“

Es erscheint der „Importassistent für die Zertifikatsverwaltung, den Sie schon von Seite 32 kennen.



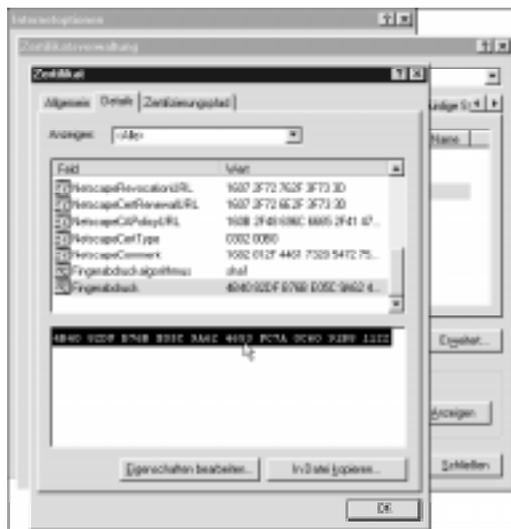
Zertifikat löschen

Eigene Zertifikate können aus dem Zertifikatsspeicher des Microsoft Internet-Explorers erst ab Version 5.0 gelöscht werden. Wählen Sie dazu das zu löschende Zertifikat per Mausklick aus und klicken Sie auf den Button „Entfernen“.

Lesen Sie die folgenden Sicherheitshinweise aufmerksam durch und bestätigen Sie das endgültige Löschen des Zertifikats.

Prüfen, ob ein Zertifikat noch gilt

Auf der TrustCenter-Homepage finden Sie die Funktion „Online-Check“. Hier kann jede und jeder anhand von Seriennummer oder Fingerabdruck ein WED.DE TrustCenter Zertifikat überprüfen. Und So wird's gemacht:



Klicken Sie im Menü „Ansicht“ (beim Internet-Explorer 5.0 das Menü „Extras“ anklicken) auf „Internetoptionen“.

Klicken Sie auf den Karteikartenreiter „Inhalt“. Klicken Sie bei den Zertifikaten auf „Andere“. Markieren Sie das Zertifikat zur Identifikation und klicken Sie anschließend auf „Zertifikat anzeigen“.

Wählen Sie bei den Zertifikatseigenschaften den Punkt „Fingerabdruck“ aus und kopieren Sie den digitalen Code im rechten Fenster in die Zwischenablage (setzen Sie den Mauszeiger an die erste Stelle des Fingerabdrucks und ziehen Sie anschließend den Mauszeiger bei gedrückter linken Maustaste bis an die letzte Stelle. Mit der Tastenkombination „STRG + C“ können Sie den Zahlenwust in die Zwischenablage kopieren).

Schließen Sie alle Fenster mit einem Klick auf „OK“. Setzen Sie den Fingerprint durch die Tastenkombination „STRG + V“ in das entsprechende Feld auf der TrustCenter-Homepage ein und klicken Sie auf „Weiter“.



Das Zertifikat wird auf die Gültigkeit geprüft.

Mit Tastenkombination »Strg-V« einfügen!

7. Ganz einfach: FreeMail

Wenn Ihnen die ganzen Anleitungen der letzten Abschnitte zu kompliziert sind, können wir Ihnen eine Alternative anbieten. Alles, was Sie dazu brauchen ist ein ganz normaler Internet-Browser. Wie das geht? Mit FreeMail, unserem kostenlosen Web-basierten E-Mail-Dienst. Für FreeMail brauchen Sie keinen S/MIME-Client, Sie brauchen sich nicht um die Konfiguration zu kümmern, Sie brauchen keinen Schlüssel beantragen und installieren. Das haben wir alles schon für Sie vorbereitet. Sie finden FreeMail unter <http://freemail.web.de>.

Alles, was Sie mitbringen müssen, ist ein Browser und ein kleines bisschen mehr Vertrauen: Denn damit FreeMail so einfach funktioniert, ist es erforderlich, die privaten Schlüssel der FreeMail-Anwender auf unserem Server zu speichern. Dass wir an diesen Server die höchsten Sicherheitsanforderungen stellen, ist klar. Wenn Ihnen das trotzdem zu riskant ist – OK, dann müssen Sie sich eben doch selbst um die ganzen komplizierten Details kümmern.

Oder Sie benutzen FreeMail, um den Umgang mit Zertifikaten, Verschlüsselung und digitaler Unterschrift auf unkomplizierte Weise zu lernen. Sie können Ihre Sicherheit dann schrittweise erhöhen bis hin zum privaten Schlüssel, dessen einziges Exemplar nur Sie besitzen und mit dem Sie die 168-Bit-Triple-DES Verschlüsselung nutzen.

Um bei FreeMail mitzumachen, müssen Sie sich mit einem Registrierungsformular anmelden. Sie bekommen dann eine kostenlose E-Mail-Adresse, die Sie sofort nutzen können. Nach ein paar Tagen erhalten Sie einen Freischaltcode mit der gelben Post. Mit diesem Freischaltcode können Sie Ihren FreeMail-Adresse dauerhaft freigeben. Indem Sie das tun, bestätigen Sie für uns, dass Ihre Postadresse stimmt. Damit ist die Voraussetzung gegeben, Ihnen ein elektronisches Zertifikat unseres TrustCenters auszustellen. Und genau das tun wir auch. Ab diesem Moment können Sie mit FreeMail elektronisch unterschreiben und verschlüsseln. Dabei ist eine Menge Arbeit schon erledigt, um die Sie sich sonst selbst kümmern müssten.

1. Erhöhen der Sicherheit

Einstieg: FreeMail arbeitet von vornherein mit starker Verschlüsselung. Sie brauchen dafür nichts zu installieren. Auf dem Weg zwischen Ihren Mail-Partnern und Ihrem Postfach ist die Mail immer optimal geschützt.

Erhöhte Sicherheit: Wenn Sie FreeMail „ohne alles“ benutzen, werden Kennwörter und Mails zwischen Ihrem Postfach auf unserem Server und Ihrem Computer im Klartext übertragen. Diese kleine Sicherheitslücke können Sie schließen, indem Sie unseren Sichereren Server benutzen. Damit die Daten zwischen diesem Sichereren Server und Ihrem Computer mit erhöhter Sicherheit verschlüsselt werden, müssen Sie gegebenenfalls das



entsprechende Sicherheitspatch installieren. Wie das geht, lesen Sie für Netscape *ab Seite 16* und für Microsoft *ab Seite 27*.

2. WEB.DE-Zertifikate installieren

Einstieg: Sie können FreeMail ganz einfach benutzen, ohne unsere Zertifikate zu installieren.

Erhöhte Sicherheit: Um unseren Sicheren Server zu benutzen, müssen Sie entweder unser Zertifikat für FreeMail oder das Site-Zertifikat für diesen Server installieren. Wie das funktioniert, lesen Sie für Netscape *ab Seite 16* und für Microsoft *ab Seite 27*.

3. Eigene Zertifikate beantragen

Alle Daten, die wir dazu brauchen, sind schon in Ihrer FreeMail-Registrierung enthalten. Das Zertifikat bekommen Sie automatisch dazu.

4. Zertifikate sichern, exportieren und importieren

Um die Datensicherheit kümmern wir uns. Wir machen täglich Sicherheitskopien und halten uns streng an einen ausgeklügelten Sicherheitsplan. Zertifikate importieren: Wenn eine unterschriebene Mail bei Ihrer FreeMail-Adresse ankommt, wird das Zertifikat automatisch gespeichert. Sie können ab sofort verschlüsselte Mails an den Inhaber dieses Zertifikates senden.

5. Unterschreiben

Wenn Sie einen Mausklick ausführen können, dann können Sie auch mit FreeMail digital unterschreiben. Sie müssen nur die entsprechende Option ankreuzen, entweder beim Schreiben  einer einzelnen Mail oder bei den Optionen  für alle Mails.

6. Verschlüsseln

Um eine Mail verschlüsseln zu können, brauchen Sie das Zertifikat des Empfängers. Lassen Sie sich vom Adressaten eine unterschriebene Mail zuschicken. Sobald diese Mail in Ihrem FreeMail-Postfach angekommen ist, können Sie verschlüsselt antworten. Umgekehrt funktioniert das genauso: Sie schicken eine unterschriebene Mail, Ihr Gegenüber kann verschlüsselt antworten.



7. Wie sieht eine an mich verschlüsselte oder unterschriebene Mail aus?

Wenn Sie eine verschlüsselte Mail erhalten, wird das in der Mail mit einem Symbol angezeigt. Das Entschlüsseln erledigt unser Server für Sie. Das gleiche gilt für digital unterschriebene Mails: Der Server prüft die Unterschrift für Sie und zeigt mit einem Symbol an, dass das geschehen ist. Mit einem Klick auf die jeweiligen Symbole können Sie zusätzliche Informationen einsehen.

Zertifikate sind digital fest mit den Benutzerdaten verbunden. Das ergibt sich

8. Zertifikate erneuern und widerrufen

logisch aus dem Sinn der Zertifikate: Es soll ja garantiert werden, dass diese Benutzerdaten stimmen. Deshalb müssen Zertifikate manchmal widerrufen oder erneuert werden, weil Ihre Adresse oder E-Mail-Adresse sich geändert haben. Auch wenn Ihr geheimer Schlüssel verloren oder offengelegt ist, müssen Sie Ihr Zertifikat widerrufen. Außerdem gelten Zertifikate genau wie ein Personalausweis nur für begrenzte Zeit. Nach dieser Zeit müssen Sie das Zertifikat erneuern, wenn Sie es weiterhin benutzen wollen. Hierbei muss man zwei Fälle unterscheiden, je nachdem, ob das vorläufige Testzertifikat mit einer Gültigkeitsdauer von 30 Tagen oder das 1 Jahr gültige WEB.DE Zertifikat ausläuft.

Das vorläufige Testzertifikat erneuern

Eine Woche vor Ablauf des vorläufigen Zertifikates erhalten Sie vom WEB.DE TrustCenter eine Erinnerungsmail. Sie sollten spätestens dann den Activator-Key, den wir Ihnen per gelber Post zugeschickt haben, eingeben.

Mit der Eingabe des Activator-Keys ist schließen Sie die Überprüfung Ihrer Anschrift ab und Sie können 1 Jahr gültige Zertifikate ausstellen lassen. Im nächsten Schritt können Sie dann sofort Ihr 1 Jahr gültiges Zertifikat beantragen.

Das 1 Jahr gültige WEB.DE Zertifikat erneuern

Etwa 30 Tage vor Ablauf Ihres ein Jahr gültigen Zertifikates werden Sie vom TrustCenter informiert. Sie haben dann die Möglichkeit, im TrustCenter unter dem Punkt „Zertifikate verwalten“ das Zertifikat zu erneuern.

Bitte beachten: Diese Funktion steht erst einen Monat vor Ablauf des Zertifikates zur Verfügung.

Wählen Sie auf der Übersichtsseite „Zertifikate verwalten“ durch ein Klick auf die E-Mail-Adresse das Zertifikat aus, das erneuert werden soll.

Klicken Sie auf den Punkt „Erneuern“.

Folgen Sie dann den Anweisungen des WEB.DE-TrustCenters.

Zertifikate widerrufen

Ein Zertifikat ist zu widerrufen, wenn der zugehörige private Schlüssel verloren, gestohlen, offengelegt oder sonstwie abhanden gekommen ist.

Ebenfalls ist das Zertifikat zu widerrufen, wenn sich die dazugehörige E-Mail-Adresse oder die Postadresse geändert hat.

Sobald das Zertifikat widerrufen wurde, wird es in die Liste der nicht mehr gültigen Zertifikate des WEB.DE-TrustCenters aufgenommen.

Verbinden Sie sich mit dem WEB.DE-TrustCenter und wählen Sie dort „Zertifikate verwalten“. Klicken Sie das Zertifikat an, das Sie widerrufen wollen. Klicken Sie auf den Punkt „Widerrufen“. Das Zertifikat wird auf der Übersichtsseite als widerrufen gekennzeichnet.

9. Hotline

Fragen und Antworten aus unserer Benutzerberatung

? Netscape stürzt beim Empfangen unterschriebener Mails ab. Was tun?

! Das ist ein Programmfehler in Netscape, der nicht nur unser TrustCenter betrifft. Installieren Sie die WEB.DE-Root-Zertifikate, um diesen Fehler zu beheben. Wenn die Zertifikate schon vorhanden sind, aktivieren Sie sie wie folgt: Rufen Sie die Sicherheitsseite auf und klicken Sie unter „Zertifikate“ auf „Untersigner“. Wählen Sie das WEB.DE-Zertifikat aus der Liste und klicken Sie auf „Bearbeiten“. Schalten Sie im folgenden Fenster mindestens die Option zum Beglaubigen von E-Mail ein.

? Mein vorläufiges Zertifikat ist trotz Eingabe des Activator Keys abgelaufen. Wie kann ich es weiter nutzen?

! Das vorläufige Zertifikat wird nicht verlängert, sondern durch ein einjähriges ersetzt. Mails, die mit dem vorläufigen Zertifikat verschlüsselt wurden, können Sie aber weiterhin lesen.

? Nach einem Festplatten-Crash wollte ich die sicherheitshalber exportierten Schlüssel wieder importieren. Mir fiel dabei auf, dass ich dummerweise nicht meine „eigenen Zertifikate“ exportiert hatte. Wie kann ich meine eigenen Zertifikate wieder bekommen? Ich weiß noch alle Kennwörter und kann ich mich auch bei trust.web.de einloggen.

! Tut uns leid. In dem Fall sind Ihre privaten Schlüssel verloren. Wir haben keine Kopie Ihrer privaten Schlüssel und wir hatten auch nie eine. Sie müssen Ihr Zertifikat widerrufen und ein neues beantragen. Wenn Sie solchen Problemen künftig aus dem Weg gehen wollen, können Sie FreeMail benutzen. Dann kümmern wir uns um Ihren privaten Schlüssel. Das Sicherheitskonzept des TrustCenters sieht jedoch vor, dass nur Sie Ihren privaten Schlüssel besitzen und Sicherheitskopien davon anfertigen können.

? Ich versuche mich beim TrustCenter einzuwählen.

Den Activator Key habe ich per Post erhalten. Aber wie lautet mein Passwort?

! Das Passwort haben Sie sich bei der Registrierung selbst ausgesucht. In dem Brief mit dem Activator Key steht dieses Passwort nicht. So ist sicher, dass nur Sie den Account freischalten können, selbst wenn der Brief abgefangen werden sollte. Rufen Sie unsere Hotline an, um das weitere Vorgehen zu klären.

? Ich möchte das Zertifikat sowohl am Arbeitsplatz als auch privat nutzen. Geht das?

! Das Zertifikat gilt nur für genau eine E-Mail-Adresse. Wenn Sie zu Hause und in der Firma die gleiche E-Mail-Adresse haben, können Sie das Zertifikat an beiden Rechnern nutzen. Haben Sie verschiedene Mail-Adressen, brauchen Sie für jede ein eigenes Zertifikat.

? Wenn ich die Adresse zum Aktivieren meines Zertifikates eingebe, meldet Ihr Server immer: „Aufruf der Seite ohne Key-Parameter“.

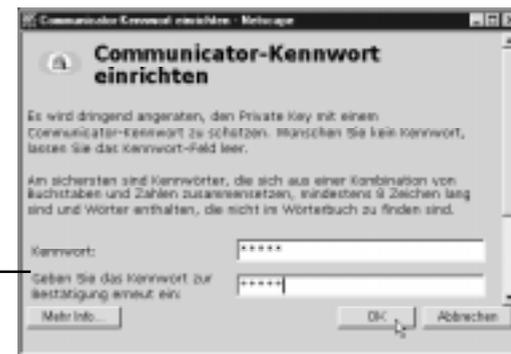
Was mache ich falsch?

! Ihr Freischalt-Schlüssel ist hinter dem Fragezeichen als fester Bestandteil in der Adresse enthalten. Am besten klicken Sie die Adresse einfach in der Mail an. So vermeiden Sie Eingabefehler. Wenn Sie die Adresse trotzdem abtippen wollen, achten Sie darauf, an keiner Stelle ein Leerzeichen zu tippen und die komplette Adresse inklusive ?key= usw. einzugeben.

```
https://trust.web.de/pickup/?key=R6Mzc5Pgzre5yk4
```

? Nachdem ich meinen Activator-Key eingegeben hatte, wollte ich mir ein Zertifikat für ein Jahr ausstellen lassen. Dabei wollte Netscape einen Private-Key erstellen. Ich drückte also auf „Weiter“. Danach gab Netscape folgende Nachricht aus: „Bitte geben Sie das Kennwort bzw. Kennnummer ein für Communicator Certificate DB“. Leider weiß ich dieses Kennwort nicht. Können Sie mir vielleicht weiter helfen?

! Die „Communicator Certificate DB“ ist die Datenbank, in der Netscape die Zertifikate speichert. Wenn man zum ersten Mal auf diese Datenbank zugreift, fragt Netscape, ob man die Datenbank mit einem Kennwort schützen will. Manchmal kommt es vor, daß man bei so einer Abfrage einfach irgendwas eingibt, nur damit es weitergeht. Das ist aber in dem Fall ein fataler Fehler. Sie können nämlich später weder private Schlüssel erzeugen noch exportieren, wenn Sie sich nicht mehr an das Passwort erinnern. In dem Fall können wir auch nicht weiterhelfen. Zur Erinnerung: Das Fenster, in dem Sie das Passwort eingegeben haben, sah so aus:



Einzige Lösung: Sie deinstallieren Netscape komplett und installieren es neu. Alle Zertifikate, die Sie bisher in Netscape gespeichert hatten, gehen dabei allerdings verloren.

? Ich benutze zwei verschiedene E-Mail-Adressen, eine zum Empfangen und eine zum Senden. Können Sie mir den Aktivierungsschlüssel für die Sendeadresse an meine Empfangs-Adresse schicken?

! Leider nein. Damit würde unser Sicherheitskonzept untergraben. Eine zertifizierte Mail-Adresse muss zum Senden und Empfangen gleichermaßen geeignet sein.

? Kann ein französischer Staatsbürger sich bei Ihnen nicht anmelden?

Frankreich ist bei Ihnen nicht als Land vorgesehen. Gibt es eine Ausnahme?

Bis vor kurzem war es in Frankreich verboten, starke Verschlüsselung einzusetzen. Daher durften wir unser TrustCenter für Franzosen nicht zugänglich machen. Mit „décret no 99-200 du 17 mars 1999“ wurde die Gesetzgebung bzgl. Verschlüsselung in Frankreich deutlich gelockert. Damit ist es nun auch für französische Staatsbürger legal, Verschlüsselungsverfahren zu privaten Zwecken einzusetzen. Aufgrund dieser Tatsache werden wir bei allernächster Gelegenheit „F“ in unsere Länderliste für FreeMail und das TrustCenter mit aufnehmen.

<http://www.internet.gouv.fr/francais/textesref/criptodecret99200.htm>

? Ich habe mit der Post keinen Activator-Key erhalten bzw. der Key funktioniert nicht, was nun?

! In diesem Fall rufen Sie bitte die Hotline-Nummer des TrustCenters an.

? Ich habe ein Zertifikat beantragt aber keine Mail vom TrustCenter erhalten, was nun?

! Es kann verschiedene Ursachen haben, wenn Sie vom TrustCenter (noch) keine E-Mail erhalten haben:

Je nach Betrieb im Internet kann sich die Zustellung der E-Mail verzögern. Vielleicht ist die Mail noch unterwegs, gedulden Sie sich noch ein wenig.

Eventuell hat sich beim Beantragen des Zertifikates ein Tippfehler in Ihre E-Mailadresse eingeschlichen, so dass deshalb die E-Mail nicht zugestellt werden konnte. Im WEB.DE TrustCenter können Sie sich unter „Zertifikate verwalten“ einen Überblick über Ihre Zertifikate verschaffen. Auch die beantragten Zertifikate sind dort aufgeführt, so dass Sie die E-Mail-Adresse dort überprüfen können.

Haben Sie Ihre E-Mail-Adresse tatsächlich falsch eingetragen, so können Sie einfach für die „richtige“ ein neues Zertifikat beantragen. Das falsch beantragte Zertifikat wird automatisch nach 30 Tagen gelöscht.

Wenn Sie keine E-Mail vom TrustCenter erhalten haben, obwohl Ihr Zertifikatsantrag schon länger zurückliegt und Sie beim Antrag Ihre E-Mail-Adresse auch korrekt eingegeben haben, dann rufen Sie bitte die Hotline-Nummer des TrustCenters an.

? Ich habe ein Zertifikat beantragt aber die Mail vom TrustCenter aus Versehen gelöscht, was nun?

! In diesem Fall rufen Sie bitte die Hotline-Nummer des TrustCenters an.

? Ich kann ein beantragtes Zertifikat nicht beim TrustCenter abholen („Kein Zertifikat vorhanden“), was nun?

! Ihr Zertifikat steht, nachdem Sie es beantragt haben, 30 Tage zum Aktivieren bereit. Danach wird es gelöscht. Wenn also seit Ihrem Zertifikatsantrag schon mehr als 30 Tage vergangen sind, so ist Ihr Zertifikat inzwischen wieder gelöscht. Beantragen Sie einfach ein neues.

? Ich habe beim Zertifikatsantrag eine falsche E-Mail-Adresse eingegeben (Tippfehler), was nun?

! Sie können einfach für die korrekte E-Mail-Adresse ein neues Zertifikat beantragen. Das falsch beantragte Zertifikat wird automatisch nach 30 Tagen gelöscht.

? Wie bekomme ich das Zertifikat einer Person, der ich eine verschlüsselte Nachricht schicken will?

! Die einfachste Möglichkeit ist, sich von dieser Person eine digital unterschriebene E-Mail zusenden zu lassen. Das darin enthaltene Zertifikat können Sie dann zum Verschieken verschlüsselter Nachrichten benutzen. Der Netscape Messenger speichert die Zertifikate automatisch ab, bei Outlook müssen Sie das Zertifikat selber im Adressbuch abspeichern.

? Kann ich eine digital unterschriebene Nachricht an jemanden senden, dessen E-Mailprogramm den S/MIME-Standard nicht unterstützt?

! Ja, aber der Empfänger kann Ihre digitale Unterschrift nicht lesen und kann daher nicht nachprüfen, ob die Nachricht tatsächlich von Ihnen stammt und ob sie unterwegs verändert wurde.

? Kann ich eine verschlüsselte Nachricht an jemanden senden, der kein eigenes E-Mail-Zertifikat besitzt?

! Nein, Sie benötigen den öffentlichen Schlüssel des Empfängers, um eine E-Mail verschlüsseln zu können. Voraussetzung dafür ist ein Zertifikat.

? Ich habe eine neue E-Mail-Adresse. Kann ich mit ihr mein Zertifikat aktualisieren?

! Nein, dies ist leider nicht möglich! Das Zertifikat wurde speziell für die damit verknüpfte E-Mail-Adresse erstellt. Wenn Sie Ihre Mail-Adresse ändern, müssen Sie sich ein neues Zertifikat für diese neue Adresse holen.

? Ich bin umgezogen oder mein Familienname hat sich geändert. Kann ich die Informationen innerhalb meines Zertifikates aktualisieren?

! Nein, dies ist leider nicht möglich! Das Zertifikat wurde speziell mit den bei der Anmeldung angegebenen Daten erstellt. Wenn sich hier etwas ändert, müssen Sie sich ein neues Zertifikat mit den neuen Daten holen.

? Ich habe einen neuen Computer. Kann ich mein bisheriges Zertifikat dorthin übertragen?

! Bitte lesen Sie hierzu die Abschnitte zu „Sichern und Übertragen von Zertifikaten“.

? Wenn ich meinen Rechner ausschalte oder das Internet verlasse, wird dadurch mein Zertifikat gelöscht?

! Nein. Ihr Zertifikat, d. h. Ihr öffentlicher und privater Schlüssel, sind Dateien, die sich auf der Festplatte Ihres Rechners befinden und weder durch Unterbrechen der Stromzufuhr, noch durch Unterbrechen der Internetverbindung beeinträchtigt werden.

10. Ausblick

Sie haben jetzt das WEB.DE-TrustCenter kennen gelernt und (hoffentlich) den Einstieg in die sichere Kommunikation per Internet gefunden. Wie wird es weitergehen?

Es werden mehr Programme S/MIME unterstützen, so dass Sie das TrustCenter damit benutzen können. Damit werden immer mehr Menschen Zugang zu sicherer E-Mail bekommen. Unsere Zertifikate werden in mehr Programme vorinstalliert werden, so dass Sie das nicht mehr selbst nachholen müssen.

Aber wir wollen auch die gesamte Entwicklung nicht aus dem Auge verlieren.

Schon seit es E-Mail gibt, werden damit trotz aller Sicherheitsmängel vertrauliche Mitteilungen ausgetauscht. Wie viel Schaden dabei durch Betrug und Spionage entstanden ist, weiß niemand. Es ist an der Zeit, ein umfassendes Sicherheitskonzept für das Internet zu entwickeln und praktisch umzusetzen. Mit S/MIME steht das Werkzeug dafür zur Verfügung.

Eine Infrastruktur für sichere Kommunikation im Internet entsteht gerade. Wir leisten unseren Beitrag dazu mit dem WEB.DE-TrustCenter. In wenigen Jahren wird es völlig selbstverständlich sein, ein E-Mail Zertifikat zu haben und damit Mails zu unterschreiben und zu verschlüsseln.

Noch ist die rechtliche Bedeutung digitaler Unterschriften unklar. Das Signaturgesetz regelt zwar die technischen Rahmenbedingungen, aber vor Gericht sind digitale Signaturen als Urkundenbeweis nicht zulässig. Wir gehen davon aus, dass sich das in einigen Jahren ändern wird.

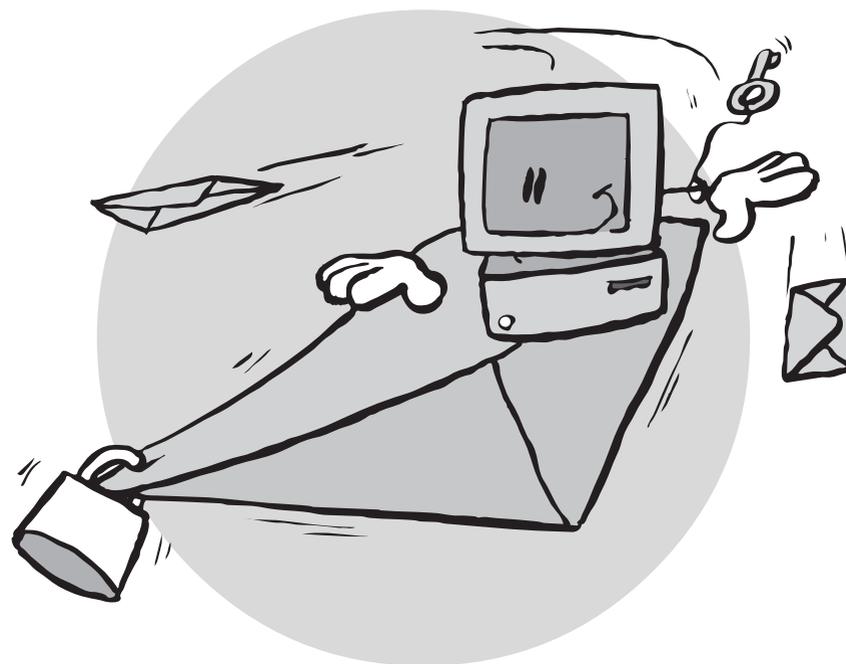
Die digitale Signatur schafft mehr Verbindlichkeit im Internet. Einen rechtsgültigen Vertrag können Sie zwar auch mit unverschlüsselter Mail abschließen. Aber im Streitfall kommen Sie in Beweisnot.

Wir glauben, dass digitale Signaturen dem Handel im Internet Auftrieb geben werden. Gerade kleine Händler, für die eine einzige gefälschte Bestellung schon problematisch ist, können mit zertifizierten Mails sichere Geschäfte abschließen. Aber auch privat profitieren Sie von Zertifikaten. E-Mails werden einfach verbindlicher. Belästigungen durch anonyme oder gefälschte Mails werden immer weniger werden.

Sichere Verschlüsselung wird von Staatsschützern immer wieder als Risiko für die Sicherheit des Staates angesehen. Die amerikanische Gesetzgebung verbietet daher immer noch den Export starker Verschlüsselungstechnik. Wir gehen davon aus, dass E-Mail-Programme aus anderen Ländern diese Lücke schließen werden. Das australische Programm Fortify für Netscape ist ein Beispiel dafür. Wir nehmen an, dass die starke Verschlüsselung für jedermann und jedefrau sich durchsetzen wird. Denn nur so ist es möglich, das Grundrecht auf Briefgeheimnis wahrzunehmen. In Deutschland sind die Initiativen für ein Verschlüsselungsverbot bis auf weiteres vom Tisch. Auch in anderen Ländern lockern sich die Vorschriften. So ist es in Frankreich seit März 1999 erlaubt, starke Verschlüsselung für private Zwecke zu nutzen. Wir gehen davon aus, dass sich dieser Trend durchsetzen wird, denn Verschlüsselungsverbote sind letztlich sinnlos:

wirkliche Verbrecher weichen auf illegale Methoden aus, und ehrliche Bürger können ihre Privatsphäre nicht schützen.

Die Umsetzung von S/MIME steckt noch in den Anfängen. Die Erfahrungen mit der Einführung unseres TrustCenters zeigen uns, dass die Technik noch viel zu kompliziert ist. Wir werden weiterhin unser möglichstes tun, um den Zugang zu sicherer E-Mail zu vereinfachen, ohne dabei auf Sicherheit zu verzichten.



Anhang II

Allgemeine Geschäftsbedingungen für das TrustCenter von WEB.DE

I. Allgemeines

1. Unsere Leistungen und Angebote erfolgen ausschließlich aufgrund dieser Geschäftsbedingungen.
2. Anders lautende Geschäftsbedingungen oder Abweichungen von den getroffenen Vereinbarungen im Bestätigungsschreiben des Kunden werden nur wirksam, wenn wir ihnen schriftlich zustimmen.
3. Ergänzungen oder Änderungen sowie Nebenabreden bedürfen zu ihrer Wirksamkeit unserer schriftlichen Bestätigung. Der Schriftform wird auch in der Form der telekommunikativen Übermittlung genügt.
4. Es gilt das formelle und materielle Recht der Bundesrepublik Deutschland.
5. Sollten einzelne Bestimmungen dieser Bedingungen unwirksam sein oder werden, so hat dies auf die Rechtswirksamkeit der übrigen Punkte keinen Einfluss. Die unwirksamen Bestimmungen müssen so umgedeutet werden, dass ihr Zweck in wirksamer Weise erfüllt werden kann.

II. Leistungen

Die nachfolgenden Dienstleistungen werden vom WEB.DE-TrustCenter als Zertifizierungsstelle angeboten.

2.1. Zertifizierung öffentlicher Schlüssel

1. Das WEB.DE-TrustCenter nimmt die Zertifizierung von öffentlichen Schlüsseln gemäß den Richtlinien des WEB.DE-TrustCenters vor.
2. Es werden nur öffentliche Schlüssel von natürlichen Personen zertifiziert. Durch die Zertifizierung bestätigt das WEB.DE-TrustCenter, die Zuordnung des Zertifikates zu der darin genannten natürlichen Person anhand der zugrundeliegenden Richtlinien durchgeführt zu haben.
3. Mit der Beantragung eines Zertifikates erklärt sich der Privatkunde damit einverstanden, dass ihm ein Zertifikat gemäß dem in Ziffer 2 dieser Allgemeinen Geschäftsbedingungen dargestellten Verfahren ausgestellt wird, das in das Zertifikatsverzeichnis vom WEB.DE-TrustCenter eingetragen und damit öffentlich zugänglich gemacht wird.
4. Ein Anspruch auf die Zertifizierung durch das WEB.DE-TrustCenter besteht nicht.
5. Eine Zertifizierung kann erst vorgenommen werden, wenn alle erforderlichen Daten vorliegen.
6. Ein Zertifikat enthält je nach Grad der Identifizierung verschiedene Angaben zum Eigentümer, mindestens jedoch die E-Mail-Adresse oder den Namen des Zertifikatinhabers.

Anhang I

Die Fingerprints des WEB.DE Trustcenters

Der Fingerprint ist genauso wie der Fingerabdruck Ihres Daumens ein weltweit einmaliges, zur eindeutigen Identifikation geeignetes Zeichen. Fingerprints sind ein Extrakt des Zertifikats, das dieses durch wenige Zeichen eindeutig identifiziert, ohne dass Sie den gesamten Schlüssel abgleichen müssen. Es ist übrigens keine schlechte Idee, Ihren eigenen Fingerprint auf Visitenkarten und Briefköpfen abzudrucken.

WEB.DE Root-Zertifikat (4096 Bits)

MD5: BD:D4:F5:1A:7D:70:46:50:DB:6F:4D:68:41:83:99:93

SHA1: 42:82:EA:8C:F2:3E:DD:56:37:D7:D0:11:93:AD:F7:10:95:2C:57:4A

WEB.DE CA-Zertifikat (2048 Bits)

MD5: D9:B2:BC:51:3C:CC:8B:5B:7C:3D:D1:2D:BD:63:43:04

SHA1: B5:11:E1:C0:0A:BB:AA:DF:9D:70:30:A7:56:59:3D:D8:52:5A:2D:FB

WEB.DE TrialCA-Zertifikat (2048 Bits)

MD5: 0B:D6:22:50:4C:74:77:61:87:0F:AD:BB:D0:2D:14:70

SHA1: 93:7D:AA:D1:5A:C8:4E:C3:C6:8F:BD:6F:4D:A9:5A:EA:B3:8B:03:E1

WEB.DE Zertifikat Cinetic Medientechnik GmbH (1024 Bits)

MD5: 5F:E4:D3:A6:7A:A6:CF:E7:5D:AC:AC:10:AC:2E:56:13

SHA1: 7E:CD:E8:38:95:8E:8C:2B:2A:EA:F1:7C:69:3A:7C:87:EF:6A:4A:B5

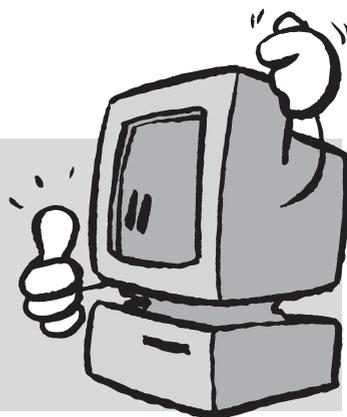
Sie können zur Überprüfung der Fingerprints auch gerne bei uns anrufen.

Sie erreichen uns unter Telefon: 0721/9432936. Dieses Telefon ist Montag-Freitag zwischen 9.00 und 17.00 Uhr besetzt.

Hinweis

Stand der in diesem Handbuch abgedruckten Fingerprints, Allgemeinen Geschäftsbedingungen und Zertifizierungsrichtlinien ist **Juli 1999**.

Über aktuelle Ergänzungen und Änderungen können Sie sich jederzeit unter <http://trust.web.de/Hilfe> informieren.



7. Das Zertifikat ist lediglich für ein Jahr gültig. Diese Dauer kann auf Antrag um ein weiteres Jahr verlängert werden. Das WEB.DE-TrustCenter hat das Recht, die Verlängerung des Zertifikates aus Sicherheitsgründen von einer erneuten Identitätsfeststellung oder einem neuen Zertifikatsantrag abhängig zu machen, um geänderten Sicherheitsanforderungen gerecht werden zu können.

2.2. Umfang der Zertifizierung

1. Bei der Zertifizierung prüft das WEB.DE-TrustCenter

1.a. bei der Ausstellung eines vorläufige Zertifikats lediglich, ob der Antragsteller unter der angegebenen E-Mail-Adresse zu erreichen ist und

1.b. beim Voll-Account zusätzlich zu a. ob die angegebene Postanschrift mittels gelber Post erreichbar ist.

2. Diese Angaben werden vom WEB.DE-TrustCenter nur bei der Zertifikatsausstellung überprüft. Eine Zusicherung der Aktualität dieser Daten wird vom TrustCenter daher nicht gegeben.

2.3 Abfragen von Zertifikaten

1. Jedermann kann im Zertifikatsverzeichnis die Gültigkeit einzelner Zertifikate überprüfen.

2. Das WEB.DE-TrustCenter sichert dem Zertifikatinhaber zu, dass sein Zertifikat bis zum Ende des Gültigkeitsdatums über das Zertifikatsverzeichnis abgefragt werden kann.

3. Jeder Zertifikatinhaber kann die Gültigkeit seines im Zertifikatsverzeichnis eingetragenen Zertifikates widerrufen. Diese Änderung wird dann vom WEB.DE-TrustCenter so schnell wie möglich in das Zertifikatsverzeichnis eingetragen.

4. Für ungültig erklärte Zertifikate werden vom WEB.DE-TrustCenter ebenfalls über das Zertifikatsverzeichnis öffentlich zur Verfügung gestellt.

5. Gibt es für das WEB.DE-TrustCenter Hinweise auf eine Verletzung der Vertraulichkeit des Zertifikates, wie sie aus einer Missachtung der Sorgfalts- und Mitwirkungspflichten gemäß Ziffer 3 dieser Allgemeinen Geschäftsbedingungen resultieren kann, so behält sich das WEB.DE-TrustCenter im Interesse des Kunden vor, dieses Zertifikat vorübergehend bis zu einer Klärung zu sperren.

6. Ebenso erfolgt eine Sperrung gemäß Ziffer 2.3.5. dieser Allgemeinen Geschäftsbedingungen, wenn der Zertifikatinhaber den Verdacht eines Verlustes seines privaten Schlüssels oder dessen Nutzung durch Dritte hat.

III. Sorgfalts- und Mitwirkungspflichten des Zertifikatinhabers

Diese folgenden Mitwirkungspflichten sind wesentliche Vertragspflichten des Kunden.

1. Der private Schlüssel und Kopien des privaten Schlüssels auf Datenträgern sind in persönlichem Gewahrsam zu halten. Bei deren Verlust ist unverzüglich die Sperrung des Zertifikates zu veranlassen. Wird ein Datenträger mit dem privaten Schlüssel nicht mehr benötigt, ist er unbrauchbar zu machen und die Sperrung des Zertifikates zu veranlassen, falls es nicht abgelaufen ist.

2. Persönliche Identifikationsnummern oder Passwörter zur Identifikation gegenüber dem Datenträger mit dem privaten Schlüssel sind geheim zu halten. Sie dürfen insbesondere nicht auf dem zugehörigen Datenträger vermerkt oder auf andere Weise zusammen mit diesem aufbewahrt werden. Bei Preisgabe oder Verdacht der Preisgabe dieser Identifikationsdaten ist unverzüglich eine Änderung vorzunehmen.

3. Es ist sicherzustellen, dass sich auf den verwendeten Geräten keine Viren oder schädigende Software befinden, die zu einer Preisgabe der Identifikationsdaten oder der geheimen Schlüssel führen können, oder den Signier- oder Signaturprüfvorgang verfälschen können.

4. Es ist zu beachten, dass es für eine optimale Sicherheit bei der Überprüfung digitaler Signaturen unerlässlich ist, in dem Zertifikatsverzeichnis beim WEB.DE-TrustCenter festzustellen, ob die Signaturschlüssel-Zertifikate gültig und nicht gesperrt sind.

IV. Rücktritt

1. Das WEB.DE-TrustCenter behält sich vor, durch schriftliche Erklärung von dem Vertrag zurückzutreten, wenn die gemachten Angaben nicht mit den bei der Identitätsfeststellung erlangten Daten übereinstimmen. Dieses Rücktrittsrecht gilt auch nach der Identitätsfeststellung durch das TrustCenter.

2. Die Gründe, die zu dem Rücktritt vom TrustCenter führten, werden dem Kunden mitgeteilt, so dass dieser die Möglichkeit zu deren Behebung hat.

3. Sollten dem Kunden hierdurch Kosten entstanden sein, hat er diese selbst zu tragen.

V. Kosten

Alle vom TrustCenter aufgrund dieser Allgemeinen Geschäftsbedingungen erbrachten Leistungen sind kostenlos.

VI. Haftung

1. Nicht ausdrücklich in diesen Bedingungen zugestandene Ansprüche, insbesondere Schadensersatzansprüche aus Unmöglichkeit, Verzug, Verletzung von vertraglichen Nebenpflichten, Verschulden bei Vertragsabschluss, unerlaubter Handlung oder aus sonstigen Rechtsgründen – auch soweit solche Ansprüche im Zusammenhang mit Gewährleistungsrechten des Kunden stehen – sind ausgeschlossen, wenn nicht das WEB.DE-TrustCenter in Fällen des Vorsatzes und bei grober Fahrlässigkeit haftet.

2. Das WEB.DE-TrustCenter haftet nicht für die Handlungen der Zertifikatinhaber oder Dritter, die unbefugt über ein Zertifikat verfügen, für ihre Geschäftsfähigkeit, ihre Zahlungsfähigkeit oder für die Gültigkeit der unter Verwendung dieser Schlüssel abgeschlossenen Geschäfte.

3. Das WEB.DE-TrustCenter haftet nicht für technische Ausfälle oder die Unerreichbarkeit des Zertifikatsverzeichnisses oder einzelner Zertifikate sowie für Ausfälle, die außerhalb des Einflussbereiches des TrustCenters liegen.

4. Das WEB.DE-TrustCenter übernimmt keinerlei Haftung für die Sicherheit der von den Kunden verwendeten Public-Key-Sicherheitssysteme.

Anhang III

Zertifizierungsrichtlinien des WEB.DE-TrustCenters

Identität des WEB.DE TrustCenters

WEB.DE AG
 Amalienbadstr. 41
 76227 Karlsruhe
 Telefon: 0721/94329-0
 Telefax: 0721/94329-22
 E-Mail: trust@web.de

Welche Zertifikate stellt das WEB.DE-TrustCenter aus?

Das WEB.DE TrustCenter stellt Zertifikate nach dem X.509-Standard aus.

X.509-Zertifikate können in vielen Browsern oder populären E-Mail-Programmen für die integrierte E-Mail-Verschlüsselung (S/MIME) verwendet werden.

X.509 ist ein Standardformat der ITU-T für Zertifikate (International Telecommunications Union-Telecommunication).

Es enthält den Namen und die digitale Signatur des Ausstellers und Angaben über die Identität des Inhabers.

Auf dem X.509-Format basieren die verwendeten Verfahren S/MIME und SSL.

Das WEB.DE TrustCenter unterscheidet bei X.509-Zertifikaten zwei Klassen:

1. Vorläufige Zertifikate, 30 Tage gültig
2. Vollzertifikate, 1 Jahr gültig

Rechtliche Bedeutung

1. Eine Zertifizierung durch das WEB.DE-TrustCenter zieht keinerlei rechtliche Implikationen nach sich.
2. Ein gesetzlicher Anspruch auf die Erteilung eines Zertifikates besteht grundsätzlich nicht.
3. Insbesondere ist die rechtliche Relevanz digitaler Signaturen derzeit allgemein nicht definiert.
4. Der Sinn eines WEB.DE-TrustCenter-Zertifikates liegt daher in der Schaffung der technischen Voraussetzungen für eine gesicherte elektronische Kommunikation, insbesondere im Hinblick auf zukünftige Entwicklungen.

Sicherheitsanforderungen an das WEB.DE-TrustCenter

Folgende Sicherheitsanforderungen an eine Certification Authority (im folgenden CA genannt) erfüllt das WEB.DE TrustCenter:

1. Für die Dienste der CA wird ein Rechner eingesetzt, der vor missbräuchlicher Benutzung geschützt ist.

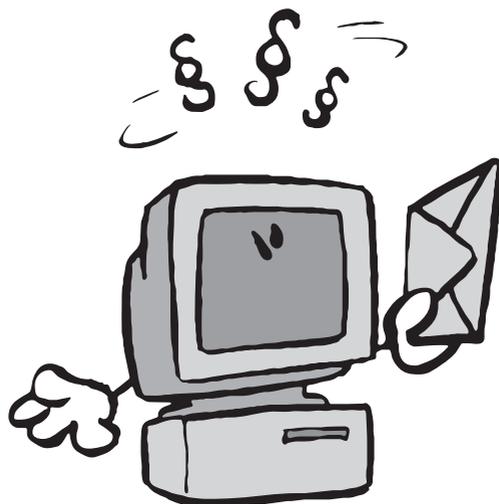
Ein unbefugter Zugriff auf den CA-Rechner und gespeicherte Schlüsseldaten ist durch den Einsatz geeigneter Hard- und Software unterbunden.

5. Der Kunde hat etwaige Schäden oder Verluste, die ihn zu Schadensersatzforderungen berechtigen, unverzüglich schriftlich mitzuteilen.

VII. Datenweitergabe

1. Das Zertifikatverzeichnis vom WEB.DE-TrustCenter übermittelt die im Zertifikat angegebenen Daten automationsunterstützt alle, die danach anfragen. Diese Übermittlung erfolgt in alle Staaten der Welt.
2. Das WEB.DE-TrustCenter wird nur die persönlichen Daten erheben, verarbeiten und nutzen, die zum Betreiben einer Zertifizierungsstelle erforderlich sind.
3. Das WEB.DE-TrustCenter verpflichtet sich, alle personenbezogenen Daten vor unbefugtem Zugriff sicher zu verwahren. Weitergegeben werden solche Daten vom TrustCenter nur auf gerichtliche Anordnung.
4. Eine weitere, kommerzielle Nutzung der durch einen Antrag auf Zertifizierung erhaltenen Daten findet seitens des WEB.DE-TrustCenters nicht statt. Daten, die während des Antrags- und Identitätsfeststellungsverfahrens erfasst werden, werden vom TrustCenter selbst verwaltet.
5. Das WEB.DE-TrustCenter wird auf Anfrage des Privatkunden diesem alle seine personenbezogenen Daten zugänglich machen.

Ihre Anerkennung dieser Geschäftsbedingungen ist Voraussetzung zur Nutzung der kostenlosen Dienste des TrustCenters von WEB.DE



2. Dieser Rechner ist nicht an das allgemein zugängliche WEB.DE-Netzwerk angeschlossen.

3. Die geheimen Schlüssel der CA zum Erzeugen digitaler Signaturen sind ausreichend vor Missbrauch durch Unbefugte geschützt und werden auf keinen Fall weitergegeben.

Die Verantwortung hierfür liegt bei den Administratoren der CA, welche externe Peripherie (kryptographische SmartCard) zum Schutz der geheimen CA-Schlüssel einsetzen.

Der Zugriff auf diese geheimen CA-Schlüssel ist durch komplexe Passwörter geschützt, die nur den CA-Administratoren bekannt sind und die niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden.

Die externe Peripherie wird nicht auf anderen Rechnern eingesetzt.

Mit dem geheimen Signatur-Schlüssel der CA werden Endteilnehmer-Schlüssel bzw. Widerrufslisten (CRLs) unterschrieben.

4. Das Root-Zertifikat mit der die zum Unterschreiben verwendeten CA-Zertifikate erstellt wurden, hat eine Länge von 4096 Bit RSA.

Das Asymmetrische Schlüsselpaar der CA-Zertifikate zur Erzeugung von Signaturen hat eine Länge von 2048 Bit RSA.

5. Für jegliche Standard-Kommunikation werden die geheimen Signatur-Schlüssel nicht verwendet.

6. Das WEB.DE-TrustCenter hat seine asymmetrischen Schlüsselpaare selbst erzeugt.

7. Die asymmetrische Schlüsselpaare für die Endteilnehmer werden direkt auf dem Rechner des jeweiligen Endteilnehmers erzeugt.

Sicherheitsüberprüfung der Zertifikatsnehmer

1. Nach der Anmeldung erhält jeder Anwender zunächst einen Probe-Account.

Damit kann alles ausprobiert und Zertifikate mit einer Gültigkeitsdauer von 30 Tagen erworben werden.

Bei diesen Test-Zertifikaten wird lediglich die Gültigkeit der E-Mail-Adresse geprüft.

2. Innerhalb dieser Zeit schickt das WEB.DE TrustCenter dem Anwender mit der gelben Post einen Activator Key zu, mit dem sein Vollaccount aktiviert werden kann.

Dadurch wird für den Vollaccount zusätzlich auch die Anschrift verifiziert.

Bei den ein Jahr gültigen Zertifikaten wurde vor Herausgabe eines Zertifikates zusätzlich die Postanschrift und die E-Mail-Adresse überprüft.

Sicherheitsanforderungen an Zertifikatsnehmer

1. Der geheime Schlüssel des Endteilnehmers muss ausreichend vor Missbrauch durch Unbefugte geschützt und darf nicht weitergegeben werden; hierfür ist jeder Endteilnehmer selbst verantwortlich.

2. Das asymmetrische Schlüsselpaar des Benutzers weist eine minimale Länge von 512 Bit RSA auf.

Die Wahl größerer Schlüssellängen wird dringend empfohlen, richtet sich aber nach der technischen Verfügbarkeit der auf der Endanwenderseite eingesetzten Software.

Der Benutzer hat den Zugriff auf seinen geheimen Schlüssel durch das Setzen eines komplexen Passworts zu schützen, sofern die eingesetzte Software dies unterstützt.

Das Verzeichnis bzw. die Dateien, in dem die kryptographischen Schlüssel von der Applikation gespeichert werden, sind vom Benutzer nach Maßgabe der Möglichkeiten vor unbefugtem Missbrauch zu schützen

Dies kann z.B. durch das Setzen bestimmter Zugriffsrechte geschehen, sofern das eingesetzte Betriebssystem dies unterstützt

Die Speicherung der kryptographischen Schlüssel auf externen Datenträgern (z.B. Diskette) wird dringend empfohlen.

3. Wird keine externe Peripherie (z.B. Diskette) zum Speichern des geheimen Schlüssels eingesetzt, sollte der Zugriff auf den geheimen Schlüssel des Endteilnehmers durch das Setzen eines komplexen Passworts (Mindestlänge: 8 Zeichen) geschützt werden

Weder die Diskette noch das Passwort dürfen an andere Personen weitergegeben werden.

Das Passwort darf niemals im Klartext abgelegt bzw. über ungeschützte Netzwerkverbindungen gesendet werden.

Zertifikats-Erweiterungen

X.509v3-Zertifikate zeichnen sich dadurch aus, dass jedes Zertifikat beliebige Erweiterungen („certificate extensions“) enthalten kann. Folgende Zertifikatserweiterungen werden vom WEB.DE-TrustCenter unterstützt:

1. NetscapeCAREvocationURL
2. NetscapeBaseURL
3. NetscapeRevocationURL
4. NetscapeCertRenewalURL
5. NetscapeCAPolicyURL
6. NetscapeCertType
7. NetscapeComment
8. CRL Distribution Points
9. Certificate Policies

Management von Zertifikaten

1. Alle Anwender des WEB.DE-TrustCenters erklären sich grundsätzlich mit der Veröffentlichung ihres Zertifikates einverstanden.

2. Für die Überprüfung der Zertifikate hat das WEB.DE-TrustCenter ein Verzeichnis eingerichtet, dessen Aufgabe die Überprüfung und Verteilung von Zertifikaten und CRLs ist.

1. Widerruf von Zertifikaten

Das WEB.DE TrustCenter kann erteilte Zertifikate jederzeit vor Ablauf der Gültigkeitsdauer ohne Angabe expliziter Gründe widerrufen.

2. Jeder Zertifikatsnehmer kann von der Instanz, die seinen Public Key zertifiziert hat, ohne Angabe von Gründen verlangen, dass diese ein für ihn ausgestelltes Zertifikat widerruft.

Das WEB.DE TrustCenter stellt diese Funktion im Hauptmenü im Unterpunkt „Zertifikate verwalten“ zur Verfügung.

Alle widerrufenen Zertifikate werden auf einer Widerrufsliste („Certificate Revocation List“, CRL) veröffentlicht, welche allen Teilnehmern zur Verfügung gestellt wird.

Diese CRL enthält u.a. das Datum der CRL-Herausgabe und wird von der CA digital signiert.

Widerrufene Zertifikate bleiben solange auf der CRL, bis die ursprüngliche Gültigkeitsdauer überschritten wurde.

3. Einmal widerrufen Zertifikate können nicht erneuert oder verlängert werden.

Jedoch hat jeder Teilnehmer grundsätzlich die Möglichkeit, ein neues Zertifikat zu beantragen.

Unmittelbar nach der Aufnahme des eigenen Betriebs hat das WEB.DE-TrustCenter eine CRL herausgegeben.

Die CRL wird im monatlichen Abstand erneuert.

4. Für die Bereitstellung von CRLs hat das WEB.DE-TrustCenter ein Verzeichnis eingerichtet.

Namensgebung

1. Allen Zertifikatnehmern wird ein eindeutiger Name (Distinguished Name, DN) zugeordnet, welches bei der Ausstellung eines Zertifikates für einen Teilnehmer als dessen Subjektname verwendet wird.

2. Ein DN enthält eine Folge von eindeutig kennzeichnenden Namensattributen, durch die alle Teilnehmer einer Hierarchie identifiziert werden.

3. Die Namensgebung jedes Zertifikatnehmers hält sich an das folgende Schema:

Feld	Bedeutung	Inhalt
C	Country	Hier wird der Domain-Name eingetragen, der zum Wohnort des Zertifikatsempfängers gehört, z.B. DE
L	Locality	Wohnort, z.B. D-76227 Karlsruhe
O	Organization	Firmenname (sofern bei der Antragstellung angegeben), z.B. WEB.DE AG
CN	Common Name	Vorname und Nachname (bei vorläufigen Zertifikaten erscheint zusätzlich der Vermerk »vorläufiges Zertifikat«), z.B. Fritz Anwender (vorläufiges Zertifikat)
E-Mail	E-Mail	Hier wird die zum Zertifikat gehörende E-Mail-Adresse eingesetzt, z.B. Fritz_Anwender@T-Online.de

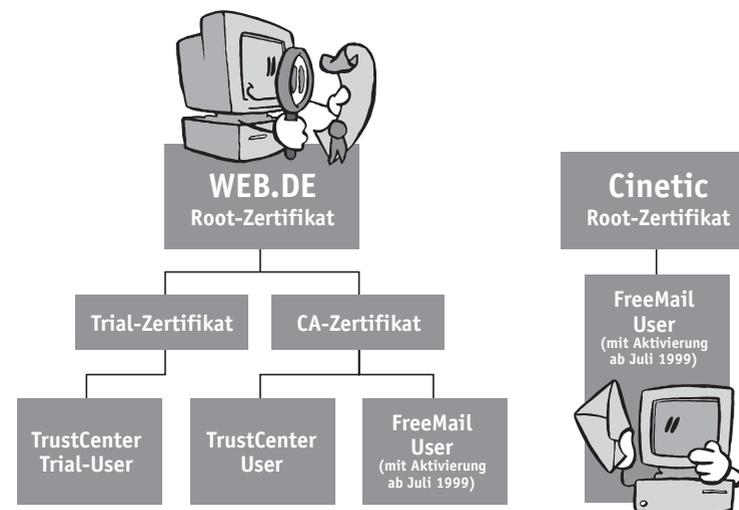
Zusätzlich zu diesen Feldern wird das Zertifikat noch mit einem Kommentar versehen, der Hinweise zum WEB.DE-TrustCenter enthält und bei dem Anwender mit einem Vollaccount zusätzlich eine eigene Kommentarzeile eingeben können.

Anhang IV

Die Zertifikatshierarchie des WEB.DE-TrustCenters

Die Zertifikatshierarchie von WEB.DE besteht aus dem „WEB.DE Root“ Zertifikat, dem „WEB.DE CA“ Zertifikat und dem „WEB.DE Trial“ Zertifikat. Daneben steht noch das „Cinetic Root“ Zertifikat, das bis Ende Juni 1999 die digitalen Ausweise der WEB.DE FreeMail-User unterschrieben hat. Seit Juli 1999 werden die FreeMail-Zertifikate mit dem „WEB.DE CA“ Zertifikat unterschrieben. Da die älteren FreeMail-Zertifikate weit verbreitet wurden, behält das „Cinetic Root“ Zertifikat selbstverständlich seine Gültigkeit und steht auch weiterhin zur Installation bereit.

Den hierarchischen Aufbau der Zertifikatshierarchie illustriert das folgende Schaubild:



Das „WEB.DE Root“ Zertifikat ist die Wurzel aller weiteren Zertifikate. Es stellt die oberste Ebene dar und sagt aus, dass es sich bei allen weiteren Zertifikaten um WEB.DE TrustCenter Zertifikate handelt. Diese Zertifikate wurden generiert und mit dem private Key dieses Wurzel-Zertifikats wurden die beiden Zertifikate der nächsten Ebene unterzeichnet. Danach ist dieser Private Key sicher in einen Tresor gewandert und wird für die tägliche Arbeit nicht mehr benötigt. Sie müssen sich lediglich den Public Key des „WEB.DE Root“ Zertifikats in Ihren Browser installieren, damit die Zertifizierung an der obersten Ebene beginnen kann.

Den Alltagsbetrieb, das Ausstellen und Zertifizieren der User-Zertifikate übernehmen dann das „WEB.DE CA“ Zertifikat und das „WEB.DE Trial“ Zertifikat.

Anhang V

Glossar

Die wichtigsten Begriffe zu den Themen Kryptografie, Verschlüsselung und Zertifikate.

B Blowfish

Der 1994 vorgestellte Algorithmus ist eine Alternative zu IDEA, Triple-DES oder DES zur symmetrischen Verschlüsselung. Blowfish arbeitet mit variabler Schlüssellänge und 448-Bit-Schlüssel. Auch mehrfache Kryptoanalysen konnten keine Schwächen des Algorithmus aufdecken. Da er ohne Lizenzgebühr genutzt werden kann, wenig Speicherplatz benötigt und deutlich schneller arbeitet als DES, wird er bereits in einigen Produkten eingesetzt, etwa in Mail Guardian.

D DES

DES (Data Encryption Standard) ist ein Verschlüsselungsverfahren, das in den 70er Jahren von IBM entwickelt und 1977 von der US-Regierung als offizieller Standard anerkannt wurde. Die Schlüssellänge beträgt 56 Bit. Wegen des vergleichsweise kurzen Schlüssels gilt DES heute nicht mehr als ganz sicher, da er durch eine Brute-Force-Angriff zu schnell geknackt werden kann.

Diffie-Hellman-Verfahren

Diffie und Hellman stellten 1976 als erste ein Public-Key-Verfahren vor, das ähnlich wie RSA zu einem Public-Private-Schlüsselpaar führt. Das Diffie-Hellman-Verfahren (DH) nutzt den Elgamal-Algorithmus, der bei gleicher Schlüssellänge genauso sicher ist wie der RSA-Algorithmus.

E Elgamal-Algorithmus

Der Elgamal-Algorithmus wird vom Diffie-Hellman-Verfahren (DH) genutzt und ist bei gleicher Schlüssellänge genauso sicher wie der RSA-Algorithmus. Elgamal beruht auf der Schwierigkeit, diskrete Logarithmen zu berechnen.

F Fingerprint

Der Fingerprint (Fingerabdruck) ist eine mit dem Algorithmen MD5 oder SHA1 berechnete „Quersumme“ über die einzelnen Bits, aus denen der öffentliche Schlüssel zusammengesetzt ist.

Wenn der Fingerabdruck eines Schlüssels entsprechend weit verbreitet ist, ist der Schlüssel sicher davor, unbemerkt von einem auf dem Nachrichtenweg lauernden Bösewicht ausgetauscht zu werden, weil es praktisch unmöglich ist, einen zu einem vorgegebenen Fingerabdruck passenden Schlüssel zu generieren. Drucken Sie Ihren Fingerprint auf Ihre Visitenkarte und auf Briefbögen.

I IDEA

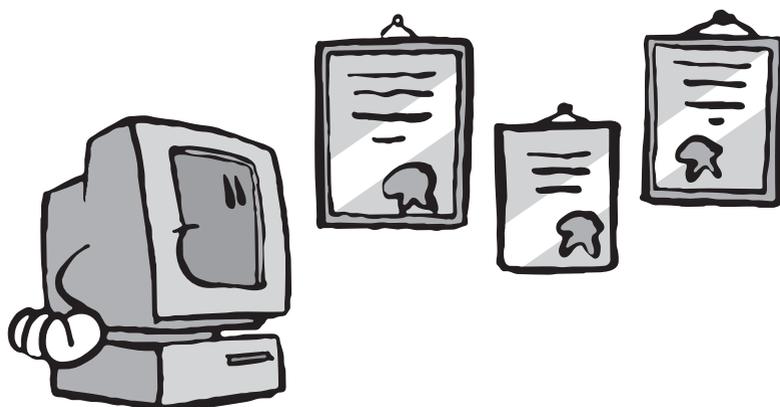
IDEA (International Data Encryption Algorithm) arbeitet ähnlich wie DES, verwendet jedoch einen 128-Bit-Schlüssel. IDEA wurde 1990 am Swiss Federal Institute of Technology entwickelt. Durch seinen deutlich längeren Schlüssel ($2^{128} = 3,4 \times 10^{38}$

Die verschiedenen Klassen

Das WEB.DE TrustCenter stellt zwei Klassen von Zertifikaten aus: Bei den vorläufigen Zertifikaten ist die Gültigkeitsdauer auf 30 Tage beschränkt und auf der Anwender-Seite die Existenz der E-Mail-Adressen geprüft worden. Diese vorläufigen Zertifikate werden vom WEB.DE Trial- Zertifikat unterschrieben.

Bei den 1 Jahr gültigen Zertifikaten hat das WEB.DE TrustCenter die Postanschrift des Anwenders per gelber Post überprüft. Diese Zertifikate werden vom „WEB.DE CA“ Zertifikat unterschrieben. Das gleiche Verifizierungsverfahren wird auf alle neuen FreeMail-User angewandt. Daher unterschreibt WEB.DE auch die Zertifikate der FreeMail-User mit dem „WEB.DE CA“-Zertifikat. Wenn Sie die Public Keys des „WEB.DE CA“ Zertifikats und des „WEB.DE Trial“ Zertifikats in Ihren Browser installieren, sind Sie in der Lage, alle Variationen der WEB.DE TrustCenter Zertifikate zu installieren.

Alle möglichen Fälle decken Sie ab, wenn Sie zusätzlich noch das ältere „Cinetic Root Zertifikat“ installieren.



mögliche unterschiedliche Schlüssel statt $256 = 7,2 \times 1016$ wie in DES) gilt IDEA im Unterschied zu DES als sehr sicher. Vor allem aber ist kein Fall bekannt, in dem der IDEA-Algorithmus selbst geknackt wurde.

M MD2, MD4 und MD5

Bei MD2, MD4 und MD5 handelt es sich um Algorithmen, die nicht zur Verschlüsselung, sondern zum Erzeugen digitaler Unterschriften eingesetzt werden. Während der MD4-Algorithmus sehr leicht zu durchbrechen ist, gelten MD2 und MD5 nach wie vor als sicher. Alle genannten Algorithmen berechnen aus einer Nachricht eine Prüfsumme, bei MD5 ist diese Prüfsumme 128 Bit lang.

P PKCS (Public Key Encryption Standards)

Von der RSA herausgegebene Standards zur Public Key Verschlüsselung. PKCS unterstützt das RSA- und das Diffie-Hellman-Verfahren. Außerdem umfasst PKCS eine Algorithmus-unabhängige Syntax für digitale Unterschriften und digitale Umschläge. Die Syntax, die in S/Mime verwendet wird, entspricht z.B. dem Standard PKCS #7.

Private Key

Geheimer Teil eines Schlüsselsatzes. Den privaten Schlüssel halten Sie geheim und hüten ihn wie Ihren Augapfel. Er dient zum Lesen verschlüsselter Mails, die Sie empfangen und zum unterschreiben ausgehender Mail.

Public Key Verschlüsselung

Bei diesem asymmetrischen Verschlüsselungsverfahren besitzt jede Person eine einzigartige Kombination zweier unterschiedlicher, aber zueinander gehörender Schlüssel: einen öffentlichen (Public Key) und einen privaten Schlüssel (Secret Key). Eine Nachricht, die mit einem öffentlichen Schlüssel kodiert wurde, lässt sich nur mit dem zugehörigen privaten Schlüssel dekodieren.

R RSA

RSA ist ein 1977 von Rivest, Shamir und Adleman vorgestellter Algorithmus, der zur asymmetrischen Verschlüsselung verwendet wird. Die Schlüssel entstehen dabei durch Multiplikation zweier Primzahlen mit mehreren hundert Stellen. Die hohe Sicherheit von RSA beruht darauf, dass es erheblich aufwendiger ist, aus dem Ergebnis wieder die ursprünglichen Primzahlen zu ermitteln. Kritisch für die Sicherheit einer RSA-Verschlüsselung ist die Länge des verwendeten Schlüssels.

Problematisch bei RSA ist, dass die Ver- beziehungsweise Entschlüsselung ungleich länger dauert als etwa bei den Algorithmen DES und IDEA. Aus diesem Grund setzen die meisten Public-Key-Produkte auf zwei Algorithmen: Zum Kodieren wird zum Beispiel IDEA verwendet, der dabei benutzte Schlüssel wird anschließend mit RSA kodiert und (in kodierter Form) mit der Nachricht übertragen.

S SHA und SHA-1

SHA und SHA-1 (Secure Hash Algorithm) sind wie MD2 bis MD5 für digitale Signaturen gedacht. Ähnlich wie MD4 enthält SHA einen Fehler, der diesen Algorithmus unsicher macht. SHA-1 korrigiert dies und gilt als sicherer als MD5, dafür arbeitet MD5 etwas schneller. Beide Algorithmen berechnen (genau wie MD2, MD4 und MD5) aus einer Nachricht eine Prüfsumme, bei SHA ist diese Prüfsumme 160 Bit lang.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) erweitert das MIME-Format um Verschlüsselung und digitale Unterschriften. Das MIME-Format ermöglicht das Einbetten von Binärdateien in eine E-Mail. Die in S/MIME verwendete Syntax für verschlüsselte oder unterschriebene Nachrichten entspricht dem unter anderem von Microsoft, Sun, Lotus und dem MIT entwickelten Standard PKCS #7 (Public-Key Cryptography Standards). PKCS unterstützt das RSA- und das Diffie-Hellman-Verfahren. Außerdem umfasst PKCS eine Algorithmus-unabhängige Syntax für digitale Unterschriften und digitale Umschläge.

T Triple-DES

Triple-DES ist eine Weiterentwicklung von DES. Bei diesem Verfahren werden drei Verschlüsselungsläufe durchgeführt und entweder zwei oder drei Schlüssel verwendet. Die höchste Sicherheit bietet die Verwendung dreier unterschiedlicher Schlüssel; man kommt dann auf eine effektive Schlüssellänge von 112 Bit.

X X.509

X.509 ist ein Standardformat der ITU-T für Zertifikate (International Telecommunications Union-Telecommunication). Es enthält den Namen und die digitale Signatur des Ausstellers und Angaben über die Identität des Inhabers. Auf dem X.509-Format basieren die hier verwendeten Verfahren S/Mime und SSL. Das WEB.DE TrustCenter unterscheidet bei X.509-Zertifikaten zwei Klassen:

1. vorläufige Zertifikate (30 Tage gültig)
2. 1 Jahr gültige Zertifikate

Z Zertifikat

Ein Zertifikat enthält den Namen und die digitale Signatur des Ausstellers und Angaben über die Identität des Inhabers. Die vom WEB.DE TrustCenter ausgegebenen Zertifikate basieren auf dem X.509-Format.

IMPRESSUM:

Design, Konzeption, Realisierung & Betrieb:

WEB.DE AG
Amalienbadstr. 41, 76227 Karlsruhe,
Tel: 0721/943290, Fax: 0721/9432922

Feedback, Vorschläge und Kritik sind immer willkommen bei:
trust@web.de

Software-Design, Entwicklung
Thomas Schäfer, WEB.DE AG

Gesamtkonzeption & -realisierung
Stefan Rinke, WEB.DE AG

Herausgeber: WEB.DE AG

Projektleitung: Armin Gellweiler

Texte: Achim Wagenknecht

Grafik & Layout: ArtCrash
Werbeagentur GmbH

Hotline: 0721/9432936

Dieses Handbuch unterliegt dem Urheberrecht. Alle Rechte vorbehalten.