Einstieg in elektronische Signaturen

Vorwort

Ziel dieser Anleitung ist es, eine sigenannte *elektronische Signatur* im E-Mailverkehr nutzen zu können.

Angesprochen sind Laien, blutige Anfänger und sonstige Interessierte.

Wir beziehen uns auf sogenannte *Fortgeschrittene Signaturen*, welche viele Hochschulen in Deutschland über den Verein zur Förderung des Deutschen Forschungsnetzes e.V., kurz DFN. ihren Nutzern zugänglich machen können. Das Prinzip von /elektronische Signaturen *dieser Art, ist aber auch bei anderen Anbietern, in anderen Umgebungen das selbe. Wir verzichten in dieser Erklärung praktisch komplett auf Fachbegriffe. Details beschreiben wir nicht und dafür sind wir an manchen Stellen sicher auch etwas ungenau. Sofern dies dem einfacheren Verständnis für E-Mail und elektronische Signaturen dient, sei dies hier akzeptiert. Im letzten Kapitel bieten wir dann Links und Informationen an, welche sich sicherlich für das weitere Studium eignen. Über Korrekturen und Verbesserungsvorschläge freuen wir uns sehr! Wir unterstellen folgende Kenntnisse: - Sie haben bereits E-Mails geschrieben, empfangen, kennen E-Mail - Sie wissen, was ein Browser ist (Programm zum Anschauen von Webseite) Was wir im folgenden* ***nicht*** *erklären: - Signierte E-Mails sind nicht verschlüsselt, über Verschlüsselung sprechen wir nicht. - Wir bieten keine Dokumentation und Erklärung für Mailprogramme, Computer.* ***Hinweis:*** *Wir werden hier nicht erklären, wie sie ihren Computer sicher und „geschützt“ betreiben. Auch wenn sie keine Zertifikate einsetzten werden: Ihr Computer muss immer mit Virenscanner, Updates und einer Firewall geschützt werden. Dies gehört einfach zum Einmaleins und hierzu finden sie auch sehr viele gute Tips und Anleitung an anderer Stelle. ===== E-Mail - Der große Irrtum ===== Ein häufiger Irrtum ist die Meinung, dass die Absenderadresse in herkömmlichen E-Mails irgendwo/irgendwie geprüft und geschützt werden kann. Dies ist praktisch nicht, bzw. nur in sehr bescheidenem Ausmaß möglich. Absolut überaschend ist, dass so wenig einigermaßen gut gefälschte E-Mails unterwegs sind! Vielleicht ist dies für Kriminelle auch gar nicht notwendig, so lange genügend Anwender auf erbärmlichst schlecht und schlampig erstellte E-Mails (siehe phishing) hereinfallen. Hie und da findet man aber auch einigermasen schöne, gut verfasste E-Mails von Betrügern und Spammern. Ein Grund, weshalb so viele Betrügereien mit E-Mails möglich sind, ist einfach der Sachverhalt, dass wir so wenig über E-Mail wissen und verstehen. Bei jeder E-Mail sollten wir vorsichtig sein: „gute Mail“ oder „Spam“? Aber wie sollen wir sicher sein und* gute E-Mails *von* schlechten E-Mails *unterscheiden können? Eine digitale Signatur, über das was wir hier sprechen, ist genau hierfür eine enorme Hilfe!* ***Von nun an sollten sie wissen:*** *Es ist nur glücklicher „Zufall“, dass die meisten E-Mails ihrer Freunde und Bekannten „echt“ sind. In Mailprogrammen geben sie selbst an, wie ihre Absenderadresse lauten soll. Genauso einfach schreiben sie eine richtige oder eine falsche Adresse auf einen Postbrief. Natürlich ist es verboten, fremde Namen und Identitäten vorzugaukeln. Es ist Betrug! Nur: Herkömmliche E-Mails bieten dagegen einfach keinen Schutz. Glauben sie an die Echtheit oder nicht. Überprüfen oder beweisen können sie dies ohne weitere Hilfsmittel nicht. Beim Verschicken einer E-Mail werden sie oft nach einem Kennwort gefragt. Dies wird aber fast ausschließlich dafür genutzt um zu überprüfen, ob sie auch das Recht zum Schicken von E-Mails haben. Es stellt quasi die Briefmarke dar, oder das Öffnen der Klappe für den Briefkasten - nicht mehr und nicht weniger. Sie sie nun verunsichert? Sollten sie nicht. Die Tageszeitung in Ihrem Briefkasten wurde auch von niemandem unterschrieben oder sonstwie überprüft. Ich kenne keinen Fall, in welchem einem Bekannten von mir eine gefälschte Tageszeitung in den Briefkasten gelegt wurde. Sie müssen nur wissen: Eine E-Mail kann einfach mit*

falschen Angaben versehen werden. Der E-Mailverkehr wurde bei seiner Erfindung nicht mit Mitteln gegen Betrug und Fälschung entworfen. Denn genau darum geht es hier: Das Nachholen von Sicherheit, Vertraulichkeit im Bezug auf E-Mail. Wir wollen dies nicht mehr dem Zufall überlassen. ===== Was ist eine Signatur ===== Kurz angemerkt: Das Thema Signatur spielt unter anderem auch im Web und bei Software eine große Rolle. *==== Von welcher Signatur reden wir? ==== Wir müssen hier auf ein Verwirrspiel bei der Begrifflichkeit hinweisen. So wie Schloß und Schloß das selbe, oder auch etwas ganz anderes meinen kann, so ist dies mit* Signatur *auch. === Der übliche Text unter einer E-Mail… === Oft findet sich unter dem eigentlichen Text einer E-Mail etwas wie z.B.: … Mit Freundliche Grüßen, Ihr Support-Team Doch davon reden wir hier nicht! Dennoch nennt man dies auch* Signatur*. Manch andere hängen ein Bild an die E-Mail, auch das meinen wir nicht. === Die elektronische Signatur === Was wir meinen ist ein Zusatz, welcher kein weiterer Text unter der E-Mails ist. Es ist eher eine weiterer Bestandteil der Verpackung einer E-Mail. Und unser E-Mailprogramm muss diese Verpackung lesen und verstehen können. Viele Mailprogramme können das leider nicht! So verstehen wir unter unserer* elektronischen Signatur *also etwas, was in unser Mailprogramm neue Funktionen hinzufügt. Beim Senden und Empfangen können wir dann diese Signatur eben lesen und prüfen (besser: prüfen lassen, denn unser E-Mailprogramm erledigt dies von ganz alleine). Auch ohne elektronische Signatur kann man leben, doch sobald Absender und Empfänger mit einer Signatur umgehen können, so ist sichergestellt…: * ob der Brief auf seinem Weg vom Absender zum Empfäner unverändert blieb und * ob dieser wirklich von unserem erwarteten Absender und keinem Betrüger stammt.* ***Fazit:*** *Die elektronische Signatur soll für Sicherheit sorgen:* ***Der Absender*** hat wirklich ***das*** geschrieben. **Signierte E-Mails sind nicht verschlüsselt! Die Daten sind nicht vor Diebstahl und fremden Einblicken Geschützt!** *Wenn wir uns einen herkömmlichen Brief auf Papier vorstellen, finden wir Unterschiede und Parallelen: Ist uns die Handschrift gut bekannt, kennen wir die Unterschrift, dann sind wir uns auch relativ sicher, ob* **Er** *das war. Was wir auf Papier aber nicht immer so gut kontrollieren können: Hat noch ein fremder einen Satz dazu geschrieben?! Denken wir an Verträge: Eine zweifache Ausfertigung soll dies hier verhindern. Beide Parteien unterschrieben, jeder erhält eine Ausführung. So ist dort ein nachträgliches Hinzufügen von Text auf nur einer der Vertragsausführungen ein wahrhaft „schlechter" Betrug. Mit einer elektronischen Signatur ist dies anders. Hier hilft uns etwas „Magie" aus der Mathematik- und Technikkiste. Wir benötigen keine doppelte Ausführung von E-Mails. Der eigentliche Text wird vor Veränderungen geschützt (besser: Ändern kann man schon, nur wird eine Änderung erkannt und wir davor gewarnt!). Ein klarer Pluspunkt für die elektronische Signatur. Die Frage, wie sicher, wie vertrauenswürdig so eine Signatur ist, leitet sich über die gesetzlichen Bestimmungen und den daraus folgenden technischen und organisatorischen Masnahmen ab. „Schon echt sicher", könnte man hier sagen. Eine „normale" E-Mail ohne solch eine Signatur dagegen ist „absolut unfassbar unsicher und unvertrauenswürdig". ==== Unser Sprachgebrauch ==== Im Folgenden reden wir also meist nur noch von* **Signatur** *und meinen damit die* Fortgeschrittene elektronische Signatur*, siehe folgendes Kapitel. Ebenso werden wir den Begriff* **Zertifikat** *nun häufiger verwenden. Gewöhnen Sie sich daran: Auch dieser Begriff meint praktisch das Selbe. Mit einem Zertifikat signieren wir, die E-Mail ist eine signierte E-Mail… so oder ähnlich ist der Sprachgebrauch. ====== Welche Organisationen oder Gesetzte bilden unseren Rahmen ====== Unseren Personalausweis bekommen wir nur von der öffentlichen Hand. Signaturen hingegen können Firmen, Einrichtungen ausstellen. Der Gesetztgeber hat aber drei Qualutäts- oder Sicherheitsstufen definiert. Jene sind im Gesetz über Rahmenbedingungen für elektronische Signaturen, kurz SigG, definiert. ===== Personalausweis und Reisepass - Drei verschiedene Signaturen ===== So wir wir in Deutschland zwei verschiedene Ausweispapiere kennen, hat der Gesetzgeber drei verschiedene Signaturen beschrieben. Wir behandeln hier die mittlere, die* Fortgeschrittene Signatur*. Die hier in Deutschland höchste Sicherheitssture wird mit der* Qualifizierte Signatur *umgesetzt. Die praktische Anwendung ist im Vergleich zur* Fortgeschrittenen Signatur *viel aufwendiger, komplizierter und somit auch viel teurer. Kaum jemand hat bisher überhaupt die Technik im Haus, um mit* Qualifizierten Signaturen *arbeiten zu können. Hingegen reicht für die* Fortgeschrittene Signatur *etwas Wissen und*

Verantwortungsbewußtsein, ein handelsüblicher Computer und ein passendes Mailprogramm (oft kostenlos). Die Qualifizierte Signatur *hat aber den Vorteil: Auch ein Profi mit vollem Zugriff auch Ihren PC kann die Signatur nicht klauen. Mit dem neuen elektronischen Personalausweis haben wir schon ein Baustein zur Nutzung einer* Qualifizierten Signatur*, doch der Weg dorthin ist noch lange und teuer. Auch findet man kaum Kommunikationspartner, welche bereits etwas mit diesem „Sicherheitslevel“ anfangen können. Einfach und kurz formuliert kann man sagen: Eine* Qualifizierte Signatur *ist so „heilig“ und rechtskräftig wie eine handschriftliche Unterschrift. Bei der* Fortgeschrittenen Signatur *verlangt der Gesetztgeber aber bereits schon eine gründliche Überprüfung der Identität des Antragstellers und dessen E-Mailadresse. So kann unsere hier beschriebene* Fortgeschrittene Signatur *bereits Vertragspartner genügen, um gewisse Formalitäten und Prozesse damit durchzuführen. Die Partner vereinbaren zum Beispiel, dass der formlose Antrag per elektronisch signierter E-Mails genügt, um einen Raum buchen zu können, oder mehr Speicherplatz zu bekommen. Sie können dies natürlich auch ohne signierten E-Mails - wie bisher - erledigenn. Es ist einfach eine Frage des „ich vertraue und glaube dem Inhalt einer E-Mail“, oder eben nicht. ===== Woher kommen dann die Zertifikate? ===== Als Anweder und Nutzer von Zertifikaten/Signaturen sind wir auf Organisationen, eine Infrastruktur angewiesen, welche uns passende Signaturen/Zertifikate ausstellen. So gibt es Firmen und Unternehmen, welche entgetlich Dienste diesbezüglich anbieten. In unserem Fall hier betrachten wir nur das* Deutsche Forschungsnetzes DFN*, welches seinen Mitgliedern (also Hochschulen, Universitäten u.a) unentgeltlich* Fortgeschrittene Signaturen *verfügbar macht. Dazu aber später mehr in Lektion 3! Merken sie sich nur: Der Gesetztgeber diktiert die Spielregeln, umgesetzt und angeboten werden die Dienste aber durch Firmen, Einrichtungen (vgl. Riesterrente, Haftpflichtversicherungen u.v.m). ====== Das Mindeste was wir wissen und verstehen müssen ====== ===== Rechte und Pflichten rund um's Zertifikat ===== Das Recht ein Zertifikat nutzen und ausgestellt zu bekommen, setzt voraus, dass sie die grundlegende Funktionen verstanden und vereinbarte Pflichtungen kennen und einhalten. Die Vereinbarung welche getroffen werden, müssen von ihnen eigenhändig unterschrieben werden. Die Organisation, welche ihnen dann ein Zertifikat ausstellt, muss auch ihren Personalausweis oder Reisepass in Augenschein nehmen. Die letzten fünf Ziffern Ihrer Personalausweisnummer werden auf dem Dokument festgehalten. Ist ihre Pass abgelaufen, dann darf kein Zertifikat erstellt werden. Sie verpflichten sich in dieser Vereinbarung besonders zu drei Dingen: * Nur sie alleine dürfen das Zertifikat nutzten, (Verständlich: Soll dieses doch den Beweis erbringen, dass sie sie sind). * Sie „schützen“ und „sichern“ dieses Zertifikat (man wird Ihnen sagen wie das geht). * Sie lassen das Zertifikat sperren, wenn es abhanden gekommen ist. Und umgekehrt haben sie das Recht (hier im Beispiel DFN), dass man sie einweist und schult: * Wie man mit dem Zertifikat umgeht, wie man dieses nutzt, * was sie genau wo und wie schützen müssen (und was nicht), * wo sie ein Zertifikat beantragen oder sperren können. Kurzum, der „Aussteller“ eines Zertifikates im DFN Verbund muss…: * sich um sie kümmern, sie schulen. * Er muss sich sicher sein, dass sie sie sind (→ Ausweis prüfen), * prüfen, ob sie ein Recht auf das Zertifikat haben (vgl.: Den Deutschen Personalausweis kann man erhalten, wenn man die deutsche Staatsbürgerschaft hat. Ein Zertifikat hier aus der DFN, wenn man zum Nutzerkreis einer Hochschule im DFN Verbund gehört. Andernfalls müsste man andere Organisationen/Firmen als Aussteller ausfindig machen), * sich sicher sein, dass sie in der Lage sind, ihr Zertifikat zu schützen, * nachfragen, Gewissheit haben, dass auch nur ihnen dieses Zertifikat bekannt ist. ===== Und so funktioniert's! ===== Endlich sind wir soweit! Wir erklären nun anhand von Beispielen in vier Lektionen die Verwendung und Beschaffung einer Signatur, eines Zertifikats. Fachwörter werden verwendet, sofern sie mit diesen im Alltag konfrontiert werden. Bitte merken sie sich jene und die hier beschriebenen Funktion oder Aufgabe der Bausteine. Das „wie genau“ dürfen sie gerne studieren, das verlangen wir aber nicht. Zu Beginn, aus den einzelnen Bausteinen, erschließt sich Anfangs sicher noch kein ganzes Bild. Darum fassen wir am Ende die Bausteine nochmals zusammen. ==== Lektion 1: Public-key-Verfahren - Wilde Zahlenhaufen ==== Schlaue Leute haben herausgefunden, dass man mit anspruchsvoller Mathematik, zwei wilden, aber zueinander passenden Zahlenhäufen einen Auf- und Abschließmechanismus bauen kann. Nehme ich die Mathematik und den einen Zahlenhaufen, kann*

*ich damit Daten verschlüsseln. Nehme ich nun wieder Mathematik, den anderen Zahlenhaufen, kann ich eben jene Daten wieder entschlüsseln. Das ist besonders? Das ist einer der wichtigsten „Geheimnisse“?! JA! Denn wieder schlaue Leute hatten dann einfach diese Idee: „Also… wenn ich den einen Zahlenhaufen für mich geheim halte und schütze, den anderen Zahlenhaufen aber jedem bekannt mache, irgendwo veröffentliche… dann, ja dann kann ich doch jedem x-beliebigen eine von mir verschlüsselte Nachricht schicken. Und der Empfänger holt sich meinen überall verfügbaren zweiten Zahlenhaufen und entschlüsselt somit meine Post! Wenn das entschlüsseln klappt, weiss man: Das kam echt von dem mit dem anderen Zahlenhaufen“. Et voila - Sie sind nun ein Experte in Sachen Kryptographie und kennen das public key Verfahren. Die Eigenschaften dieser Zahlenhäufen und der verwendeten Mathematik ist so gut, dass Wissenschaftler, Geheimdienste dies nicht knacken können. Das weiss man, da man öffentlich und weltweit darüber berät und forscht. Sofern die geheime Information, der geheime Schlüssel nicht in falsche Hände gerät, ist die Sache sicher. Wenn Sie also nun den nächsten Spielfilm schauen und irgend ein Held sich anstrengt und einen „2048 bit Schlüssel“ knackt *gähn*, es ist eben für den Film… Große Zahlenhaufen, einen Teil gut schützen: Unknackbar (PS: Das mit dem „2048 bit Schlüssel“ war nun echt Fachchinesisch. Denn in der Tat ist das eine gültige Formulierung für die Länge eines Zahlenhaufens. Noch länger, noch besser. Doch die verwendete Mathematik spiel auch eine Rolle. Hier dazu nicht mehr, das wäre zuviel Fachchinesisch). Der Vollständigkeit sei hier noch angemerkt: Das obige Ver- und Entschlüsseln geht in alle Richtungen… man kann auch mit dem öffentlichen Schlüssel verschlüsseln. Das „dumme“ (oder sagenhafte) ist dann aber, dass die Daten dann nur vom Inhaber des privaten Schlüssels entschlüsselt werden können. Für die elektronische Signatur wird Ihre Mail nicht verschlüsselt. Nur ein Prüfsumme wird verschlüsselt. Das Mailprogramm des Empfängers wertet diese Daten aus. Ihre E-Mail ist also weiterhin lesbar, nicht verschlüsselt. Es wurde nur eine Art Fingerabdruck geschützt. Hierfür braucht man eben genau dieses public-key-Verfahren. === Sprachgebrauch === Den einen Haufen nennen wir nun im Folgenden den* **privaten und oder geheimen Schlüssel***. Den anderen Haufen nennen wir den* **öffentlichen Schlüssel, oder public key***. (Es kann schon vorkommen, dass ein Informatiker einem einen public key ganz geheim und verschlüsselt zukommen lassen will. Der hat's dann einfach nicht ganz begriffen…). Man spricht von* **Public-Key-Verfahren***. ==== Lektion 2 - Erzeugen, Schützen von „Zahlenhaufen“ ==== Woher kommt nun unser Schlüsselpaar aus Lektion 1? Ganz einfach: In quasi all unseren Computern sind bereits Programme vorhanden, welche uns mit ein, zwei Mausklicks solche Schlüsselpaare generieren. Es ist für uns ganz unerheblich, wie diese zufälligen Schlüssel lauten, es sind einfach zufällig erzeugte Zahlenkolonnen, welche zueinander passen. Das Wichtige ist nur immer: Den einen Teil davon schützen wir wie unseren Augapfel, den anderen Teil können wir gerne in der Stadt plakatieren gehen… Meist legt so ein Programm diese Schlüsselpaare irgendwo in einem extra Bereich für Schlüssel ab. Doch Achtung! Viele Programme schützen eben diese Schlüssel nicht von vornherein! Sie müssen prüfen und dafür sorgen, dass ihr Programm das tut!* ***Fragen*** *sie bei ihrer CA (siehe nachfolgende Lektion 3)* ***vor der Schlüsselerzeugzung um Rat*** *und Hilfe! Ohne diesen Schutz der Schlüssel kann der nächste Besucher unseres PCs einfach jene entwenden und unter unserem Namen Unfug anstellen! Sehr ungemütlich! Das will man nicht und das ist auch nicht erlaubt. Man* ***MUSS*** *seinen Schlüssel schützen! Sie haben also nicht die Wahl, ob sie das tun oder nicht. Ohne Schutz wird man ihnen kein Zertifikat ausstellen. Darum müssen Sie auf folgendes achten: * Wo legt mein Programm den Schlüssel ab und * habe ich diesen mit einem guten Kennwort (min. 8 Stellen) geschützt? Fragen Sie vor Ort bei Ihrer Registrierungsstelle nach, wie die Erzeugung der Schlüssel erfolgen soll. Es ist in jedem Fall einfach. Denn oft ist dies mit ein, zwei Klicks schon erledigt. Zum Beispiel nennt sich in Firefox oder Thunderbird der entsprechende Bereich in den Einstellungen einfach „Passwörter“. Und wenn sie diesen dort schützen wollen, müssen sie dort ein sogenanntes „Master-Passwort“ dort verwenden (Sprachgebrauch von Thunderbird und Firefox. Oft wird von keystore geredet. Und eben einem Kennwort des keystores). Sie werden weitere Menüpunkten in ihrem Programm finden, um die dort hinterlegten und gespeicherten Zertifikate und Schlüssel auf USB Stick etc. speichern zu können. So können Sie dann auch diese Daten in das nächste Programm laden, an einem anderen PC nutzen.*

Sie sollten eine Kopie an sicherem Ort auf z.B. USB Stick bewahren. Denn wie sie ja nun wissen: Ausser ihnen hat ja niemand anderes ihren privaten Schlüssel. ***Hinweis:*** *Unsere hier verwendete Sicherheitsstufe (siehe Vorwort) akzeptiert, dass wir unsere geheimen Informationen in Dateien auf Computern speichern. Dies birgt die Gefahr, dass Administratoren, Personen/Hacker mit Vollzugriff auf Ihren PC, sich den Schlüssel stehlen/kopieren könnten! Ihr Schlüssel ist maximal so sicher geschützt, wie ihr PC geschützt ist. Sie müssen den PC also "pflegen" (Software Updates, Firewall, Virenscanner, nicht als Administrator arbeiten usw.). Das Kennwort für den Schlüssel ist ein Schutz, doch ist dieser Schutz nicht unumwindbar: Bösewichte können ihren Computer so erweitern und umbauen, dass er die Eingabe ihrer Tastatur mitliest. So könnte das Kennwort in fremde Hände gelangen. ==== Lektion 3: Die Zertifizierungsstelle - Fast wie ein Telefonbuch mit öffentlichen Schlüsseln ==== Bisher wissen wir, dass wir den privaten Schlüssel schützen müssen, dieser darf nur uns bekannt sein. Wir wissen auch, dass der öffentliche Schlüssel aber irgendwie zu den Empfängern muss. Aber halt: Im Schlüssel steht kein Name, nicht von wem dieser ist. Wir brauchen somit eine Art Telefonbuch, eine Zentrale, welche den öffentlichen Schlüssel notiert, sowie unseren Namen, unsere E-Mailadresse dazu schreibt. Diese Telefobuchstelle muss dann aber auch noch mehr können: Was passiert, wenn ich den geheimen Schlüssel nicht mehr habe? Dann muss auch der Telefonbucheintrag raus. Es erübrigt sich zu erwähnen, dass die Telefonbuchstelle von sehr gewissenhaften Personen geführt werden muss. Wenn es einem Betrüger dort gelingen würde, unter fremdem Namen etwas zu hinterlegen... aua! Und es geht noch weiter: Es besteht die weitere Gefahr, dass sie dem Telefonbuch eines Betrüges aufsitzen! Denn es gibt etliche „Telefonbücher", unser Computer, unsere Programm kennen sehr viele. Diese Telefonbücher sind also sehr wichtig, es sind unseren heiligen Kühe! Gott sei Dank, müssen wir uns um die Pflege nicht extra kümmern, denn wenn wir unseren PC, unsere Programme aktuell halten, so werden auch diese Telefonbücher mit gepflegt und aktualisiert, voll automatisch! Es versteht sich also von selbst: Sie hegen und pflegen ihren PC: Updates, Virenscanner, Firewall - alles tip top und taufrisch! Auch arbeiten sie nicht am PC als sogenannter „Administrator"! Schützen sie sich und ihren PC, lassen sie sich beraten wie! === Sprachgebrauch === Wir nennen diese „Telefonbuchstelle" nun* Registrierungsstelle*. Da jene Stellen international aggieren, bekannt sind, der engliche Begriff:* Certification Authority*, kurz* CA*. Die obige Wortwahl „Telefonbuch" ist also totaler quark, wurde nur als Erklärungsbrücke gewählt. === Ein Zertifikat erhalten === Nimmt eine CA von uns einen Zahlenhaufen, also unseren öffentlichen Schlüssel, sowie unsere Daten (Name...) an, dann hat diese von uns einen Zertifikatsantrag angenommen/erhalten (dies wird auch certificate signing request, kurz CSR genannt. Doch es genügt, wenn sie irgendwie wissen, dass sie einen Antrag für so ein Ding einreichen müssen). Gibt diese Stelle, die CA dann ein „ok", dann erhalten wir einen neuen Haufen zurück. In jenem neuen Haufen steckt unser Name (etc.), unser öffentlicher Schlüssel und: - Unseren Namen, unsere E-Mailadresse, - unseren öffentlicher Schlüssel, - Erstell- und Ablaufdatum u.v.a, - sowie Informationen zur CA und zur Überprüfung dieses Zertifikates (siehe hierzu auch X.509) Das was man hier zurück erhält, das ist das Zertifikat! Sie können dies öffentlich bekannt machen, auf ihrer Webseite zum Download anbieten - wie auch immer. Das müssen sie aber nicht, denn schicken sie eine signierte E-Mail, wird ihr Zertifikat gleich mitgeschickt. Hat der Empfänger ein Mailprogramm mit Unterstützung für diese Zertifikate, wird der Empfänger sehen, ob die Mail von ihnen signiert ist.* ***Hinweis:*** *Unser Bild mit dem Telefonbuch passt nur ein wenig. Daten wie Name, Adresse können wir in der CA veröffentlichen lassen, müssen aber nicht. Auch ohne Veröffentlichung kann das Mailprogramm unseres Empfänger einer signierten Mail prüfen, ob wir in der CA so geführt sind. Wie das geht, das müssen sie nicht wissen, darum erklären wir es hier nicht (siehe weitere Informationsquellem am Ende dieses Dokuments). ==== Lektion 4 - Zertifikate nutzen ==== Nehmen wir an, sie haben Lektionen 1 bis 3 verstanden. Was dann?! Laden sie nun das in Lektion drei beschriebene Zertifikat in ihr Mailprogramm (Achtung: Nicht alle Mailprogramme sind verwendbar). Oft müssen Sie nun noch einen Schalter im Mailprogramm anklicken, ob denn nun jede Mail von ihnen signiert werden soll, oder eben nur hie und da. Doch wichtiger wird folgender Punkt: Sie müssen die Zeichen, Symbole und Hinweise beim Empfangen von signierten E-Mails verstehen! Was nutzt es, wenn man man die Warnung vom Mailprogramm als ein Hinweis „Hey, alles Super!" missdeutet?*

Darum: *Fragen Sie bei Ihrer Nutzerbetreuung oder in den Unterlagen des Mailprogramms nach, wie dort die Symbole und Warnungen aussehen. Jene sind meist sehr, sehr einfach zu verstehen. Ähnlich einer Ampel. Doch kennen Sie bereits die Farben und Symbole? Nein. ===== Zusammenfassung ===== Obige Erklärungen zusammengefasst:* **Lektion 1** *informiert uns über ein wichtiges* **Prinzip**, *dem* **public-key Verfahren**. *Es besteht aus einem Schlüsselpaar mit privatem und öffnetlichen Schlüssel (pro Person/Teilnehmer). Den* **privaten Schlüssel** *dürfen nur sie besitzten und diesen müssen sie* **schützen**. *Werden Daten mit privatem Schlüssel verschlüsselt, kann man mit öffentlichem entschlüsseln (und umgekehrt). Die* **zweite Lektion** *erklärt, wie einfach wir das* **Schlüsselpaar erzeugen**. *Der einzige Haken dabei ist: Zuvor müssen wir unseren zukünftigen Schlüsselspeicher im PC durch ein Kennwort schützen. Das passiert nicht von alleine! Also: Bei Registrierungsstelle nachfragen...* **Lektion 3** *sagt, dass eine* **Zertifizierungsstelle (CA)** *auf unseren Antrag hin Angaben von uns bestehend aus* **unserem öffentlichen Schlüssel, E-Mailadresse, Name etc. signiert**. *Die CA muss auch unsere Identität gründlich prüfen. Sie muss uns grundlegende Informationen aushändigen und sicher sein, dass wir diese verstanden haben und einhalten. Wird dem Antrag von uns statt gegeben, erhalten wir* **von der CA** *das sogenannte* **Zertifikat ausgestellt**. *Als letztes werden wir in der* **Lektion 4** *darauf hingewiesen, dass nicht alle Mailprogramme mit Zertifikaten umgehen können (machen Sie sich auf eine Rückfrage wie „Ich kann Ihren Anhang in der E-Mail nicht öffnen“ gefasst). Viel wichtiger ist aber: Sie müssen lernen, erklärt bekommen,* **wie** *sie von nun an* **in ihrem Mailprogramm mit Zertifikaten umgehen**. *Wie sieht eine Warnungen aus, wo lege ich fest, wann signiert wird, wie überprüfe ich eine Signatur und deren Aussteller, die Zertifizierungsstelle? Wenn sie bis hier hin durchgehalten und gelesen haben: Vielen Dank, das war alles! Sollten sie nun tatsächlich mitmachen wollen, signierte E-Mails schreiben/empfangen können, dann müssen sich sich nur noch bei ihrem EDV Dienstleister die grobe Anleitung zu den dort verwendeten Programmen aushändigen lassen. Mit ihrem neuen Hintergrundwissen ist es dann sehr einfach, auch über Lücken in den Anleitungen hinwegsehen zu können: Sie wissen ja nun, was wann wo passiert/passieren muss. ====== Kleine Linksammlung ====== Obwohl es tonnenweise Literatur zu dem Themengebiet gibt, haben wir noch keine Quelle gefunden, welche Anwender in das Thema versändlich, einfach, kurz und kompakt einführt. Das ist auch der Grund für dieses Dokument. Haben Sie etwas tolles zu dem Thema gefunden, sagen Sie uns bitte Bescheid! Eine ganz kurze Liste mit empfehlenswerten Informationen (es gibt sooo viele Informationen im Web): Digitale Signatur nach Wikipedia Grundlagen der Signature, Herausgeber Bundesnetzagentur Tolle Informationen rund um SSL usw., Pierre Feldbusch ~~DISCUSSION~~*