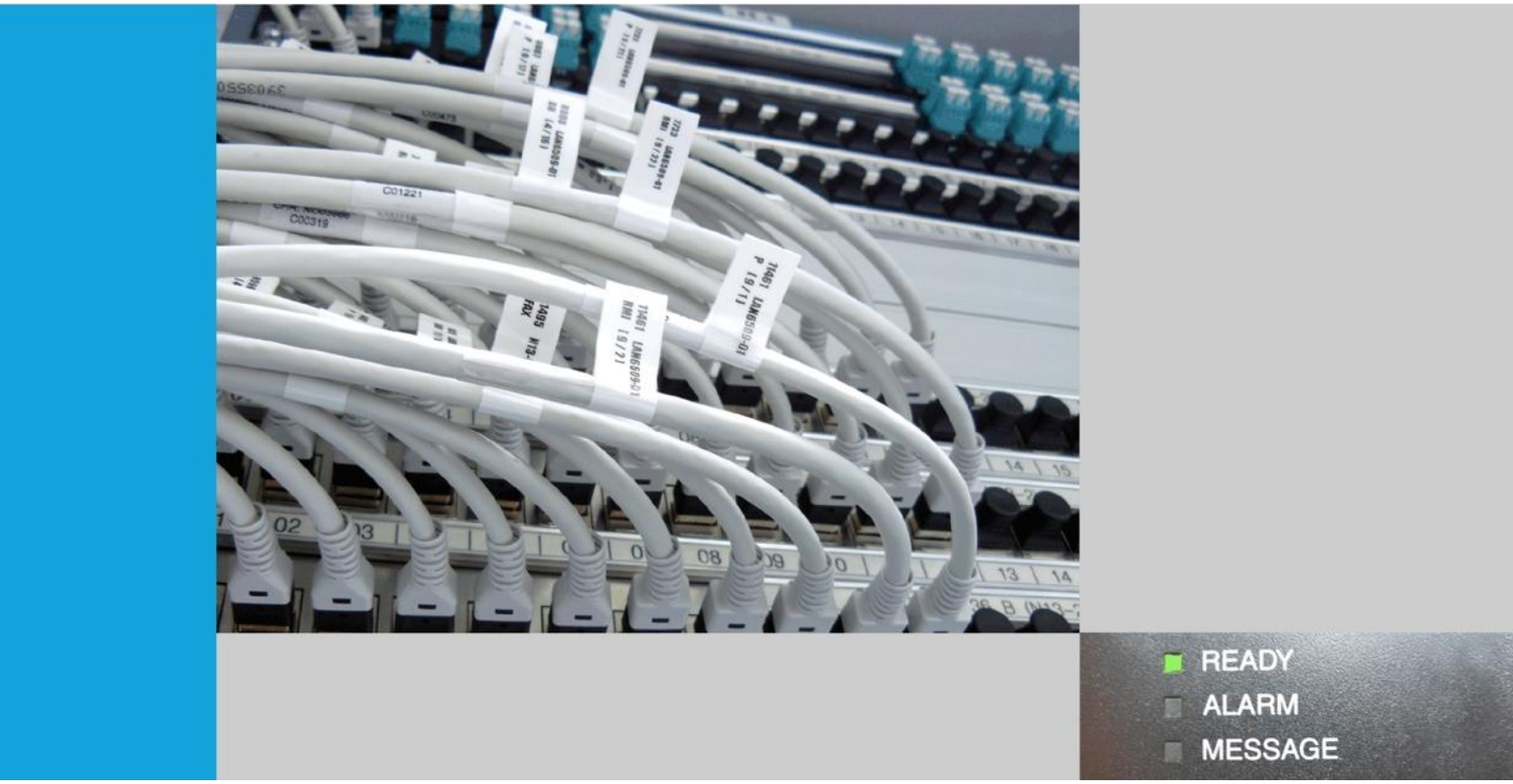

IT-Dienstleistungszentrum des Freistaats Bayern

Handbuch für Nutzer von Zertifikaten der Zertifizierungsstellen (CAs) des Bayerischen Behördennetzes (BYBN) zur Sicherung von E-Mails

Grundlagen

1 Sicherheit durch Verschlüsselung und Signatur

Der Versand von Nachrichten als E-Mail hat gegenüber der herkömmlichen Post einige entscheidende Vorteile: Schnelligkeit, Kostenersparnis, etc. Er birgt jedoch auch eine Reihe von Gefahren in sich, die vom Nutzer auf den ersten Blick nicht wahrgenommen werden:

Eine E-Mail besitzt dieselbe Vertraulichkeit und Sicherheit wie eine Bleistift geschriebene Postkarte, denn sie kann in der elektronischen Welt auf den Datenautobahnen und Zwischenstationen (Servern) ohne größeren Aufwand gelesen und verändert werden. Mit Hilfe von Schnüffelprogrammen kann der durchlaufende Datenverkehr sogar auf ganz bestimmte Inhalte hin analysiert und aussortiert werden. Eine Verlockung, der Sicherheitsdienste und Kriminelle nicht widerstehen können.

Experten sind sich einig, dass ein nicht unwesentlicher Teil des Datenverkehrs im Internet (davon der E-Mail-Verkehr bis zu 100%) systematisch mitgelesen und bearbeitet wird. Genaue Zahlen sind naturgemäß nicht verfügbar, noch dazu, da das Manipulieren elektronischer Daten keine Spuren hinterlässt.

Daraus lässt sich schließen, dass die elektronische Kommunikation ohne Mechanismen zum Schutz der Integrität, der Urheberschaft und der Vertraulichkeit sehr viel verletzlicher für Manipulationen aller Art ist als die traditionelle papiergebundene Kommunikation mit Schriftstück, Unterschrift und Briefumschlag.

Folgende vier Grundanforderungen müssen bei jeder Form von Kommunikation sinnvollerweise erfüllt sein und sind daher bei elektronischer Nachrichtenübermittlung durch geeignete Verfahren sicherzustellen:

Authentizität bedeutet die sichere Bestimmung des Ursprungs einer Nachricht. Der Ursprung kann z.B. eine Person, Institution oder auch ein Rechner sein. Das Versenden von Nachrichten unter falschem Namen kann dadurch aufgedeckt werden.

> ***Beispiel**: Ein Mitarbeiter empfängt eine E-Mail, die als Absenderadresse die seines Chefs trägt. Darin steht, er soll sich sofort in eine andere Stadt zu einer wichtigen Besprechung begeben. Dort angekommen erfährt er, dass er einem Betrüger aufgesessen ist und dass sein Chef diese Mail niemals geschrieben hat.*

Nicht-Abstreitbarkeit des Ursprungs unterbindet die Möglichkeit, dass der Absender seine Urheberschaft an einer Nachricht abstreiten kann.

> ***Beispiel**: Ein Kunde bestellt per E-Mail ein Buch. Nachher gefällt es ihm nicht, und er sagt zur Versandfirma, er habe diese Bestellung gar nicht abgesendet, sondern irgendein anderer in seinem Namen hätte bestellt.*

Nachrichtenintegrität bezeichnet die Unversehrtheit oder Echtheit der Nachricht. Es muss sichergestellt werden, dass der Empfänger es zumindest merkt, wenn an der Nachricht auf dem Übertragungsweg etwas geändert wurde.

> ***Beispiel**: Eine Behörde bestellt per E-Mail 100 neue PCs für ihre Mitarbeiter. Ein Hacker fängt die Mail ab und ändert den Wert 100 in 1000. Die Firma liefert 1000 PCs und die Behörde ist in der Beweisnot, dass sie nicht 1000, sondern 100 PCs bestellt hat.*

Vertraulichkeit heißt, dass unberechtigte Dritte die Nachricht nicht einsehen können. Dies kann sich auf den bloßen Übertragungsweg beschränken, geht aber wie im Falle von E-Mail noch weiter bis zur sicheren Aufbewahrung in der Mailbox des Empfängers (Ende-zu-Ende-Sicherheit).

> ***Beispiel**: Eine Firma A erstellt ein Angebot für ein Produkt und schickt es per E-Mail an den potentiellen Kunden. Die Konkurrenz Firma B liest die Mail mit und*

unterbietet das Angebot der Firma A um wenige Euro. Firma B erhält den Auftrag, und Firma A erleidet einen Verlust in Millionenhöhe.

Die ersten drei Sicherheitsanforderungen werden durch *digitale Signatur* (*elektronische Unterschrift*) erreicht, die letzte durch *Verschlüsselung*. Diesen Zwecken dienen Zertifikate, welche das Trustcenter des bayerischen Behördennetzes (BYBN) den Mitarbeitern der Verwaltung ausstellt.

Auf eine weitere Gefahr sei hier nur kurz verwiesen: Der elektronische Nachrichtenaustausch über E-Mail dient nicht selten Kriminellen und Scharlatanen dazu, Viren, Würmer, etc. zu verbreiten. Zwar verhindern inzwischen z. T. Filter in Mail-Clients den Empfang von verdächtigen Anlagen, dennoch tragen Sie als Absender und/oder Empfänger die Verantwortung dafür, dass Sie keine derartigen Anwendungen verbreiten. Beachten Sie, dass der Versand oder Empfang von verschlüsselten und/oder signierten Mails Ihnen diese Verantwortung nicht abnimmt. Vielmehr besteht durch die Verschlüsselung die Gefahr, dass zentral installierte Viren-Scanner (z.B. am Mail-Server) den Eindringling nicht erkennen können und der Anwender sich durch dieses Medium zu sicher fühlt.

2 Ein Ausflug in die Kryptografie

Zur Verschlüsselung bzw. Signatur verwendet der Rechner hoch komplizierte mathematische Verfahren. Genügte es früher einzelne Buchstaben in den Nachrichten zu vertauschen, um diese unkenntlich zu machen, bedarf es nun immer neuer und besserer Verfahren, um zu verhindern, dass durch die ständig leistungsstärkeren Rechner der Geheimcode aufgedeckt und die Vertraulichkeit einer Nachricht damit verletzt wird.

2.1 Verschlüsselung durch Einsatz kryptografischer Verfahren

Kryptografische Verfahren wurden primär entwickelt, um Informationen zu ver- und entschlüsseln. Aus diesem Grund sollen kryptografische Verfahren auch anhand dieses Einsatzgebietes erläutert werden.

Die Information, die geschützt werden soll, wird nach einem rechnergestützten mathematischen Verfahren in Verbindung mit einem Schlüssel codiert (verschlüsselt) und damit gezielt verschleiert. Was wir beim herkömmlichen Postversand mit einem verschlossenen Kuvert erreichen wollen, geschieht bei der Kryptographie durch Transformation des ursprünglichen Zustands digitaler Zeichen in einen vorübergehend neuen, womit auch der Informationswert vorübergehend entzogen wird.

In Verbindung mit dem passenden Schlüssel lässt sich der ursprüngliche Zustand wiederherstellen, wenn der Schutzbedarf entbehrlich geworden ist.

Es gibt grundsätzlich drei Arten von Verfahren zur Verschlüsselung:

1. **symmetrische** Verfahren,
2. **asymmetrische** Verfahren, auch Public-Key-Kryptosysteme genannt und
3. **hybride** Verfahren (Kombination aus symmetrischen und asymmetrischen Verfahren)

Bei **symmetrischen Verfahren** bezieht sich die Symmetrie alleine auf den Schlüssel. Zum Verschlüsseln und Entschlüsseln einer Information wird der **gleiche** Schlüssel verwendet. Beim Entschlüsseln läuft das gleiche mathematische Verfahren in umgekehrter Reihenfolge unter Nutzung des gleichen Schlüssels ab. Alle Beteiligten eines Kommunikationsprozesses, die sich gegenüber anderen abschirmen wollen und die sich gegenseitig vertrauen, benutzen den gleichen Schlüssel, ähnlich den Bewohnern einer Wohnung, die alle mit dem gleichen Schlüssel die Wohnungstür schließen und öffnen. Die Schwierigkeit und der Aufwand des symmetrischen Krypto-Verfahrens bestehen darin, den gemeinsamen Schlüssel vertraulich auf die Kommunikationspartner zu verteilen und geheim zu halten. Eine Verteilung über das Internet kommt damit nicht in Betracht, denn dann wäre das Problem der sicheren Nachrichtenübertragung nur verlagert auf das Problem der sicheren Schlüsselübertragung. Eine persönliche Übermittlung der Schlüssel ist in großen Anwendergruppen (z.B. dem BYBN) nicht praktikabel.

Ein weiteres Sicherheitsrisiko ergibt sich daraus, dass **ein gemeinsamer** Schlüssel an **mehreren** Orten verwahrt wird und dieser eine Schlüssel die volle Krypto-Funktionalität ermöglicht, also sowohl das **Verschlüsseln** als auch das **Entschlüsseln.** Auch insofern ist also ein symmetrisches Verfahren der gemeinsamen Benutzung eines Wohnungsschlüssels vergleichbar. Wenn einer den Schlüssel verliert oder ein Unbefugter Kenntnis erhält, die ihm eine Kopie des gemeinsamen Schlüssels verschafft, müssen die Schlüssel aller Benutzer ausgetauscht werden.

Die Asymmetrie bei **asymmetrischen Verfahren** bezieht sich hier auf die Benutzung **unterschiedlicher** Schlüssel für die Ver- und Entschlüsselung. Das Konzept der asymmetrischen Verschlüsselung basiert auf einem Schlüssel**paar**. Es besteht aus zwei unterschiedlichen, gleichlangen Schlüsseln für die Ver- und Entschlüsselung:

- dem öffentlichen Schlüssel (**Public Key**) zur Verschlüsselung

- und dem privaten (geheimen) Schlüssel (**Private Key**) zur Entschlüsselung.

Aus dem einem der Schlüssel kann der jeweils andere nicht abgeleitet werden. Auch die digitale Signatur basiert auf der asymmetrischen Verschlüsselungstechnik (siehe unten).

Für jeden Nutzer wird zunächst ein eigenes Schlüsselpaar erzeugt. Der private Schlüssel wird geheim gehalten, und zwar PIN (persönliche Identifikationsnummer)-geschützt auf Festplatte, Diskette oder Chipkarte. Das Medium, auf dem er sich befindet, heißt **Personal Security Environment (PSE).** Der private Schlüssel ist eine lange Folge von Bits, z.B. 1024 Bit lang. Er muss dem Benutzer nicht persönlich bekannt sein im Sinne von Auswendiglernen. Wichtig ist nur, dass nur ein bestimmter Benutzer den Schlüssel verwenden kann. Dies sichert man durch das Prinzip „**Besitz + Wissen**“: nur wer die PSE besitzt und die dazugehörige PIN weiß, kann den privaten Schlüssel aktivieren (vgl. Benutzung einer Euroscheckkarte zum Geldabheben).

Der öffentliche Schlüssel wird in Verbindung mit der digitalen Beglaubigung, dass er zu einer ganz bestimmten Person gehört (Authentizität des öffentlichen Schlüssels), allgemein bekannt gegeben (z.B. über das Internet). Der öffentliche Schlüssel ist also vergleichbar mit einer Telefonnummer, die jeder wissen darf. An ihm ist nichts Geheimes.

Der Aufwand und das Risiko des geheimen Schlüsselaustausches, der beim symmetrischen Verfahren erforderlich ist, entfallen damit. Absender und Empfänger müssen sich vorher nie getroffen haben.

Der private Schlüssel verbleibt beim Besitzer, muss aber streng vor unbefugtem Zugriff geschützt werden. Der öffentliche Schlüssel kann beliebig verteilt werden, da er nur zum Verschlüsseln benutzt wird und mit ihm verschlüsselte Nachrichten nur mit dem privaten Schlüssel entschlüsselt und damit gelesen werden können. Die Verteilung geschieht entweder auf direktem Weg (d.h. der eine schickt irgendwann mal dem anderen seinen öffentlichen Schlüssel zu) oder über zentrale Schlüsselverzeichnisse (**Key-Server)**, auf die jeder zugreifen kann.

Durch die so genannten **Hybridverfahren** werden die Vorteile beider Verfahren vereinigt. Mit dem schnellen symmetrischen Verfahren werden die kompletten Daten (Text, Sprache, Videokonferenzdaten) verschlüsselt, mit dem langsamen asymmetrischen Verfahren wird nur der symmetrische Schlüssel verschlüsselt und damit der sichere und unkomplizierte Schlüsselaustausch realisiert. Moderne Sicherheitsprodukte setzen also i.d.R. symmetrische und asymmetrische Verschlüsselungsverfahren nebeneinander ein.

Für jede Nachricht erzeugt der Absender einen Schlüssel (**symmetrischer Sitzungsschlüssel**, **Session Key**) mit Hilfe eines Zufallszahlengenerators. Die Originalnachricht, die geschützt werden soll, wird unter Benutzung des Session Key symmetrisch verschlüsselt. Speziell für den sicheren Schlüsselaustausch wird daraufhin nur der Session Key (normalerweise sehr viel kürzer als die Nachricht) mit dem langsameren asymmetrischen Verfahren und mit Hilfe des öffentlichen Schlüssels des Empfängers verschlüsselt.

Beides zusammen, die symmetrisch verschlüsselte Information und der mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselte Session Key können nun gemeinsam über das öffentliche Netz zum Empfänger transportiert werden. Nur der Empfänger kann den Session Key mit seinem privaten Schlüssel entschlüsseln und daraufhin durch Entschlüsselung des Nachrichtenteils die Originaldaten rekonstruieren.

Wenn das Schlüsselpaar nicht zusammengehört, weil der Empfänger unbefugt ist oder nach der Verschlüsselung ein neues Schlüsselpaar für den Empfänger generiert wurde, kann das Ergebnis der Entschlüsselung nicht interpretiert werden. Im zweiten Fall muss der Empfänger die Verschlüsselung vom Sender nochmals veranlassen.

2.2 Elektronische Signatur

Wenn der **Absender** eine Nachricht **signiert**, wendet er folgendes Verfahren an:

Aus der Nachricht, die elektronisch unterschrieben werden soll, wird ein auf mindestens 128 Bit komprimierter, nicht umkehrbarer Wert errechnet (kryptografische Hash-Summe, sog. digitaler Fingerabdruck oder MAC = Message Authentification Code). Die typische Länge dieses Komprimats (im Folgenden = „Hash 1“ genannt) war bisher 128 Bit, neuerdings zwischen 128 und 256 Bit.

Dieses Komprimat wird mit dem privaten Signierschlüssel des Signierenden nach dem asymmetrischen Verfahren verschlüsselt (= signiert). Das Ergebnis wird als **digitale Signatur** bezeichnet. Es wird mit der ursprünglichen Nachricht, die zusätzlich verschlüsselt sein kann, versandt. Der Signierende versieht die Nachricht also mit einem Merkmal (privater Schlüssel), über das nur er verfügt, genauso wie normalerweise nur eine bestimmte Person eine bestimmte handschriftliche Unterschrift erzeugen kann.

Wenn der **Empfänger** die Signatur **verifiziert**, wendet er folgendes Verfahren an:

Das mitgelieferte verschlüsselte Komprimat Hash 1 wird mit dem öffentlichen Schlüssel des Signierenden entschlüsselt und man erhält wieder das ursprüngliche unverschlüsselte Komprimat Hash 1. Danach wird aus dem ggf. entschlüsselten Nachrichtentext mit dem gleichen Hash-Algorithmus ein neues Komprimat „Hash 2“ gebildet.

Stimmen Hash 1 und Hash 2 überein, sind die empfangenen Daten unverfälscht und der für den Inhalt verantwortliche Absender ist identifiziert, ohne sich auf die Absenderangaben der E-Mail verlassen zu müssen. Bei Nichtübereinstimmung sind entweder die Daten gefälscht oder das Schlüsselpaar (öffentlicher und privater Schlüssel) gehört nicht zusammen. Unterschreiben kann nur der Besitzer des privaten Schlüssels, die Unterschrift überprüfen (Verifizierung der Authentizität des Absenders) kann jeder, der die Nachricht liest und den zugehörigen öffentlichen Schlüssel hat.

2.3 Ablauf von Verschlüsselung und Signatur

Die folgende Abbildung stellt nochmals den gesamten Ablauf zum Versenden und Empfangen einer verschlüsselten und signierten E-Mail dar. Die Verschlüsselung erfolgt mittels des oben beschriebenen Hybridverfahrens.

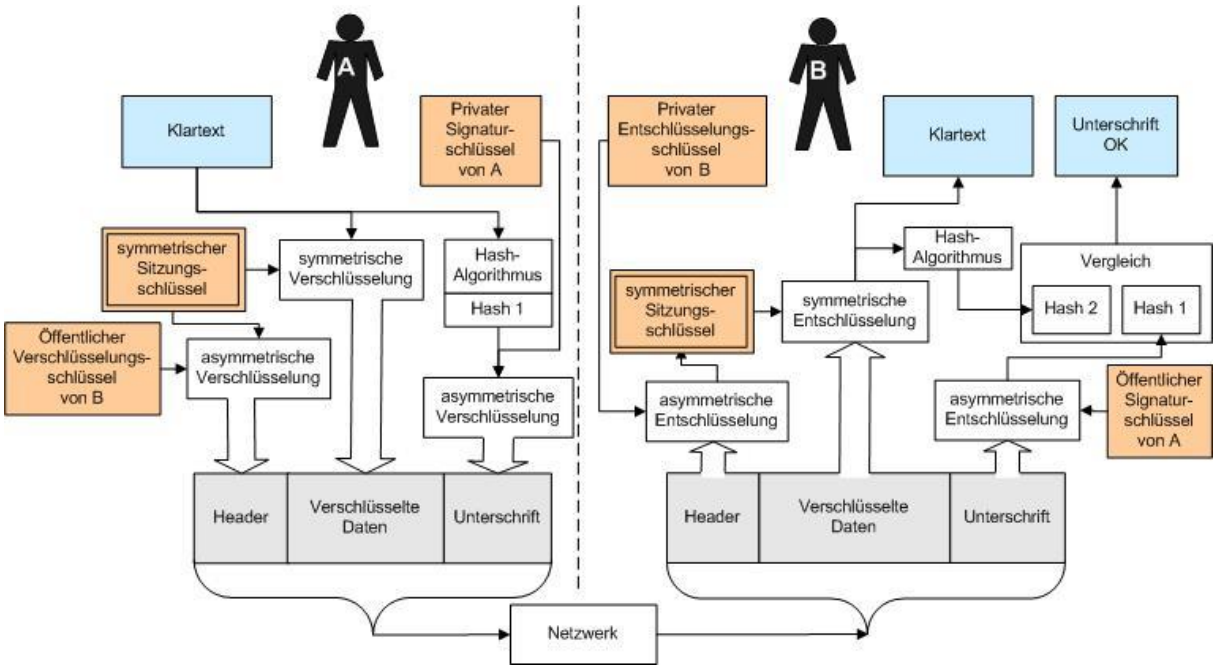

Abbildung 1: Ablauf hybride Verschlüsselung und digitale Signatur

2.4 Zertifikat

Im vorherigen Abschnitt wurden asymmetrische kryptografische Verfahren zur Sicherung der elektronischen Kommunikation erläutert. Diese Verfahren setzen private und öffentliche

Schlüssel ein, um Verschlüsselung und digitale Signatur zu realisieren. Ein wesentlicher Punkt ist jedoch die Glaubwürdigkeit der in diesen Verfahren verwendeten (öffentlichen) Schlüssel:

Ein bestimmter öffentlicher Schlüssel muss zweifelsfrei einem Teilnehmer zugeordnet werden können.

Hier kommen die **Zertifikate** und **Zertifizierungsstellen** ins Spiel. Ein digitales Zertifikat besteht im wesentlichen aus einem weltweit eindeutigen Namen (**Distinguished Name**, DN) eines Teilnehmers und dessen öffentlichen Schlüssel und stellt eine Verbindung zwischen öffentlichem Schlüssel und Teilnehmer (End-Entität) dar. Sie werden üblicherweise auf öffentlich zugänglichen Verzeichnissen abrufbereit gehalten.

Es muss nun sichergestellt sein, dass nicht ein Angreifer *X* auf dem Übertragungsweg den öffentlichen Schlüssel im Zertifikat des Kommunikationspartners gegen seinen eigenen austauscht („Man-in-the-Middle-Attack“).

Dann würde der Absender, ohne es zu wissen oder zu wollen, eine für den Empfänger vertrauliche Nachricht erzeugen, die aber nicht vom Empfänger, sondern vom Angreifer *X* gelesen werden kann, und zwar *nur* von *X*. Die Vertraulichkeit wäre damit trotz asymmetrischer Verschlüsselung nicht mehr gewährleistet.

Damit dies nicht passieren kann, gibt es eine zentrale Instanz, die mit **CA**, **Trustcenter** oder **Zertifizierungsstelle** bezeichnet wird, und die jedes Zertifikat digital mit ihrem und nur ihr bekannten privaten Schlüssel signiert. Man kann also die Unversehrtheit des angelieferten Zertifikats mit Hilfe des bekannten öffentlichen Schlüssels der CA, welche die Zertifikate ausgestellt hat, verifizieren. Diesen öffentlichen CA-Schlüssel muss jeder Teilnehmer irgendwann einmal auf sicherem Wege erhalten, üblicherweise gleich bei der Installation der Sicherheitssoftware.

Die folgende Abbildung zeigt ein Zertifikat, das nach dem weltweit etablierten Standard X.509v3 aufgebaut ist:

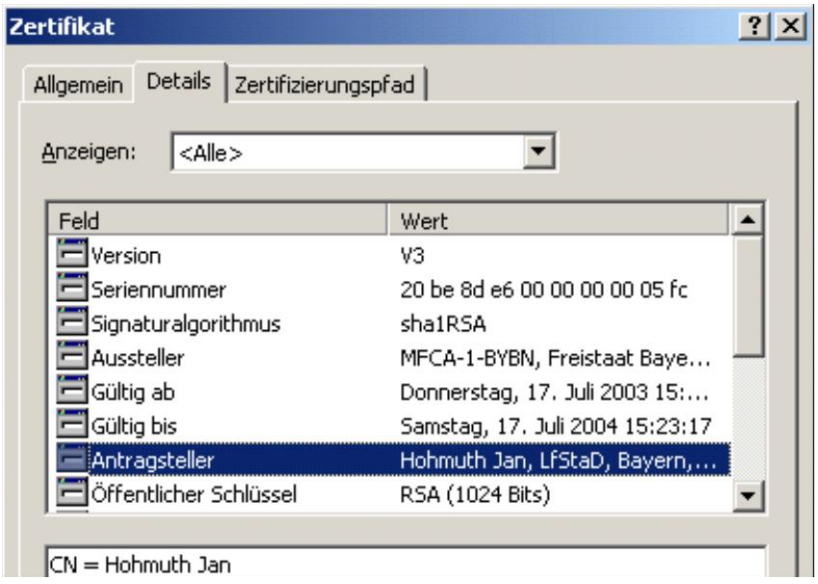

Abbildung 2: Ansicht eines Zertifikates unter Windows

Ein Zertifikat ist also eine sichere Verbindung von Name und öffentlichem Schlüssel. Durch die digitale Signatur der CA ist das Zertifikat integritätsgeschützt, d.h. man würde bei einer oben beschriebenen „Man-in-the-Middle-Attack“ merken, dass unterwegs etwas verfälscht wurde.

Die Entscheidung für ein zertifikatsbasiertes Sicherheitssystem erfordert stets die Implementierung einer sog. **Public-Key-Infrastruktur (PKI).** Eine solche PKI besteht aus:

- technischen Komponenten (Hardware und Software), welche die Generierung und Verwaltung von Schlüsseln und Zertifikaten ermöglichen;
- Teilnehmern, die mittels eines asymmetrischen Verfahrens sicher miteinander kommunizieren wollen;
- einem Organisationskonzept, das den gesamten Prozess angefangen von der Antragstellung auf ein Zertifikat über die Zertifikatserstellung und Schlüsselverteilung bis hin zum Zertifikatswiderruf umfasst. Der weitaus größere Teil der Projektarbeit an einer PKI besteht in der Erstellung und Installierung dieses Konzepts.

Die Teilnehmer vertrauen also darauf, dass ein von der CA unterschriebenes Zertifikat eines beliebigen Zertifikatsinhabers, diesem auch zweifelsfrei zugeordnet werden kann.

3 Zertifikatsmanagement

Im Bereich des BYBN werden Zertifikate getrennt für Verschlüsselung und Signatur eingesetzt. Das heißt, dass sie mit Ihrem Antrag auf Zertifizierung in der Regel zwei Zertifikate beantragen müssen und erhalten, von denen eines für die Verschlüsselung und das zweite für das Signieren von E-Mails vorgesehen ist.

3.1 Ausstellung von Zertifikaten

Die Zertifikate werden zentral vom IT-DLZ (im Landesamt für Digitalisierung, Breitband und Vermessung) zur Verfügung gestellt.

Zur Sicherung von elektronischen Nachrichten (E-Mails) werden diese Zertifikate im Normalfall in einem E-Mail Client eingesetzt. PKI taugliche E-Mail Clients sind z.B. MS Outlook ab 2000, MS Outlook Express ab Version 5.5 sowie Mozilla ab der Version 1.2.1..

Das Ausstellen von Zertifikaten über das IT-DLZ geschieht wie folgt:

Sie lassen sich über eine Registrierungsstelle (RA), die in Ihrer Behörde eingerichtet wurde, als Teilnehmer registrieren.

Von der Registrierungsstelle erhalten Sie danach einen Registrierungsbrief mit folgenden wichtigen Informationen:

- URL zum Antragsverfahren „PRIME“ – hier müssen Sie sich mit den nachfolgenden Daten anmelden, um Ihre Zertifikate beantragen und verwalten zu können
- Benutzername – entspricht Ihrer E-Mail Adresse
- Passwort – wurde automatisch erstellt und entspricht einem Zufallswert bestehend aus Großbuchstaben, Kleinbuchstaben, Ziffern
- Sperr-PIN – wurde automatisch generiert und entspricht einem Zufallswert bestehend aus Ziffern
- URL zum Informationsangebot PKI – Hier finden Sie diverse Anleitungen und Hinweise, u.a. auch ein Benutzerhandbuch für das Zertifikatsverwaltungssystem icms.

Im PRIME-Benutzerhandbuch wird die Handhabung des Zertifikatsverwaltungssystems PRIME (inkl. Zertifikatsantragsverfahren) erläutert.

Ihre beantragten Zertifikate und ggf. privaten Schlüssel erhalten Sie per E-Mail. Speichern Sie die Anlagen der E-Mail in einem nur Ihnen zugänglichen Bereich Ihrer Festplatte bzw. Netzwerkressource.

Über das Zertifikatsverwaltungssystem PRIME können Sie für jeden privaten Schlüssel, den Sie per E-Mail erhalten haben, die sog. Transport-PIN abfragen. Diese PIN benötigen Sie, um das erhaltene Schlüsselmaterial auf Ihrem Rechner installieren und in Betrieb nehmen zu können.

Für die Zertifikatsbeantragung ist eine Identifikation Ihrer Person erforderlich, um die Zuordnung einer Person zu ihrem Schlüssel zu dokumentieren. Diese Identifikation wird von der in Ihrer Behörde eingerichteten Registrierungsstelle vorgenommen.

Falls es in Ihrer Behörde keine Registrierungsstelle gibt, muss diese zunächst eingerichtet werden. Für Fragen und Beratung steht Ihnen das IT-DLZ zur Verfügung.

Die erzeugten Zertifikate für Sichere E-Mail (S/MIME) sind i.d.R. drei Jahre gültig und werden dann automatisch verlängert, sofern in der Zwischenzeit keine Zertifikatsrückruf (Sperrung) erfolgt ist.

3.2 Rückruf

Zertifikate binden nicht nur den öffentlichen Schlüssel an eine Person, sondern bestätigen insbesondere auch die Zugehörigkeit eines Mitarbeiters zu einer Dienststelle. Wird diese Zugehörigkeit durch Personalmaßnahmen wie Versetzung, Beurlaubung, Abordnung, Ausscheiden aus dem Dienst aufgehoben, so ist ein erteiltes, noch gültiges Zertifikat zurückzurufen.

Ein Rückruf ist ferner zu veranlassen, wenn:

- der Verdacht besteht, dass der private Entschlüsselungs- oder Signaturschlüssel kompromittiert wurde (z.B. durch Bekannt werden der PIN),
- die Zertifikate unrichtige Angaben enthalten (auch Namensänderungen, z.B. durch Heirat)

Für einen Rückruf gibt es drei Möglichkeiten:

- Sie beantragen den Rückruf selbst über der Zertifikatsverwaltungssystem icms,
- Sie wenden sich an Ihre Registrierungsstelle, die den Rückruf beantragt oder
- Sie wenden sich an den Servicedesk im IT-DLZ, welches den Rückruf-Antrag entgegen nimmt, erfasst und weiterleitet.

4 Vertrauenswürdigkeit

Der Vertrauenswürdigkeit der verwendeten Zertifikate kommt eine besondere Bedeutung im praktischen Betrieb zu. Letztendlich möchte man sicher gehen, dass der zur Entschlüsselung benötigte Schlüssel auch tatsächlich im Besitz des Empfängers der Nachricht ist, und eine digitale Unterschrift auch tatsächlich vom Absender der Nachricht stammt.

4.1 Vertrauen in das Trustcenter

Das Landesamt für Digitalisierung,Breitband und Vermessung stellt in seiner Eigenschaft als Trustcenter Zertifikate aus, welche für den dienstlichen Gebrauch von allen Behörden als vertrauenswürdig angesehen werden.

Es lassen sich grundsätzlich drei verschiedene Klassen von Zertifikaten definieren:

Zertifikate des eigenen Trustcenters:

Durch den Import des eigenen Zertifikates bzw. durch vom Betriebssystem bereitgestellte Mechanismen werden die Zertifikate des eigenen Trustcenters von den Mail-Clients immer als vertrauenswürdig eingestuft.

Zertifikate von Trustcentern der PCA-1-Verwaltung:

In der PCA-1-Verwaltung hat sich die Bundesverwaltung mit den Verwaltungen der Bundesländer zusammengeschlossen. Ziel dieser PCA-1-Verwaltung ist die gegenseitige Anerkennung und Bereitstellung von Zertifikaten. Auch Bayern ist Mitglied dieser PCA-1-Verwaltung, deren Trustcenter als Root (Wurzel) für unser Trustcenter gilt.

Zertifikate von anderen Trustcentern der PCA-1-Verwaltung werden von den Mail-Clients automatisch als vertrauenswürdig eingestuft.

Zertifikate von sonstigen Trustcentern

Zertifikate dieser Anbieter werden von den Mail-Clients nicht automatisch als vertrauenswürdig eingestuft. In der Regel muss dies explizit durch den Benutzer geschehen.

Es obliegt ferner dem Benutzer sich von der Vertrauenswürdigkeit des Trustcenters zu überzeugen.

4.2 Rechtsgültigkeit einer Digitalen Signatur

Um die Rechtsgültigkeit bei der elektronischen Signatur zu erreichen, wurde 1997 das Signaturgesetz verabschiedet. Im Jahr 2001 erfolgte eine Anpassung des Gesetzes an die 1999 von der EU erlassene Richtlinie über „gemeinschaftliche Rahmenrichtlinien für die elektronische Signatur“.

Die vom Trustcenter des BYBN in Übereinstimmung mit der PCA-1-Verwaltung erstellten Zertifikate repräsentieren nach dem Signaturgesetz eine fortgeschrittene digitale Signatur, die jedoch nicht die gleiche Rechtsgültigkeit wie eine qualifizierte elektronische Signatur entfaltet. D.h. diese Zertifikate würden z.B. bei einem Rechtsstreit nicht anerkannt werden.