universität wien

Diplomarbeit

Titel der Diplomarbeit

„State of the Art und Trends der digitalen Signatur“

Verfasser

Qais Ayni

angestrebter akademischer Grad

Magister.rer.soc.oec

Wien, 2008

Studienkennzahl lt. Studienbuchblatt:	A 175
Studienrichtung lt. Studienbuchblatt:	Diplomstudium Wirtschaftsinformatik
Betreuerin:	ao. Univ.-Prof. Dr. Christine Strauß

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

Vorwort

Die Unterschrift beziehungsweise elektronische Signatur begeleitet uns durch das ganze Leben. Kein Vertrag, keine Geldüberweisung, keine rechtsverbindliche Willenserklärung irgendeiner Art ist ohne den Nachweis der eigenen Identität gültig.

Die vorliegende Arbeit soll einen Einblick in digitale Signaturen, ihre rechtlichen und technische Grundlagen geben. Insbesondere gehe ich auf die mobilen elektronischen Signaturen ein. In diesem Zusammenhang werden auch die verschiedenen Systeme der Mobilkommunikation (GSM-Dienste) behandelt. Weiters wird anhand einiger Anwendungsbeispiele gezeigt, dass mobile elektronische Signaturen heutzutage eine sehr große Rolle spielen. Das Ziel ist es, die Brücke zwischen der mobilen Kommunikation und elektronischen Signaturen zu schlagen und diese in einem globalen Netz zu vereinen.

In diesem Zusammenhang möchte ich mich ganz besonders bei Fr. Professor Dr. Christine Strauß bedanken, da sie diese Arbeit mit viel Geduld und Verständnis betreut hat. Weiters bei meinen Freunden, ebenso ganz herzlich bei meiner ganzen Familie, die mich unterstützt hat.

Ganz besonderen Dank schulde ich meiner Schwester Robia Ayni, die mich sehr motiviert hat und mir zur Seite gestanden ist und damit zum erfolgreichen Abschluss dieser Arbeit beigetragen hat.

Ich habe mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit eingeholt. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir.

1. Einführung

1.1 Bedeutung der Elektronischen Signatur

Der Fortschritt der Kommunikations- und Informationstechnik eröffnet neue Möglichkeiten und Perspektiven im Bereich des Informationsaustausches und der wirtschaftlichen Betätigung. Bestellungen von Waren, Zahlungsaufträge an Banken, Gesuche oder Einsprüche bei öffentlichen Ämtern, die Übersendung sensibler Daten auf dem medizinischen Sektor und eine Menge weiterer Kommunikationsbeziehungen sowohl in formfreien als auch in formgebundenen öffentlich-rechtlichen Bereichen, die vor einigen Jahren mittels Papier erledigt wurden, werden heutzutage großteils auf elektronischem Wege erfüllt. Hierzu zählt man auch die Dokumentation von Daten, wie etwa in Bezug auf Produkthaftung oder im medizinischen Bereich. Den neuesten Trend stellen multimediale Anwendungen dar.

Elektronische Signaturen[1] dienen nicht zur Geheimhaltung von Informationen und schützen das signierte Dokument auch nicht vor Veränderungen. Nach der bis 2001 geltenden Rechtslage konnte sich ein Unternehmen im Streitfall nur dann beruhigt auf die Beweiskraft seiner Dokumente verlassen, wenn diese in Papier, und mit einer traditionellen Unterschrift versehen, vorlagen.

Dies führt bereits seit Jahren zu Szenarien, in denen für den Geschäftsverkehr relevante Dokumente zwar mit EDV erstellt werden, dann aber ausgedruckt, unterschrieben und auf dem normalen Postweg versandt werden. Dabei ist es prinzipiell unerheblich, ob es um einen großen oder kleinen Auftrag geht, und ob es sich bei dem Dokument um einen Brief, einen Antrag/Auftrag, einen Vertrag, eine Auftragsbestätigung, einen Lieferschein oder eine Rechnung/Mahnung handelt. Bei dem Empfänger durchläuft dieser Brief wiederum einen mehr oder weniger aufwändigen Posteingangsprozess.

Natürlich ist die Ineffizienz dieses Verfahrens seit langem erkannt und über verschiedene Ansätze (z.B. Signaturgesetz von 1997, EDI-Verfahren[2]) ist eine Lösung versucht worden. Juristische Regelungen müssen jedoch weitgehend unabhängig von technologischen Trends Bestand und Gültigkeit haben.

[1] vgl. http://www.ecin.de/sicherheit/bedeutung-signatur/index-2.html

[2] vgl. http://www.bulmc.de/Kompetenzen/Esig/downloads/Bedeutung-E-Sig.pdf

Die Nachfrage nach einer digitalen Lösung ist sehr groß, da sich die Dokumentationserstellung, Archivierung und Kommunikation auf Grundlage digitaler Daten angepasst hat und sich immer mehr ausweitet. Die digitale Lösung sollte die Anforderung einer offenen Kommunikation erfüllen, was bedeutet, die Teilnehmer müssen sich nicht kennen, es muss jedoch eine Gewährleistung gegeben sein, sicher auf den Urheber schließen zu können. Dabei darf nicht außer Acht gelassen werden, dass die Daten vor unbemerkter Veränderung geschützt sein müssen. Alle diese Anforderungen werden durch die gesetzliche „qualifizierte elektronische Signatur“ erfüllt[3].

1.2 Anforderungen an elektronische Signaturen

Aus den Anforderungen an ein zu signierendes elektronisches Dokument ergeben sich die Anforderungen an elektronische Signaturen.
Die Identifikation, Echtheit, der richtige und vollständige Abschluss und die Warnung (durch die Notwendigkeit, dass eine Unterschrift geleistet werden, muss wird dem Verfasser die rechtliche Bedeutung des Dokuments angezeigt) werden als Anforderungen an die elektronische Signatur gestellt.

Die Signatur muss die Identität des Unterzeichners zweifelsfrei bestätigen. Sie darf nicht wieder verwendbar und nur zusammen mit dem Originaldokument gültig sein. Ein signiertes Dokument darf nicht mehr veränderbar sein, bzw. eine nachträgliche Veränderung muss erkennbar sein. Eine Signatur darf nicht zurückgewiesen werden können, d.h. der Unterzeichner eines Dokuments darf das Unterzeichnen des Dokuments nicht im Nachhinein erfolgreich abstreiten können.

Die gestellten Anforderungen sind nicht leicht zu erfüllen, da durch die spezifischen Eigenschaften digital repräsentierter Informationen Angriffe auf Signaturen, wie beispielsweise das Herausfiltern der Unterschrift und deren Verbindung mit einem anderen Dokument, wesentlich einfacher durchzuführen sind als bei handschriftlichen Unterschriften auf Papier. Der Einsatz digitaler Techniken zur Unterschriftenherstellung eröffnet andererseits aber auch Vorteile gegenüber handschriftlichen Signaturen. So kann durch die Verwendung von Verschlüsselungstechniken zusätzlich der Inhalt eines Dokuments geheim gehalten werden und durch die message-authentication codes bzw.

[3] vgl. http://www.infotech-systems.de/infotech/signatur.htm

kryptografische Hashfunktionen ist ein höheres Maß an Sicherheit vor unbemerkter nachträglicher Manipulation erreichbar.

Durch die Verwendung von Zeitstempeln ist es weiterhin einfach möglich, die Gültigkeit einer Signatur auf einen festgelegten Zeitraum zu begrenzen. Da digitale Signaturen mithilfe kryptografischer Verfahren erstellt werden, können die verwendeten Schlüssel bei einer vertrauenswürdigen Instanz hinterlegt werden, sodass der Urheber einer Unterschrift durch eine einfache Anfrage bei dieser Instanz ermittelbar ist.

1.3 Unterschrift auf Papier und elektronische Signatur

Auf dem Papier ist die Unterschrift ein eindeutiges Kennzeichnen einer Willenserklärung, stets einmalig und untrennbar mit der Person verbunden, die sie leistet und stellt zugleich eine Bestätigung dafür dar, dass der Unterzeichner mit dem Inhalt des Dokumentes einverstanden ist. Unter dem Begriff der elektronischen Signatur wird in der Regel nicht nur die erzeugte Signatur verstanden - es werden auch die dazugehörigen Verschlüsselungsverfahren einbezogen. Verwirrend wirken ähnlich klingende Begriffe.

Die Bezeichnung „digitale Signatur“ entstammt einem mittlerweile stark überarbeiteten Gesetz aus dem Jahr 1997. 1999 wurde in einer Richtlinie der Europäischen Union der Rechtsbegriff der „elektronische Signatur" eingeführt, der technisch weniger limitierend sein soll und auch im Signaturgesetz von 2001 (SigG2O01) verankert wurde. Im Gesetz von 2001 finden sich drei Ausprägungen von elektronischen Signaturen wieder: "einfache", "fortgeschrittene" sowie qualifizierte". Juristische Festlegungen existieren für Signaturen die als „qualifiziert" eingestuft werden. Anbieter der letztgenannten Signaturform können sich wiederum einem zeit- und kostenaufwändigen Akkreditierungsverfahren durch die Regulierungsbehörde für Telekommunikation und Post (RegTP[4]) unterwerfen.

Die einfache elektronische Signatur umfasst alle Daten, die anderen elektronischen Daten beigefügt werden und zur Authentifizierung dienen. Sie stellt die einfachste Form der Signatur dar, besitzt aber keinerlei Authentifizierungs- und Integritätsfunktion.

[4] siehe http://www.bundesnetzagentur.de/enid/2.html

Eine fortgeschrittene Signatur muss mit Mitteln erzeugt werden, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle hat, sie muss ausschließlich dem Unterzeichner zugeordnet sein und dadurch seine Identifizierung ermöglichen. Das am 10. Januar 2005 in Kraft getretene erste Gesetz zur Änderung des Signaturgesetzes (1.SignAndCl) stellt dies ebenso klar wie in §2 Abs. 9[5] wie die Tatsache, dass fortgeschrittene Signaturen nicht an Zertifikate gebunden sein müssen. Außerdem soll sie mit den Daten, auf die sie sich bezieht, verknüpft sein, damit eine nachträgliche Veränderung der Daten erkannt werden kann. Im Rahmen der freien Beweiswürdigung gewährleisten diese Merkmale Authentizität und Integrität.

Unter den fortgeschrittenen elektronischen Signaturen befinden sich eine Reihe technisch anspruchsvoller Verfahren. Eine Prüfung der technologischen Qualität durch unabhängige Dritte ist lediglich für die Anerkennung als qualifizierte Signatur vorab erforderlich. Bei fortgeschrittenen Signaturen erfolgt diese Prüfung erst im Falle eines Rechtsstreites. Ein Jurist wird die Beweisqualität des rechtsgeschäftlichen Handelns zum einen von der technischen Qualität und zum anderen von den Rahmenbedingungen ihres Einsatzes abhängig machen. Hierbei ist darauf zu achten, dass man nicht die Begriffe "Qualität" und "qualifiziert" zusammenfassen kann. Während der Beweis über eine herkömmliche Urkunde durch physische Vorlage des Originals auf dem Richtertisch angetreten wird, bestimmt der neu eingefügte §371 [6] der Zivilprozessordnung (ZPO) für elektronische Dokumente, dass der Beweisantritt die Vorlegung oder Übermittlung der Datei voraussetzt. Das heißt auch, dass die einfache Vorlage des Dokumentes nicht genügt - sein Inhalt muss auch prüfbar sein.

Nach Ansicht von Dr. Johann Bizer von der Universität Frankfurt sind fortgeschrittene elektronische Signaturen in Anwendungsfeldern, wo Interaktion, soziale Kontrollmechanismen oder geschlossene Benutzergruppen vorhanden sind, ausreichend. Ein Beispiel für eine solche geschlossene Benutzergruppe findet sich im Klinikum Ingolstadt[7].

[5] siehe Anhang S. 88
[6] vgl. http://www.jusline.at/371_ZPO.html
[7] siehe http://www.iuk.fraunhofer.de/summit-42/downloads/IuK-Summit-42_Kleemann.pdf?PHPSESSID=efb290bc07

2. Grundlegende Richtlinien

2.1 Signaturrichtlinie

Die Grundlage für die Anerkennung elektronischer Signaturen im österreichischen Recht wurde durch das Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl I 1999/190 geschaffen. Österreich ist damit das erste Land, das die Signaturrichtlinie [8] 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen umgesetzt hat[9].
In Deutschland wurde das Gesetz zur digitalen Signatur (SigG.) als Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste am 13.06.97 vom deutschen Bundestag beschlossen und trat am 1. Aug. 1997 in Kraft.

2.1.1 Sicherheit digitaler Signaturen

Die Basis für die Sicherheit stellt das SigG mit der Signaturverordnung dar. Die staatliche Aufsichtsstelle Telecom-Conroll-Commission und A-Sit (Bestätigungsstelle) überprüfen, ob die Anforderungen des SigG eingehalten werden oder nicht. Dabei legt man großen Wert auf die verwendeten technischen Komponenten und die Verfahren, die für die Herstellung von sicheren Signaturen verwendet wurden.

2.1.2 Signaturrichtlinie der EU

Die im April 1999 verabschiedeten EU-Richtlinien sehen weit weniger restriktive Regelungen vor. Das Ziel der Richtlinien ist es, eine grenzüberschreitende Anerkennung von digitalen Signaturen und Zertifikaten sicherzustellen und einen harmonisierten rechtlichen Rahmen für die Europäische Gemeinschaft zu schaffen.
Die Richtlinien enthalten nur allgemeine Anforderungen an den Zertifizierungsdienst[10].
Den Mitgliedsstaaten ist es freigestellt, durch Akkreditierungsregelungen auf freiwilliger Basis ein höheres Sicherheitsniveau anzustreben.

Die europäischen Signatur-Richtlinien zielen in erster Linie auf ein Haftungskonzept ab. Damit will man die Vertrauensbildung zwischen Verbrauchern und Unternehmen fördern. Diese Haftungsregelung, die vorgeschlagen wurde, besagt, dass der

[8] vgl. http://www.signatur.rtr.at/de/legal/directive.html
[9] vgl. http://www.signatur.rtr.at/de/legal/index.html, 28.08.2006
[10] schwaches Sicherheitsniveau

Dienstanbieter für die inhaltliche Richtigkeit des Zertifikats sowie für die korrekte Funktionalität seiner Signaturverfahren haftet. Da digitale Signaturen mit herkömmlichen Unterschriften rechtlich gleichgestellt sind, sind die Rechtsfolgen für die Verordnung von digitalen Signaturen geklärt.

2.1.3 Signaturgesetz in Österreich

Ihre Grundlage findet das Signaturgesetz[11] mit seiner Verordnung im europäischen Recht. Die Details und was genau im österreichischen Signaturgesetz und in der Signaturverordnung geregelt wird, ist auf der Homepage der Aufsichtsstelle aufrufbar (www.rtr.atwww.rtr.at; www.tkc.at).

Folgende Aufgaben werden durch das österreichische Signaturgesetz geregelt:

- Erstellung und Verwendung der elektronischen Signaturen
- Rechtswirkungen elektronische Signaturen
- Aufgaben und Tätigkeiten von Zertifizierungsdienstanbietern und die staatliche Aufsicht durch die Telekom-Control-Kommission

§ 3 SigG[12] ist die Kernbestimmung für die rechtliche Anerkennung elektronischer Signaturen. Gemäß dieser technologieneutralen Bestimmung können im Rechts- und Geschäftsverkehr Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden. Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdienstanbieter ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 SigG[13] erstellt wurde.

So genannte "sichere elektronische Signaturen" sind sogar eigenhändigen Unterschriften gleichgestellt und erfüllen damit (mit einigen, in § 4 SigG[14] genannten Ausnahmen) das rechtliche Erfordernis der "Schriftform".

[11] vgl. http://www.signatur.rtr.at/de/legal/overview.html, 28.08.2006
[12] siehe Anhang Seite 89
[13] siehe Anhang Seite 95
[14] siehe Anhang Seite 89

Was ein qualifiziertes Zertifikat ist und welche Pflichten die Zertifizierungsdienstanbieter treffen, die solche Zertifikate ausstellen, finden Sie in den §§ 5 und 7 SigG[15].

Die Aufnahme und Ausübung der Tätigkeit eines Zertifizierungsdienstanbieters bedürfen keiner gesonderten Genehmigung. Der Anbieter muss die Aufnahme der Tätigkeit lediglich der Aufsichtsstelle anzeigen (§ 6 SigG[16]). Ein Anbieter, der sichere elektronische Signaturverfahren bereitstellt, kann sich aber vor der Aufnahme der Tätigkeit von der Aufsichtsstelle akkreditieren lassen (§ 17 SigG[17]).

Die Pflichten des Signators sind in § 21[18], die Haftung der Zertifizierungsdienstanbieter ist in §23 SigG[19] geregelt.

2.1.4 Signaturgesetz in Deutschland

Das Gesetz[20] trat am 22.5.2001 in Kraft und löste das Signaturgesetz von 1997 ab. Das Gesetz soll Rahmenbedingungen schaffen, durch deren Einhaltung qualifizierte elektronische Signaturen als gleichwertig zu handschriftlichen Signaturen vor Gericht anerkannt werden.

Das Signaturgesetz [21] unterscheidet drei Arten elektronischer Signaturen. Aufsteigend nach den Sicherheitsanforderungen, die für diese gestellt sind, handelt es sich dabei um folgende Arten:

- die einfache elektronische Signatur
- die fortgeschrittene elektronische Signatur
- und die qualifizierte elektronische Signatur

Die einfache sowie die fortgeschrittene Signatur sind vollständig unreguliert. Als Beweismittel vor Gericht und als Ersatz für die eigenhändige Unterschrift wird nur die qualifizierte Signatur zugelassen. Im Sinne dieses Gesetzes ist eine qualifizierte elektronische Signatur eine fortgeschrittene Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren

[15] siehe Anhang Seite 90, 91
[16] siehe Anhang Seite 90
[17] siehe Anhang Seite 95
[18] siehe Anhang Seite 97
[19] siehe Anhang Seite 97
[20] vgl. http://www.bsi.de/esig/basics/legalbas/sigg2001.pdf
[21] vgl. http://bundesrecht.juris.de/sigv_2001/index.html

Signatur-Erstellungseinheit erzeugt wurde. Die qualifizierte elektronische Signatur[22] ist somit ein mit einem privaten Signaturschlüssel erzeugtes Siegel.

2.1.5 A-Trust

Das österreichische Unternehmen A-Trust bietet alle Leistungen über die elektronische Signatur an. A-Trust[23] arbeitet auf der Grundlage des österreichischen Signaturgesetzes und der europäischen Signaturrichtlinie. Im Trust Center, wie das A-Trust besteht die Möglichkeit die jeweilige Identität des Kommunikationspartners in elektronischen Kommunikationsprozessen zu prüfen. A-Trust besitzt ein öffentliches Register, in dem alle ausgestellten Zertifikate und die Nummer der widerrufenen und gesperrten Zertifikate eingetragen sind.

Im Gegensatz zum "analogen" Geschäftsleben, wo die Identitätsprüfung durch amtliche Ausweise erfolgt, geschieht dies in der "digitalen Welt" durch Zertifikate. Das Unternehmen A-Trust ist einzige akkreditierte Zertifizierungs-Dienste-Anbieter (ZDA) für die Ausgabe von qualifizierten Zertifikaten in Österreich. Um auf dem Markt zeigen zu können, bei welchen digitalen Signaturen es sich auch wirklich um sichere Signaturen im Sinne des Signaturgesetzes (Österreich) handelt, bedient man sich dem A-Trust Gütezeichen.

Die von einem Zertifizierungs-Dienste-Anbieter (ZDA) in Verwendung genommenen Systeme und zum Einsatz empfohlenen Komponenten müssen von einer staatlichen Bestätigungsstelle kontrolliert werden. Auf der einen Seite bezieht sich das Gesetz auf die technischen Komponenten und die Verfahren zur sicheren Herstellung und Speicherung von Signaturerzeugungs- und -prüfdaten (Schlüsselpaar), auf der anderen Seite auf die technischen Werkzeuge und Verfahren für die Erzeugung sicherer Signaturen.

Nach dem Stand der Technik muss alles nach international anerkannten Normen und Verfahren (z.B.: ITSEC[24]) hinreichend geprüft sein. Um einen korrekten Ablauf zu garantieren, wurde in Österreich der Verein "Zentrum für sichere Informationstechnologie - Austria" (A-SIT) als Bestätigungsstelle gegründet. A-SIT

[22] vgl. http://www.bundesnetzagentur.de/enid/pi.html

[23] vgl. http://www.a-trust.at/

[24] siehe http://www.bsi.bund.de/zertifiz/itkrit/itsec-dt.pdf

repräsentiert Österreich in Normungsgremien[25] für die digitale Signatur in der EU und kontrolliert auch die Sicherheit der digitalen Signaturen.

Die Hauptaufgabe einer Bestätigungsstelle ist es Bescheinigungen gemäß §18(5)[26] Signaturgesetz zu vergeben. Im SigG §23 (2)[27] steht: Ein Zertifizierungs-Dienste-Anbieter, der sichere elektronische Signaturverfahren bereitstellt, haftet zudem dafür, dass für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstige Mittel für die Erstellung sicherer elektronischer Signaturen sowie für die Darstellung zu signierender Daten nur technische Komponenten und Verfahren nach §18[28] verwendet werden. In der Erklärung des SigG steht dafür: Ein Zertifizierungs-Dienste-Anbieter, der sichere Signaturverfahren bereitstellt, muss dafür garantieren, dass nur geeignete technische Komponenten verwendet werden.

Die eingesetzten Komponenten und Systeme (auch empfohlene Systeme) eines Zertifizierungsdienstanbieters müssen von einer staatlichen Bestätigungsstelle überprüft worden sein. Für diese Überprüfung gibt es international anerkannte Normen und Verfahren.
A-Sit wurde als solch eine Bestätigungsstelle in Österreich gegründet (A-Sit = Zentrum für sichere Informationstechnologie). Es ist sehr schwierig die Systemumgebung bei individuellen Signatoren zu kontrollieren, daher wird von A-Trust nicht nur anhand eines Merkblattes, sondern auch durch den RO über sichere einfache digitale Signaturen und deren Rechtswirkungen belehrt.

2.2 Unterschriften in Verbindung mit Zertifikaten

Als weiteres Instrument zur Sicherung der Authentizität setzt das Klinikum Ingolstadt[29] auf Zertifikate, bei denen man selbst als Herausgeber agiert, also eine eigene Zertifizierungsstelle (Certification Authority, CA) unterhält.

Ein weit verbreitetes Format für Zertifikate stellt „X.509“ dar, ein internationaler Standard, der kontinuierlich weiterentwickelt wird. Seit der Version 3 kann das Zertifikat um zusätzliche Felder mit individuellen Informationen erweitert werden. Seit

[25] siehe http://www.a-sit.at/de/dokumente_publikationen/normen_standards/index.php
[26] siehe Anhang Seite 97
[27] siehe Anhang Seite 99
[28] siehe Anhang Seite 97
[29] siehe Bsp. Seite 14

dem Jahr 2000 ist die Version 4 verfügbar. Der X.509-Standard wird von gängigen Browsern unterstützt, dem verbreiteten Secure Socket Layer (SSL)-Protokoll sowie den meisten E-Mail Programmen. Er erfordert folglich keine Zusatzsoftware. Wer eine verschlüsselte Mail empfängt, bekommt einen Hinweis in der Mailanwendung und kann die Zertifikatsdaten abfragen.

Der private Schlüssel und das Zertifikat werden auf sicherem Wege in den lokalen Zertifikatsspeicher des Rechners übertragen. Diese Zertifikate beinhalten den Namen des Ausstellers (hier ist es das Klinikum selbst), Informationen über die Identität des Inhabers sowie die elektronische Signatur des Ausstellers. Als erweiterte Informationen können zusätzliche Attribute, wie die Zuordnung zum Heilberuf (z.B. „Arzt" oder „Pflegekraft") hinterlegt werden. Da es sich im Klinikum um eine geschlossene Benutzergruppe handelt, wird die Gültigkeitsdauer der Zertifikate auf 5 Jahre festgesetzt.

Die Unterschrift kann übrigens auch dort, wo eine qualifizierte elektronische Signatur verlangt wird, zur Authentifizierung herangezogen werden: Die mögliche Autorisierung einer anderen Person (z.B. durch Weitergabe der sicheren Signaturerstellungseinheit und PIN) kann ausgeschlossen werden, indem die Signaturerstellungseinheit über die Nutzung biometrischer Merkmale[30] ausschließlich an eine Person gebunden wird" (SigG - Begründung zu §15 Absatz 1 Satz 4[31]). So ist also die Freischaltung einer Anwendung zur Erzeugung einer qualifizierten Signatur auch via Unterschrift denkbar.

2.2.1 Zertifizierung

Man kann sich also ein Zertifikat wie einen Personalausweis in digitaler Form vorstellen: Beim Personalausweis garantiert die zuständige Vertrauensstelle "Meldeamt", dass die Unterschrift, die sich auf dem Ausweis befindet, auch tatsächlich zu der Person gehört, deren Stammdaten und Passbild sich auf dem Ausweis befinden.

Mit einem Zertifikat wird eine digitale Bescheinigung über die Zuordnung des öffentlichen Signierschlüssels zu einer natürlichen oder juristischen Person ausgestellt.

Daher sind folgende Punkte zu klären:

- welche Struktur ein solches Zertifikat besitzt,

[30] vgl. Biometrie Seite 19
[31] siehe Anhang Seite 94

- auf welche Art und Weise es ausgestellt wird und
- wie diese Zertifikate verifiziert werden können.

Es ist natürlich selbstverständlich, dass ein Zertifikat keine Aussage über den Inhalt signierter Dokumente oder über die Vertrauenswürdigkeit der signierenden Person machen kann. Ein Zertifikat trägt zwar zur Vertrauensbildung bei, ersetzt aber keinesfalls weitere Kontrollen, die besonders dann notwendig sind, wenn es sich, um einen signierten ausführbaren Code handelt.

2.2.2 Zertifikate

Ein Zertifikat enthält Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle.

Inhalt	**Erläuterung**
Versionsnummer	beschreibt verwendetes Zertifikatformat
Seriennummer	eindeutiger Identifikator
Signatur	verwendete Algorithmen und Parameter
Zertifikataussteller	Name der ausstellenden Instanz
Gültigkeitsdauer	Angabe eines Zeitintervalls
Benutzername	eindeutiger Name des Benutzers
Schlüsselinformationen	Schlüssel des Benutzers und Algorithmen
eindeutiger Identifikator	in Version v2, v3
Erweiterungen	in Version v2, v3

Tabelle 1. Struktur eines Zertifikats

Diese Daten wie in Tabelle 1 beschrieben können mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden, da diese im Normalfall mit dem privaten Schlüssel der Zertifizierungsstelle signiert sind. Auf einige Punkte aus Tabelle1 möchte ich noch näher eingehen. Die Angabe des eindeutigen Namens des Benutzers oder des Ausstellers im Zertifikat ermöglicht es, diesen Namen mehrfach zu verwenden. Das Erweiterungsfeld definiert eine Folge von einer oder mehreren Erweiterungen. Beispiele für solche Erweiterungen sind key-usage, private key-usage period oder certificate policies. Die key-usage Erweiterung definiert, für welchen Zweck (Verschlüsseln, Signieren, Zertifizieren) der Schlüssel, der im Zertifikat enthalten ist, eingesetzt werden darf. Die private key-usage Perioden Erweiterung ermöglicht es, unterschiedliche Gültigkeitsdauern für den privaten Schlüssel des Benutzers festzulegen. Die

ausstellende Instanz ist dafür verantwortlich, dass keine zwei Zertifikate mit gleichen Seriennummern ausgestellt werden, damit eine eindeutige Zuordnung möglich ist.

2.2.3 Zertifikationspolicy

Certificate Policy (CP) oder auch nur Policy sind die gebräuchlichen Bezeichnungen der internationalen Zertifikatspolicy.

Das Signaturgesetz und die Signaturverordnung informieren uns über den Mindestinhalt der Policy. Was ein Zertifikat beinhalten soll und unter welchen Bedingungen das Zertifikat durch den Signator sicher benützt wird, wird von der Policy vorgegeben. Dadurch entsteht eine gewisse Sicherheit für den Empfänger einer Signatur. Er erhält eine Information über die Qualität der Signatur und das ihr zu Grunde liegende Zertifikat, somit einen Hinweis darauf, worauf er vertrauen darf.
Zum Beispiel darf und kann das Signaturzertifikat gem. dem Signaturgesetz zur Ver- und Entschlüsselung von Dokumenten nicht verwendet werden

2.2.4 Signierte Dokumente als Beweismittel

Zuerst möchte ich auf etwas Wichtiges hinweisen, was öfters zu Missverständnissen führt. Es handelt sich dabei um zwei Begriffe, Gültigkeit und Beweisfähigkeit. Diese beiden Begriffe werden bei vielen Diskussionen verwechselt.

Beweisfähigkeit bezieht sich vor allem auf die erstellten elektronischen Signaturen, während Gültigkeit sich auf die Verwendbarkeit von Verschlüsselungsalgorithmen und Zertifikate bezieht. Das heißt, elektronische Signaturen sind ab dem Zeitpunkt ihrer Erstellung immer gültig und sind zeitlich nicht beschränkt. Ungültig werden nur die Verschlüsselungs-Algorithmen, die für die Erstellung der Signaturen verwendet wurden sowie die Zertifikate bei Zertifikat-basierten Signatur-Verfahren.

2.2.5 Gültigkeit von Zertifikaten

Zertifikate sind maximal fünf Jahre und im Durchschnitt zwei bis drei Jahre gültig. Das bedeutet, dass der Private Key eines Unterzeichners nur während dieser Zeit für die Erstellung von Signaturen verwendet wurde, er wird dann im Trust-Center als gesperrt eingeordnet. Trotz der Sperre müssen Zertifikate für die qualifizierten elektronischen Signaturen noch weitere fünf Jahre von Zertifizierung-Dienste-Anbieter zur

Identifizierung zur Verfügung stehen, bei qualifizierten Signaturen mit Anbieter-Akkreditierung sogar dreißig Jahre.

Für geprüfte Verschlüsselungsalgorithmen wird eine maximale Gültigkeit von fünf Jahren angenommen, um höhere Sicherheit zu gewähren. Der Grund dafür ist die Annahme, dass in sechs Jahren wahrscheinlich durch den Fortschritt der Technik und neuer Software die Private Key aus der Public Key geknackt werden kann. Die Umsetzung solcher Möglichkeiten wird jedoch in der Realität einen größeren Zeitraum in Anspruch nehmen.

2.2.6 Zertifizierungsstelle

Eine Zertifizierungsstelle ist im Sinne dieses Gesetzes eine natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln zu natürlichen Personen bescheinigt.

Generell ist der Betrieb einer Zertifizierungsstelle im Rahmen des Gesetzes genehmigungsfrei. Zertifizierungs-Dienste-Anbieter können sich auf eigenen Antrag bei der RegTP akkreditieren lassen. Ein akkreditierter Anbieter darf für seine Zertifizierungstätigkeit nur geprüfte Produkte für qualifizierte elektronische Signaturen einsetzen. Mit dem Gütezeichen der RegTP wird bestätigt, dass der akkreditierte Anbieter den Nachweis erbracht hat, dass seine technischen und administrativen Sicherheitsmaßnahmen den gesetzlichen Anforderungen entsprechen. Der Anbieter ist berechtigt, qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung zu erstellen.

Das Gesetz schreibt vor, dass die Teilnehmerdaten, das Zertifikat des öffentlichen Schlüssels sowie der öffentliche Schlüssel der Zertifizierungsstelle auf einem geeigneten Trägermedium für den Teilnehmer (z.B. Chipkarte) gespeichert werden sollten. Stattdessen kann auch der mit dem Zeitstempel versehene Hashwert zusammen mit einem Verweis auf die entsprechenden Daten in einem öffentlich zugänglichen Verzeichnis bekannt gegeben werden.

Der allgemeine Ablauf, wie in Abb. 1 dargestellt, zur Nutzung der vorgestellten Dienste eines Trust-Dienst-Nutzung-Centers lässt sich wie folgt zusammenfassen: Zunächst wird vom Teilnehmer selbst oder in der Zertifizierungsstelle ein Schlüsselpaar generiert. Der Teilnehmer identifiziert sich, lässt sich registrieren und beantragt ein Zertifikat.

Dieses Zertifikat wird anhand der Teilnehmer- und Schlüsseldaten von der Zertifizierungsstelle erstellt und sowohl an den Personalisierungsdienst als auch an den Verzeichnisdienst übermittelt.

Der Verzeichnisdienst ermöglicht anderen Benutzern Zugriff auf das Zertifikat. Ungültige Zertifikate sind durch einen Sperrvermerk zu kennzeichnen, der Auskunft über den Zeitpunkt des Eintretens der Ungültigkeit gibt.

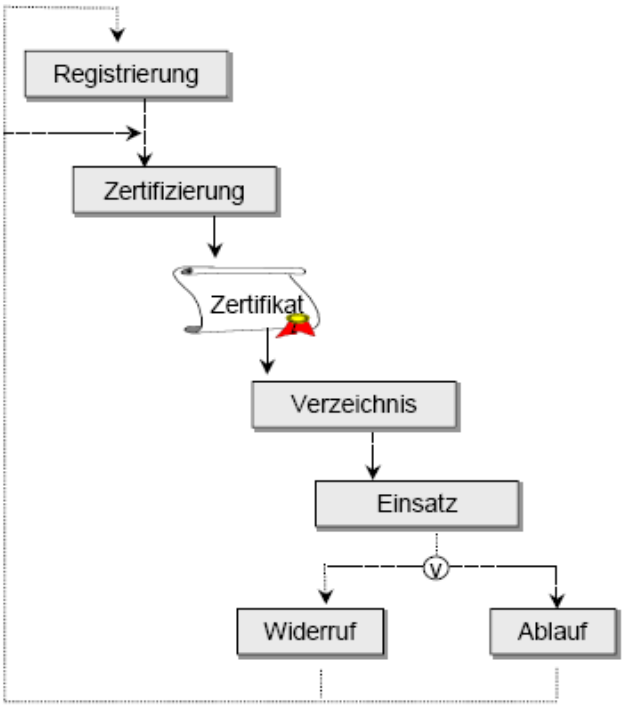

Abb. 1. Lebenszyklus eines Zertifikats [32]

2.2.7 Zeitstempel

Zeitstempel[33] werden vorwiegend bei der elektronischen Archivierung von Dokumenten eingesetzt. Zusätzlich werden sie auch als Anhang zu qualifizierten Signaturen hinzugefügt.

Der Vorteil von Zeitstempel bei der elektronischen Archivierung besteht darin, dass der Inhalt zum Archivierungszeitpunkt dokumentierbar ist. Jedoch kann die elektronische Signatur nicht dadurch ersetzt werden. Bei qualifizierten Signaturen dienen Zeitstempel als Dokumentation der Signaturzeit, die durch die Signatur alleine nicht erreicht werden kann. Dieser Vorgang ist essentiell, denn nach Ablauf der benötigten Zertifikate wären die elektronischen Signaturen ungültig.

[32] vgl. http://wi.wu-wien.ac.at/home/madlberger/E-Commerce%20und%20Neue%20Medien/ECNM_VO_03_04_Sicherheit.pdf, Folie 22, 18.09.06
[33] vgl. http://www.signaturrecht.de/beispiele/index.html

Technisch gesehen werden Zeitstempeln wie elektronische Signaturen erstellt, sind aber keine personengebundenen Signaturen, sondern dienen nur dem Nachweis, dass der Inhalt eines elektronischen Dokumentes zu einem bestimmten Zeitpunkt vorlag.

Die Erstellung von Zeitstempeln erfolgt entweder online über Zeitstempeldienste oder über bestimmte Server, die als Black Box ins Netz gestellt werden. Die Datenstrukturen eines Zeitstempels beinhalten das Erstellungsdatum, die Uhrzeit des Zeitstempels und den Hashwert (=Prüfsumme des gestempelten Dokumenteninhaltes). Die Erstellung von qualifizierten Zeitstempeln kann nur durch zertifizierte Unternehmen wie dem Trust-Center[34] oder durch bestimmte zertifizierte Geräte erfolgen.

Zeitstempel dienen als Nachweis (d.h. Ergänzung zu qualifizierten Signaturen) darüber, dass eine zertifikatbasierte Signatur vor demjenigen Zeitpunkt erstellt wurde, an dem das Zertifikat ungültig wurde. In Kombination mit einem sicheren Zeitstempel kann gewährleistet werden, dass eine qualifizierte Signatur zur gleichen Zeit der Zertifikatsgültigkeit erstellt wurde.

2.3 Biometrie

Es gibt zwei verschiedene Arten von biometrischen Merkmalen: einerseits die passiven Merkmale und andererseits die aktiven Merkmale.

Passive Merkmale:

- Fingerprint, siehe Abb. 3
- Iriserkennung
- Gesichtserkennung, siehe Abb. 2

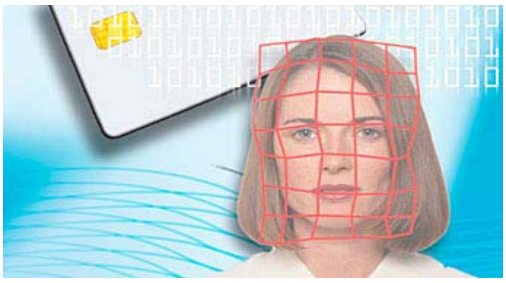

Abb. 2. Gesichtserkennung[35]

Abb. 3. Fingerprint [36]

[34] vgl. http://www.a-trust.at/info.asp?node=516&lang=GE&ch=4
[35] vgl. http://www.sagem-orga.com/image/identification_Biometrie.jpg
[36] vgl.http://www.digitalpersona.com/company/news/pressKit/4000%20Fingerprint%20Reader%20with%20finger.jp

Aktive biometrische Merkmale:

- Spracherkennung
- Eigenhändige Unterschrift

Für den mobilen Bereich wie z.B.: für Handys, Laptops, und PDAs wären Fingerprint, Iriserkennung und die Spracherkennung sehr gefragt. Die Spracherkennung wird in kleinster Form, für das Speichern von Befehlen und Namen, bei Handys, PDAs und Laptops schon angewendet.

2.3.1 Biometrie für qualifizierte Signaturen

Die PIN können durch biometrische Verfahren (Fingerprint, Gesichtserkennung und Iriserkennung), welche eine Person anhand von körpereignen Merkmalen erkennen lassen, ersetzt werden.

In Kombination mit qualifizierten Signaturen will man sicherstellen, dass der private key auch wirklich von der richtigen Person freigeschaltet wird. Aber im Moment lassen sich die biometrischen Algorithmen wegen der begrenzten Speicherkapazität des Chips nicht auf Signaturkarten (bei mobilen Geräten auf SIMS) unterbringen.

2.3.2 Biometrie in der Praxis

Hier möchte ich noch ein paar Beispiele aus einigen Bereichen erwähnen, in denen, Biometrie zu Einsatz kommt:

- Zutrittssysteme in Gebäuden
- Personaldokumente wie Reisepass und Personalausweis
- Personalisierung im Auto
- IT-Security
- Fingerprint als Boardkarte

3 Technische Grundlagen der elektronischen Signatur

In diesem Kapitel werden die technischen Grundlagen der elektronischen Signatur dargestellt. Neben der grundlegenden Funktionsweise und den gängigsten Standards der symmetrischen und asymmetrischen Kryptographie wird das Verfahren zur Erzeugung einer elektronischen Signatur erklärt.

Heutige kryptografische Verfahren sind stark mathematisch geprägt. Aufgrund der extrem gewachsenen Rechnerleistung werden inzwischen Zahlen mit mehreren hundert Ziffern verwendet. Diese technischen Grundlagen bilden das Grundgerüst für die Verwendung der Signaturtechnologie.

3.1 Symmetrische Verfahren

Der älteste Zweig der Kryptographie beschäftigt sich mit der Geheimhaltung von Nachrichten durch Verschlüsselung. In der klassischen Kryptologie wird dies so realisiert, dass Sender und Empfänger einen gemeinsamen geheimen Schlüssel besitzen und sich auf diese Weise gegen die Außenwelt schützen. Dieses Verfahren nennt man symmetrische Verschlüsselungsverfahren[37].

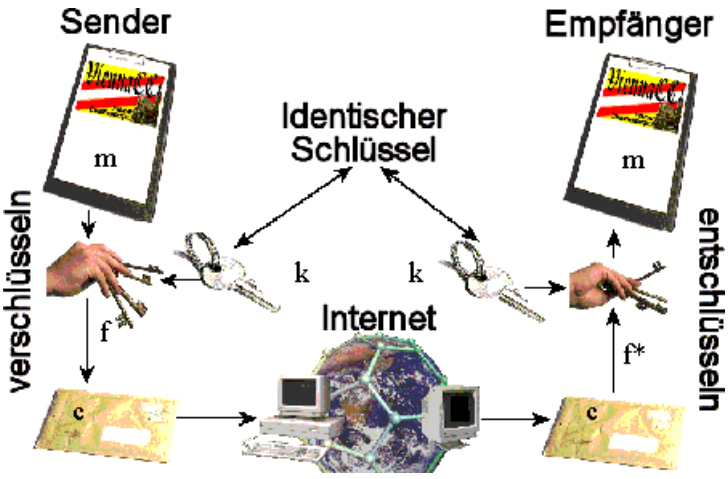

Abb. 4. Symmetrisches Verschlüsselngsverfahren

Wie in Abb. 4 ersichtlich, besteht ein symmetrischer Verschlüsselungsalgorithmus aus einer Funktion `f` mit zwei Eingabewerten, dem Schlüssel `k` und dem Klartext `m`, und einer Ausgabe, dem Geheimtext `c`, der sich aus `k` und m ergibt.

[37] vgl. Beutelspacher, Albrecht : Moderne Verfahren der Kryptographie

Eine Verschlüsselungsfunktion f muss umkehrbar sein, d.h. es muss eine Funktion f* geben, welche die Wirkung von f rückgängig macht und damit unter dem gleichen Schlüssel k aus dem Geheimtext c wieder den Klartext m erstellt.

Der Sender verschlüsselt eine Nachricht m, indem er

C = f(k,m)

berechnet, wobei k der gemeinsame geheime Schlüssel von Sender und Empfänger ist. Alternativ dazu schreiben wir auch $c := f_k(m)$. Der Empfänger kann mit Hilfe desselben Schlüssels k den Geheimtext entschlüsseln, indem er
f* (k,c) = m
berechnet.

3.1.1 Nachteile symmetrischer Verschlüsselungsverfahren

Symmetrische Verschlüsselungsverfahren bzw. deren Schlüssel können wie oben beschrieben zum Verschließen und zum Öffnen genutzt werden, wie für eine Wohnungstür. Daher ergeben sich vier wesentliche Nachteile[38]:

- Bei der Übermittelung des Schlüssels ist man auf andere Medien angewiesen, da nicht der gleiche Kanal wie für den anschließend verschlüsselten Text verwendet werden kann. Für die Schlüsselübermittelung muss ein anderer und sicherer Kanal benützt werden.
- Einem Teilnehmer ist es fast unmöglich die Urheberschaft des verschlüsselten Textes nachzuweisen, da keine absolute Sicherheit gegeben ist, dass ein anderer Teilnehmer den Schlüssel missbräuchlich angewandt hat.
- Bei Kommunikation vieler unabhängiger Teilnehmer untereinander steigt die Zahl der benötigten Schlüssel sehr rasch an, z.B. wären dies bei n Teilnehmer:

  n * (n-1) / 2

- Die symmetrische Kryptografie bietet außer der reinen Verschlüsselung eines Ausgangtextes keine weitere Funktionalität.

[38] vgl. Steininger, Katharina : Elektronische Signaturen

3.1.2 DES (Data Encryption Standard)

DES ist weltweit das am häufigsten eingesetzte Verschlüsselungsverfahren und wurde 1977 vom amerikanischen National Bureau of Standards (heute: National Institute of Standards and Technology – NIST) als offizieller Standard veröffentlicht.

DES beruht auf einem symmetrischen Verschlüsselungsverfahren, bei dem Daten in Blöcke zu je 64 Bit geteilt und mit einem ebenfalls 64 Bit langen Schlüssel codiert werden. Die eigentliche Chiffrierung geschieht in einem 16 Runden umfassenden Prozess von Permutation und Substitution der Daten. Das DES-Verfahren wurde 1971 von IBM entwickelt und ist unter dem Namen Lucifer bekannt. Jedoch wurde bei DES die Schlüssellänge von 128 Bit auf nur 56 Bit gekürzt, was einer der größten Schwächen dieses Standards darstellt. Da 1977 DES geknackt wurde, kann es heute nicht mehr als sicher angesehen werden und ist nicht mehr für den Einsatz geheimer Informationen geeignet. DES lässt sich sehr gut in Hardware, also in Chips [39] implementieren, die sehr kostengünstig und in großer Anzahl hergestellt werden können.

Um nun das DES-Verfahren weiter zu verwenden, hat man zwei Erweiterungen von DES entwickelt. Das IDEA-Verfahren, mit einem komplett neuen Algorithmus mit längeren Schlüsseln und das Triple-DES-Verfahren, eine Anpassung des DES-Verfahrens um längere Schlüssel zu erreichen, was den Vorteil hat, dass auf die bewährten Teile des DES-Verfahrens zurückgegriffen werden kann.

Grundsätzlich gilt ein Schlüssel dann als sicher, wenn der Aufwand zum Auffinden des Schlüssels den Wert der verschlüsselten Information übersteigt und die dazu benötigte Zeit die Dauer der Brauchbarkeit[40] der Daten übersteigt.

3.1.3 International Data Encryption Algorythm (IDEA)

IDEA[41] wurde 1990 von Lei und Messey am Swiss Federal Institute of Technology entwickelt. Dieser stellt ebenfalls einen symmetrischen, blockorientierten Verschlüsselungsmechanismus dar. IDEA arbeitet wie DES mit 64 Bit langen Datenblöcken, verwendet aber insgesamt einen 128 Bit langen Schlüssel, dadurch sind Brute Force Angriffe nicht mehr Erfolg versprechend. Die Implementierung von IDEA in PGP sorgt für eine weltweite Verbreitung.

[39] vgl. http://www.computerwelt.at/detailArticle.asp?a=99728&n=4
[40] vgl. Steininger, Katharina : Elektronische Signaturen
[41] vgl. http://de.wikipedia.org/wiki/International_Data_Encryption_Algorithm

3.1.4 Triple–DES

Das Grundprinzip dieses Verfahrens beruht nach „Menzel Thomas“ [42] auf einem dreimaligen DES-Verschlüsselungsvorgang mit je drei verschiedenen Schlüsseln. Die Länge eines Schlüsselblocks ist identisch mit jener beim DES-Verfahren, man erreicht hier also eine effektive Gesamtlänge von 3 * 56 Bit = 168 Bit. Allerdings dauert das Verfahren auch dreimal so lange wie die Verschlüsselung mit dem DES-Verfahren.

Aufgrund der Verwendung eines dreimal so langen Schlüssels gibt es zurzeit keine brauchbaren Angriffe gegenüber Triple-DES. Nach Lukas Stefan und Zenner Erik [43] gelang erst 1998 eine Analyse von Triple-DES, als an der Universität Mannheim ein Angriff mit "nur noch" 2^{105} Rechenoperationen gefunden wurde. Wenn Computer in Zukunft mit gleichem Tempo schneller werden, wie sie es in der Vergangenheit getan haben, wird es noch knapp drei Jahrzehnte dauern, bis irgendeine Instanz in der Welt über genug Rechenleistung verfügen kann, um diesen Angriff praktisch durchzuführen.

3.1.5 Advanced Encryption Standard (AES)

Aufgrund der Unsicherheiten des DES-Standards wurde vom National Institute of Standards and Technology (NIST) im Oktober 2000 ein neuer symmetrischer Verschlüsselungsalgorithmus als Nachfolger für DES bekannt gegeben und 2002 als Standard erklärt, der Advanced Encryption Standard[44] (AES). Bei AES ist die Größe der Blöcke der verschlüsselnden Daten variabel und jeder Block wird einzeln verschlüsselt. AES ist also ein Algorithmus, bei dem Blocklänge und Schlüssellänge unabhängig voneinander die Werte 128, 192 oder 256 Bit erhalten kann. Gemäß Berechnungen des NIST braucht ein Rechner, der DES in einer Sekunde knacken könnte, für AES mit 128-Bit-Schlüssel ca. 149 Billionen Jahre Rechenzeit. .

3.2 Asymmetrische Verfahren

Diese Verschlüsselungstechnik wurde 1976 von Dieffie und Hellman entwickelt. Asymmetrische Verschlüsselungsalgorithmen benötigen immer zwei Schlüssel. Einer der beiden Schlüssel dient der Verschlüsselung des Ausgangstextes, der andere wird zum Entschlüsseln verwendet. Der Verschlüsselungsschlüssel wird geheim gehalten

[42] siehe Menzel Thomas, Elektronische Signaturen, Wien 2000
[43] vgl. http://www.uni-mannheim.de/forum/p/pdf/forum_2003_14.pdf (Stand 4. Mai 2006)
[44] vgl. http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

und darf nicht weitergegeben werden, er ist nur dem Unterzeichner bekannt. Dieser Schlüssel wird auch als Private Key bezeichnet.

Den anderen Schlüssel, den Public Key, stellt man der Öffentlichkeit zur Verfügung. Dies ermöglicht die ausschließliche Kommunikation über das Internet.
Um die Sicherheit des asymmetrischen Verfahrens zu erhöhen, sollten zusätzlich zwei Hardwarekomponenten eingesetzt werden. Einerseits eine mit PIN-Code geschützte Chipkarte und ein Kartenleser. Die Eingabe des PINs und die Verschlüsselung erfolgt dabei direkt am Kartenleser, sodass selbst bei einem kompromittierten Rechner (z.B. bei installiertem Trojaner oder Key-Logger) die sichere Verschlüsselung gewährleistet bleibt.

Auf der Chipkarte wird der private Schlüssel abgespeichert. Dieser sollte von einer vertrauenswürdigen Institution, die als Trust Center, Zertifizierungsstelle oder Zertifizierungsdienstanbieter bezeichnet wird, erzeugt und produziert werden. Außerdem bestätigt diese die Zuordnung eines öffentlichen Schlüssels zu einer Person durch ein elektronisches Zertifikat. Die Karte wird durch einen so genannten Pin-Code gesichert. Um den Schutz vor unbefugtem Zugriff zu gewährleisten, benötigt man laut Signaturgesetz ein Kartenlesegerät. Die direkte Eingabe am PC wäre mit zu großen Risiken verbunden. Der Pin könnte im Speicher des PCs aufscheinen und dort gegebenenfalls von Viren oder Trojanern ausgespäht werden.

3.2.1 Asymmetrische Verschlüsselung (Prozess)

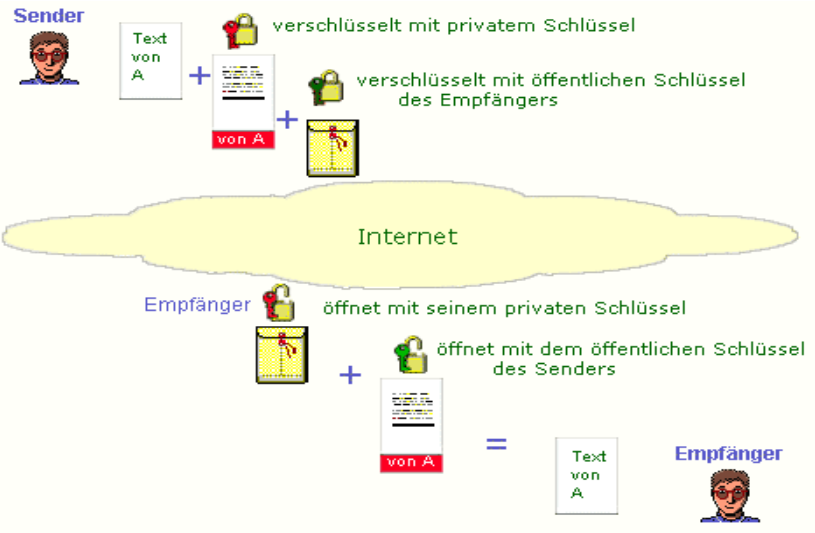

Abb. 5. Asymmetrische Verschlüsselung

Funktionsweise einer asymmetrischen Verschlüsselung laut Abb. 5

1. Sei (SA, VA) das Schlüsselpaar von Alice, bestehend aus dem privaten Protokoll Signaturschlüssel SA und dem öffentlichen Verifikationsschlüssel VA.
2. Alice hinterlegt VA in einer öffentlichen Datenbank.
3. Sie signiert ein Dokument M durch Verschlüsseln mit ihrem privaten Schlüssel, $D(M, SA) = sig$, und sendet das signierte Dokument sig an Bob.
4. Bob ruft den benötigten Verifikationsschlüssel VA aus der Datenbank ab ~. und verifiziert die Signatur sig, $M = E(sig, VA)$.

3.2.2 Anforderungen an digitale Signaturen

Dieses Protokoll ist im Vergleich zum symmetrischen wesentlich effizienter, da hier kein Vermittler benötigt wird. Jeder Beteiligte kann durch die Nutzung der öffentlich bekannten Verifikationsschlüssel die Gültigkeit der Signatur nachprüfen. Wiederum bleibt zu klären, ob das Protokoll die gestellten Anforderungen an digitale Signaturen erfüllt.

- Zweifelsfreie Identität: Unter der Voraussetzung, dass der öffentliche Verifikationsschlüssel eindeutig einer juristischen Person zuordenbar ist, bezeugt die Signatur die Identität des Unterzeichners. Durch die Verifikation wird Alice als Urheberin bestätigt, da nur sie den zum Verifikationsschlüssel passenden Signaturschlüssel kennt.

- Keine Wiederverwendbarkeit: Die Signatur kann nicht unautorisiert wieder verwendet werden, da sie das Ergebnis einer Verschlüsselungsoperation, also ein Funktionswert abhängig vom jeweiligen Dokument, ist.

- Unveränderbarkeit: Das signierte Dokument ist nicht mehr veränderbar bzw. eine Änderung ist erkennbar, da dadurch keine korrekte Verifikation mehr möglich ist.

- Verbindlichkeit: Unter der Voraussetzung, dass der private Signaturschlüssel nicht kompromittiert ist, kann Alice die Signatur nicht zurückweisen, da ausschließlich sie selbst über ihren privaten Signaturschlüssel verfügt.

Um die Verbindlichkeit zu garantieren, ist sicherzustellen, dass ein Kommunikationsteilnehmer seinen privaten Signaturschlüssel nicht absichtlich oder unabsichtlich offen legt.

Im einfachsten Fall führen Trust Center schwarze Listen, um Benutzer, deren Schlüssel offen gelegt wurden, zu identifizieren und um die weitere Verwendung dieser Schlüssel zu unterbinden. Unter Verwendung von Sicherheitsmodulen wie Smart Cards kann der direkte Zugriff auf die Schlüssel und damit deren absichtliche oder unabsichtliche Preisgabe erheblich erschwert werden.

Durch die Verwendung von Zeitstempeln lassen sich Signaturen datieren, sodass solche Signaturen zurückgewiesen werden können, die nach der Bekanntgabe der Veröffentlichung des privaten Signaturschlüssels ausgestellt wurden. Zeitstempel können daneben auch verwendet werden, um eine Mehrfachvorlage eines signierten Dokumentes, zum Beispiel eines Schecks, zu erkennen. Erforderlich ist die Ausstellung eines vertrauenswürdigen Zeitstempels, der auf einem nicht manipulierbaren Zeitgeber basiert. Um dies zu erreichen, kann beispielsweise das DCF-77 Funkzeitsignal von einer geschützten Sicherheitsbox eingefangen werden, welche der Signatur die genaue Zeit hinzufügt. Der Aufbau von Infrastrukturen mit vertrauenswürdigen Zeitstempeldiensten steckt zurzeit aber noch in den Kinderschuhen.

3.2.3 Einwegfunktionen und Trapdoor Einwegfunktionen

Eine Einwegfunktion[45] ist eine Funktion, die einfach auszuführen, aber schwer – praktisch unmöglich – zu invertieren ist. Etwas genauer formulieren wir: Eine injektive Funktion f: X → Y heißt Einwegfunktion (one way function), wenn

1. für alle x ε X der Funktionswert $f(x)$ effizient berechenbar ist und
2. wenn es kein effizientes Verfahren gibt, um aus einem Bild y = $f(x)$ das Urbild x zu berechnen.

[45] vgl. Beutelspacher, Albrecht : Kryptologie

Ein alltägliches Beispiel für eine Einwegfunktion stellt ein Telefonbuch dar. Die auszuführende Funktion ist einem Namen die entsprechende Telefonnummer zuzuordnen. Da die Namen alphabetisch geordnet sind, ist diese Zuordnung einfach auszuführen. Aber ihre Invertierung, also die Zuordnung eines Namens zu einer gegebenen Nummer, ist offensichtlich viel schwieriger, wenn man nur ein Telefonbuch zur Verfügung hat.

Eine Trapdoor Einwegfunktion ist eine Einwegfunktion, also eine außerordentlich schwer zu invertierende Funktion, zu der es aber eine Geheiminformation („Geheimtür", englisch „trapdoor") gibt, mit Hilfe derer man die Funktion leicht invertieren kann.

3.2.4 Der RSA-Algorithmus

Dieser Algorithmus wurde von seinen Namensgebern Ronald Rivest, Adi Shamir und Leonard Adleman 1978 entwickelt. Er ist nach „Menzel Thomas" [46] das am weitesten verbreitete, am meisten implementierte und am besten untersuchte Public-Key Verschlüsselungsverfahren, das sowohl zum Verschlüsseln, als auch zum elektronischen Signieren von Daten geeignet ist.

Die Verschlüsselung nach Ron Rivest, Adi Shamir und Len Adleman beruht auf einem mathematischen Verfahren.

Hier ist ein Beispiel zu RSA[47]:

Der kleine Satz von Fermat lautet:
Ist p eine Primzahl und **p** kein Teiler von **a**, so ist $\mathbf{a}^{\mathbf{p-1}} \equiv \mathbf{1} \pmod{\mathbf{p}}$
Der Beweis dieses Satzes nutzt Ergebnisse aus der Gruppentheorie.
Folgerung: Sind **p,q** prim und $\mathbf{n = p * q}$, sowie **p,q** keine Teiler von **a**, so ist $\mathbf{a}^{(p-1)\,*\,(q-1)+1} \equiv \mathbf{a} \pmod{\mathbf{n}}$

[46] siehe Menzel Thomas, Elektronische Signaturen, Wien 2000
[47] vgl. Ahmadi, Sanaz : 26 Jahre RSA-Kryptosystem

Dieses Beispiel beschreibt die Funktionsweise von RSA: [48]

Schritt 1

Qais wählt zwei große Primzahlen **p,q**. Er bildet die Produkte **n = p * q** und **φ(n) = (p - 1) * (q - 1)**.

Er wählt die Zahl **e** zwischen **1** und **n, e** teilerfremd zu **φ (n)** und er wählt eine Zahl **d** mit der Eigenschaft **e * d ≡ 1 (mod φ (n))** → d.h. **e * d = k * φ (n) + 1**

Schritt 2

Qais gibt **n** und **e** bekannt (**d nicht!**)

Fr. Prof. Strauss möchte Qais eine sehr geheime Nachricht **M** schicken. Wir denken uns **M** als eine Zahl **0 ≤ M < n**.

Fr. Prof. Strauss bestimmt **C ≡ Me (mod n)** und schickt **C** an Qais

Adam bestimmt **Cd (mod n)** und erhält???

Schritt 3

$C^d \equiv (M^e)^d \pmod n$

$\equiv M^{ed} \pmod n$

$\equiv M^{1 + k\ \varphi(n)} \pmod n$ nach Wahl von d

≡ M (mod n) nach kleinem Fermat

≡ M

……. Qais hat die Botschaft erhalten!

Die hohe Sicherheit dieses Verfahrens basiert unter anderem auf der Tatsache, dass der Schlüssel mindestens 1 KB lang sein muss. Der Quellcode von RSA ist offen gelegt und wurde von zahlreichen Wissenschaftlern und Experten auf Schwächen untersucht, was eine hohe Sicherheit garantiert. RSA ist in vielen Computerprogrammen wie z.B. PGP, Netscape Navigator oder Krypto Chips implementiert. Kyrpto Chips werden nach „Menzel Thomas" [49] auch direkt auf SmartCards implementiert, damit sensitive Daten nur mehr innerhalb der Karte unverschlüsselt vorliegen. Damit ist sichergestellt, dass niemand – nicht einmal der Karteninhaber selbst – den privaten Schlüssel kennt und missbräuchlich verwenden kann.

[48] vgl. http://www.mathematik.uni-osnabrueck.de/staff/phpages/pluemerj/krypto/sld028.htm

[49] siehe Menzel Thomas, Elektronische Signaturen, Wien 2000

Abb. 6. Rivest, Schamir und Adleman

Einer der wichtigsten Anforderungen an digitale Signaturen ist, dass die Verfahren nicht zu viele Ressourcen (Zeit, Speicher) beim Ver- und Entschlüsseln beanspruchen. Wenn man den RSA-Algorithmus anwendet und damit die gesamte Nachricht codiert, würde dies sehr viel Zeit und Speicher benötigen. Um dieses Problem zu umgehen, benützt man eine Hashfunktion. Mit ihrer Hilfe wird ein so genannter Hashwert berechnet. Nur dieser Wert wird mit Hilfe des RSA-Verfahrens codiert und gemeinsam mit der Nachricht an den Empfänger gesendet. Dieser geht auf die gleiche Art wie der Absender vor, berechnet den Hashwert der Nachricht und vergleicht diesen mit dem – mit Hilfe des öffentlichen Schlüssels des Absenders – decodierten Wert. Wenn die beiden Zahlen gleich sind, dann wurde die Nachricht nicht verfälscht.

3.2.5 Der EL Gamal Algorithmus

Das Verfahren von ElGamal [50] wird sowohl für digitale Signaturen als auch für Verschlüsselung benutzt. Der Kernpunkt der Sicherheit dieses Verfahrens beruht darauf, diskrete Algorithmen über einen endlichen Körper zu berechnen.

Zur Erzeugung eines Schlüsselpaars wählt man zuerst eine Primzahl p und zwei Zufallszahlen g und x, die beide kleiner sind als p. Dann berechnet man

$y = g^x \bmod p$

Dabei bilden y, g und p den öffentlichen Schlüssel. Es ist auch möglich, sowohl g als auch p gemeinsam in einer Benutzergruppe zu verwenden. X ist der private Schlüssel.

[50] vgl. Schneier, Bruce : Angewandte Kryptographie

Signaturen mit ElGamal:

Um eine Nachricht N zu signieren, wie in Abb. 7 auch getestet, wählt man zuerst eine Zufallszahl k, die relativ prim zu p-1 ist. Daraus berechnet man dann

$A = g^k \bmod p$

und löst folgende Gleichung mit Hilfe des erweiterten Euklidischen Algorithmus nach b auf:

$N = (xa + kb) \bmod (p - 1)$

Das Paar a und b bilden die Signatur. Der Zufallswert k muss geheim bleiben.

Zur Verifizierung der Signatur wird folgende Identität überprüft:

$Y^a a^b \bmod p = g^M \bmod p$

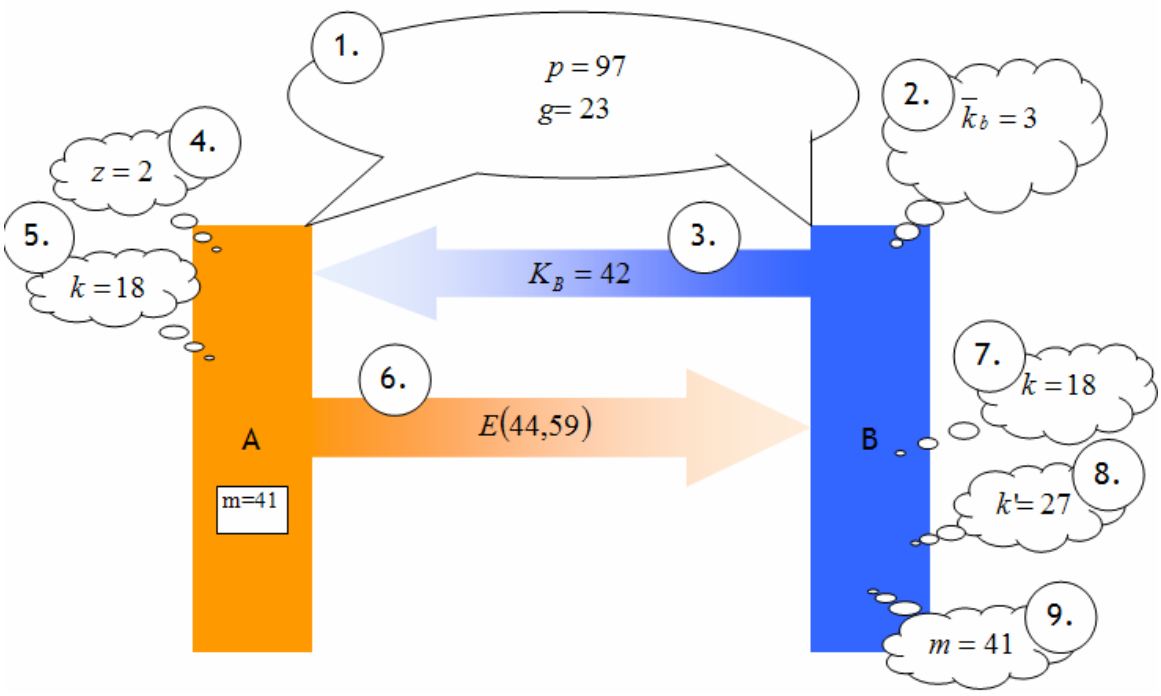

Abb. 7. ElGamal - Test[51]

[51] vgl. http://www.tu-chemnitz.de/wirtschaft/fsr/wiki/images/e/ef/Elgamal.PNG

3.3 Verfahren zur Erzeugung elektronischer Signaturen

Da eine Verschlüsselung des gesamten Ausgangtextes enorme Rechnerleistung und enormen Speicherplatz benötigt, wird bei der elektronischen Signatur das so genannte kryptografische Hashverfahren eingesetzt. Dabei wird von dem signierenden Dokument ein Fingerabdruck erzeugt.

Es wird nicht der gesamte Ausgangstext mit dem privaten Schlüssel des Absenders verschlüsselt, sondern von diesem Text ein Abbild erstellt, das dessen Inhalt eindeutig repräsentiert. Dazu wird eine Hashfunktion eingesetzt, wie Abb. 8 zeigt, die vom Ausgangstext einen so genannten Hashwert bildet, der absolut eindeutig diesem Text zugeordnet werden kann. Keine zwei verschiedenen Ausgangstexte ergeben denselben Hashwert. Dieser Hashwert wird anschließend elektronisch signiert und dem Ausgangstext beigefügt, um die Kombination anschließend zu verschicken. [52]

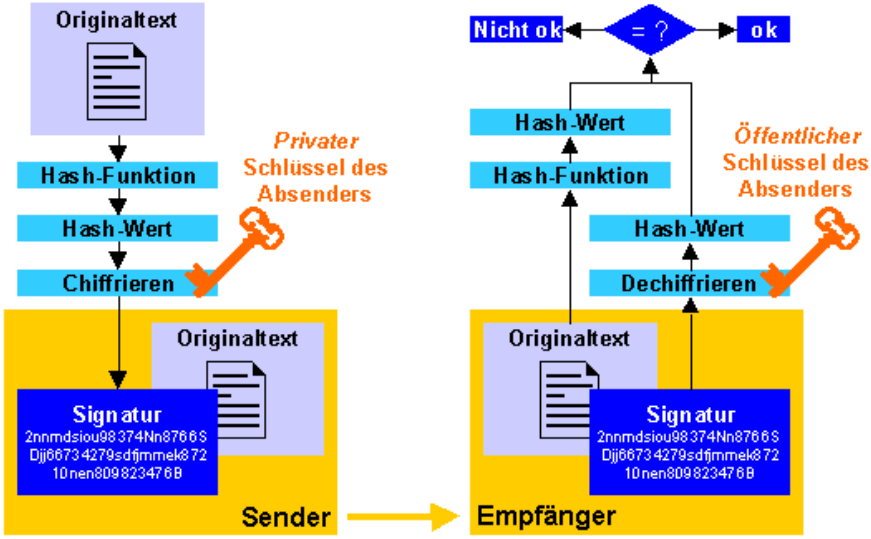

Abb. 8. Erzeugung einer elektronischen Signatur[53]

Die Hashfunktion muss so gewählt werden, dass sie folgende Anforderungen erfüllt:

- Die Hashfunktion muss kollisionsfrei sein, das heißt, es darf nach menschlichem Ermessen nicht möglich sein, zwei Dateien zu konstruieren, die den gleichen Hashwert haben.
- Der Hashwert darf nicht kleiner sein als 128 Bit. Dies zwingt einen Angreifer dazu, 264 Dokumente zu untersuchen, um zwei Nachrichten zu finden, die den gleichen Hashwert haben.

[52] vgl. Hühnlein, Detlef : Grundlagen der elektronischen Signatur
[53] Quelle: http://www.zahnaerzte-online.de/img/secure.gif

- Sie kann für eine Datei beliebiger Länge eingesetzt werden.
- Hashfunktionen dienen allgemein dazu, die Unverfälschtheit von Texten oder Daten nachzuweisen. Das Verschlüsseln des Hashwerts mit dem geheimen Schlüssel ergibt die digitale Signatur. [54]

Das Verfahren zur elektronischen Signierung erfolgt in zwei Schritten:
Im ersten Schritt der elektronischen Signierung wird gewissermaßen ein „Fingerabdruck“ der zu unterzeichnenden Daten erstellt. Genauer gesagt, es wird ihr Hashwert erzeugt. Anschließend wird dieser Hashwert asymmetrisch verschlüsselt. Dabei kommt der geheime Signaturschlüssel zum Einsatz, der im alleinigen Zugriff des Signierenden steht und dieser Code wird dann dem unverschlüsselten Originaltext beigefügt. Dieses wird dann zusammen mit dem Zertifikat des Absenders an den Empfänger gesendet.

Der Empfänger entschlüsselt anschließend die Signatur des erhaltenen Dokuments mit dem öffentlichen Schlüssel des Absenders und erhält so den Hashwert. Dann bildet er mit derselben Hashfunktion auch den Hashwert und vergleicht ihn mit dem Fingerabdruck. Sind beide identisch, so kann der Empfänger sicher sein, dass die Datei vom Inhaber des öffentlichen Schlüssels gesendet wurde. [55]

Im Folgenden werden ein Programm und zwei Standards beschrieben:

3.3.1 PGP (Pretty Good Privacy)

Pretty Good Privacy (PGP) ist eine im Internet weit verbreitete Kryptografie-Software zum Schutz der E-Mail-Kommunikation.Das PGP-Verfahren basiert auf der asymmetrischen Verschlüsselung von Rivest-Shamir-Adleman (RSA).

[54] vgl. http://www.a-trust.at/html/lexicon.asp?ch=1&lang=GE&letter=H#Hashwert (10.01.08)
[55] vgl. Hühnlein, Detlef : Grundlagen der elektronischen Signatur

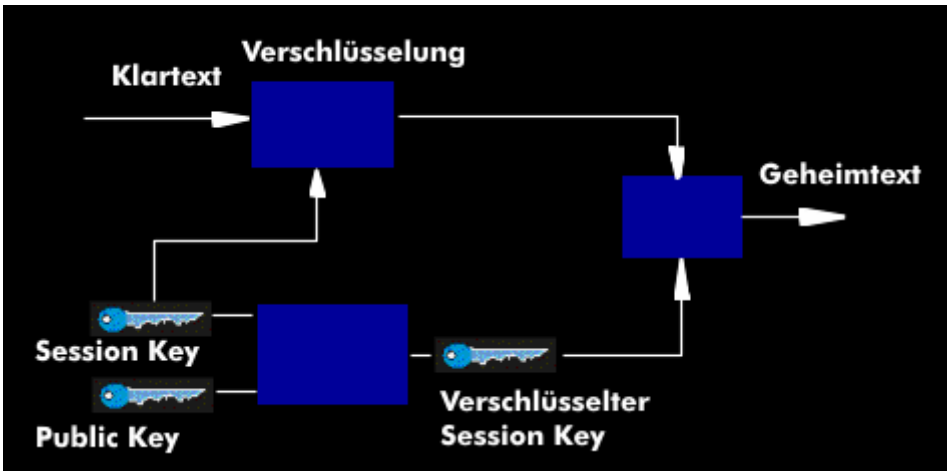

Abb. 9. PGP Verfahren[56]

Wie Abb. 9 belegt werden bei diesem Verfahren zwei Schlüssel generiert: ein privater und ein öffentlicher Schlüssel. Mit dem öffentlichen Schlüssel wird der Klartext zum Geheimtext verschlüsselt. Der jeweilige Nutzer kann diese Nachrichten mit seinem privaten Schlüssel entschlüsseln. Bei der Verschlüsselung selbst wird die Klartextdatei komprimiert und mit dem Session Key, der zufallsbedingt erzeugt wird, verschlüsselt. Darüber hinaus wird der Session Key mit dem öffentlichen Schlüssel verschlüsselt und zusammen mit dem Geheimtext übermittelt.

Beim PGP-Verfahren erfolgt der Schlüsselaustausch auf Vertrauensbasis zwischen den Partnern, die sich gegenseitig als vertrauenswürdig zertifizieren. PGP ist wegen der dezentralen Handhabung bei Internet-Nutzern weit verbreitet. Pretty Good Privacy kann für digitale Signaturen benutzt werden, mit ihr können Dokumente und Mitteilungen verschlüsselt und fälschungssicher unterschrieben werden. [57]

3.3.2 Privacy Enhanced Mail (PEM)

PEM ist ein Standard, der in das bestehende E-Mail Programm integriert ist Es erweitert bestehende E-Mail-Standards um Vertraulichkeit, Authentizität, Unleugbarkeit des Ursprungs und Integrität der Nachricht. Mit PEM gesicherte Dokumente eignen sich für den Datentransport über Netze und zur Signaturprüfung. Darüber hinaus akzeptiert das PEM-Protokoll digitale Zertifikate nach X.509.
PEM hat sich im Vergleich zu S/MIME in der Praxis nicht durchgesetzt und wird kaum verwendet.

[56] Quelle: http://www.itwissen.info/media/lex_pics/ha10g28.png
[57] vgl. http://www.itwissen.info/definition/lexikon , Kryptografie , 12.01.2008

3.3.3 Secure multipurpose Internet mail extensions (S/MIME)

S/MIME wurde zur Verschlüsselung und Authentifizierung von E-Mails entwickelt. Es ist eine Erweiterung der MIME- Spezifikation um die Funktionen Verschlüsselung und Signierung, wobei hier nur mit Zertifikaten (auch X.509) gearbeitet wird.

Abb. 10. MIME Spezifikationen[58]

Bei der Übertragung wird die Datei, wie in Abb. 10 dokumentiert ist, im Header beschrieben. Damit die Daten für alle Computer und Betriebssysteme interpretierbar werden, werden sie vor dem Versenden codiert. Die im ASCII-Zeichensatz und im erweiterten Zeichensatz verwendete 8-Bit-Codierung wird daher auch in einen 7-Bit-Code und einen 6-Bit-Code umgerechnet.

Der Vorteil von S/MIME ist, dass es von den führenden E-Mail Programmen unterstützt wird (z.B. MS Outlook, Outlook Express, Netscape, u.a.)

3.3.4 Public Key Infrastruktur (PKI)

Unter einer Public-Key-Infrastructure[59] (PKI) versteht man eine Umgebung, in der Services zur Verschlüsselung und digitalen Signatur auf Basis von Public-Key-Verfahren[60] bereitgestellt werden. Eine Public-Key-Infrastruktur wird durch die Gesamtheit aller Einheiten, die zum Verwalten der öffentlichen Schlüssel benötigt werden, gebildet.

[58] Quelle: http://itwissen.info/media/lex_pics/kb12t10.png
[59] siehe auch http://mentana.de/cms/index.php
[60] vgl. Eren, Evren : Mobile Security

Bei dieser Sicherheitsstruktur wird der öffentliche Schlüssel eines Zertifikatnehmers (ZN) mit den entsprechenden Identifikationsmerkmalen durch eine digitale Signatur von einer Zertifizierungsinstanz (CA) autorisiert.
Die beiden Schlüsseln (öffentlicher und privater Schlüssel) haben ein typische Länge von 1024 und 2048 Bit.

Die nächste Darstellung (Abb. 11) zeigt die PKI-Architektur, die aus vier Instanzen besteht:

- Policy Certification Authority (PCA)
- Certification Authority (CA)
- Registration Authority (RA)
- Zertifikatnehmer

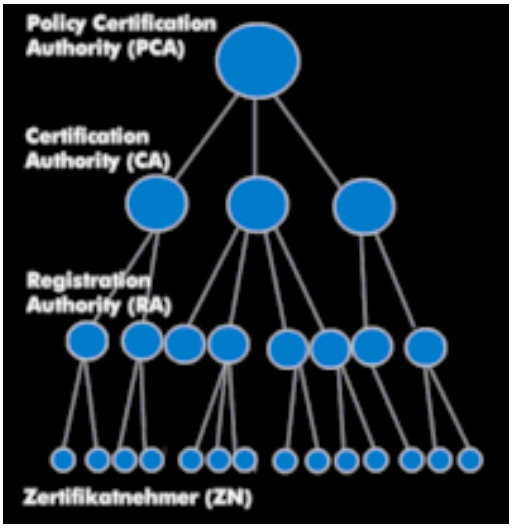

Abb. 11. PKI-Architektur [61]

Die Sicherheitsinfrastruktur muss für den Endbenutzer transparent sein, aber die genauen Abläufe des Schlüssel- und Zertifikatmanagements sollten für den Benutzer unsichtbar bleiben. Jener sollte aber trotzdem auf eine einfache Art und Weise auf alle Services Zugriff haben.

3.3.5 Public-Key-Verfahren

Das Public-Key-Verfaren ist ein asymmetrisches Verschlüsselungsverfahren zur Verschlüsselung und Entschlüsselung von Daten. Das Public-Key-Verfahren kann zur vertraulichen Kommunikation benutzt werden, aber auch für die digitale Signatur.

[61] Quelle: http://www.itwissen.info/media/lex_pics/small/ha10g13.png

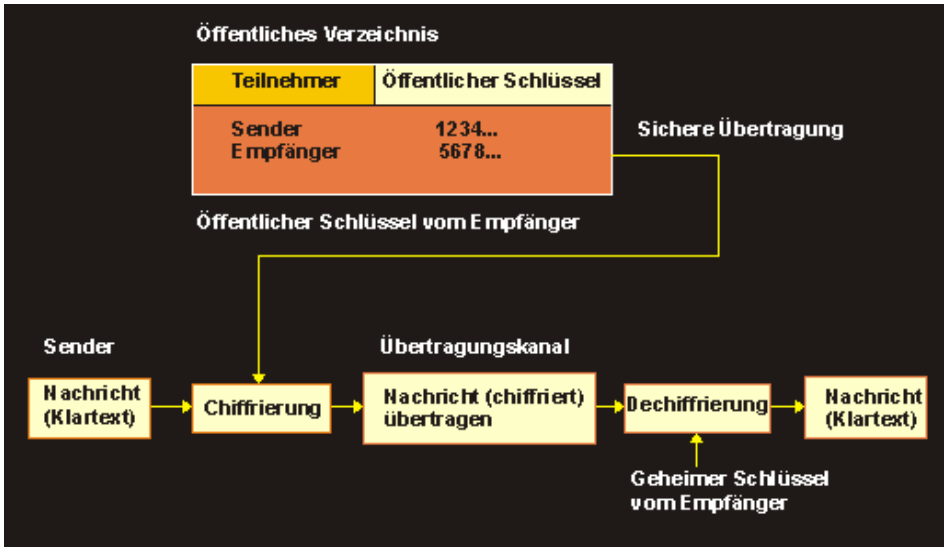

Abb. 12. PKI - Verfahren[62]

Bei diesem Verfahren werden zwei verschiedene Schlüssel verwendet: Der Public Key, der öffentlich zugänglich sein kann, und der Private Key, der privat und geheim und nur dem Inhaber bekannt ist.

Der eine Schlüssel wird zum Verschlüsseln verwendet, der zweite wird vom Inhaber benutzt, um die mit dem öffentlichen Schlüssel verschlüsselten Daten zu entschlüsseln oder zu signieren.

Die beiden Schlüssel sind nicht voneinander ableitbar. Daher kann ein Schlüssel öffentlich bekannt gegeben werden (Public Key). Die Verschlüsselung des Klartextes erfolgt durch den öffentlichen Schlüssel in Kombination mit einem mathematischen Algorithmus. Die Entschlüsselung erfolgt durch einen geheimen Private Key, den nur der Empfänger kennt.

3.3.6 mPKI (mobile PKI)

In unserem Fall wäre die mPKI[63] von großem Interesse. Bei der mPKI verschlüsselt und signiert der Benutzer Verträge, Bestellaufträge und Eingangsbestätigungen nicht über den Stand PC, sondern mobil per Handy [64]. Der Vorteil dabei ist, dass man einerseits als Kartenlesegerät das Handy verwenden kann. Die SIM Karte bietet auch genug Speicherplatz und Möglichkeit sensible Verschlüsselungsdaten zu speichern.

[62] Quelle: http://www.itwissen.info/media/lex_pics/small/ha10g10.png
[63] vgl.Eren, Evren : Mobile Security
[64] vgl. http://download.microsoft.com/download/a/b/c/abc6dd0c-2f81-4678-8ca8-6883ff42fb45/Markus_Tak.pdf

4 Mobile elektronische Signaturen

In diesem Kapitel werden die mobilen elektronischen Signaturen[65] behandelt. Hierzu wird der Aufbau der Smartcards genau analysiert und auf die Architektur eingegangen. Weiters zeigt uns dieses Kapitel die Brücke zwischen den mobilen Funknetzen (GSM-Netze) und der elektronischen Signaturen. Um das ganze nun zu veranschaulichen, stelle ich dies anhand von einigen aktuellen Anwendungsbeispielen dar.
Am Ende dieses Kapitels gehen wir auf das Netz der Zukunft ein, welches auch unter dem Namen Future Net bzw. Next Generation Network (NGN) bekannt ist.

4.1 Smartcards

Dieser Abschnitt widmet sich den Smartcards[66]. Als Geburtsstunde der Chipkarte gilt das Jahr 1974, indem dem französischen Wirtschaftsjournalisten R. Moreno ein Patent für ein „System zur Speicherung von Daten in einem unabhängigen, tragbaren Gegenstand“ erteilt wurde. Die heutige Chipkarte ist eine Plastikkarte, die in unterschiedlichen Ausprägungen vorkommt.

Durch das sich schnell verbessernde Preis/Leistungsverhältnis von Smartcards kommt diesen bereits heute eine große Bedeutung als Sicherheitswerkzeug und besonders als Mittel zur Authentifikation zu. Smartcards sind in verschiedenen Bereichen einsetzbar, als Geldkarte oder Visa-Cash Karte oder als SIM-Karte in Handys.

4.1.1 Architektur einer Smartcard

Die Struktur einer Smartcard wird durch die ISO Standards 7810, 7816-1 und 7816-2 festgehalten. Die Smartcard ist eine Plastikkarte mit den Dimensionen 85.60 * 53.98 * 0.80 mm. In dieser so genannten Plastikkarte ist eine Schaltung integriert. Die Kontakte zwischen den Komponenten werden durch gegenseitige Berührung und nicht durch Kabel hergestellt. Diese Schaltung, wie in Abb. 13 sehr gut ersichtlich, besitzt alle Teile eines vollwertigen Computers. Diese wird als Mikrocontroller [67] (MCU - Micro Controller Unit) bezeichnet.

[65] siehe auch http://mediakomm.difu.de/documents/forschung/mobile---signatur.pdf
[66] vgl. Sauter, Martin : Grundkurs Mobile Kommunikationssysteme
[67] vgl. Eckert, Claudia : IT-Sicherheit

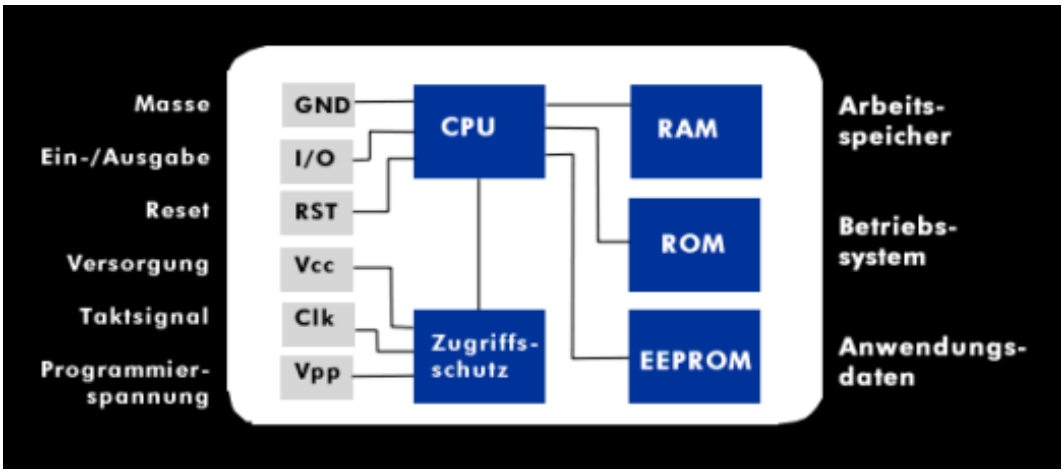

Abb. 13. Chipkarten (Smartcard) Architektur[68]

4.1.1.1 Smartcard – Mikrocontroller

Der Mikrocontroller[69] ist der zentrale Baustein der Chipkarte. Wie man in Abb. 13 sehen kann, besitzt sie eine große Ähnlichkeit mit der Architektur eines Standard PCs. Sie besteht aus einer CPU, einem ROM (Read Only Memory), einem RAM (Random Acess Memory), Eingabe/Ausgabe-Kanälen sowie einem EEPROM (Electronically Eraseable Programmable ROM) Speicher, dessen Aufgabe mit der einer Festplatte vergleichbar ist.

Die Industrie verwendet meisten den Mikrocontroller Intel 8051 oder den Motorola 6805, die preisgünstig und zuverlässig sind. Es werden zunehmend 16- und 32-Bit-Architekturen verwendet um die hohen Anforderungen an die Rechenleistung von Smartcards zu sättigen, die zum Beispiel für kryptografische Funktionen notwendig sind. Für einfache Verschlüsselungsalgorithmen sind auch 8-Bit-Prozessoren ausreichend.

Da die Größe des Controllers nicht mehr als 25 mm² betragen darf, ist eine hohe Dichte von Bauelementen notwendig. Durch eine höhere Dichte wird auch der Stromverbrauch gesenkt.

[68] http://cgi.zdnet.de/glossar/i/small/ii10g10_t.png
[69] Quelle: http://www.seccomerce.com/de/fachwissen/technologie/smartcards/smartcards_architektur.html

4.1.1.2 Mikrocontroller für Sicherheitsanwendungen

Ein Mikrocontroller, der speziell für Sicherheitsanwendungen ausgelegt ist, wird als Security Controller[70] bezeichnet. Für Signaturkarten werden hauptsächlich die 16-Bit-Security-Controller der Serien SLE 66C und SLE 66CX von Infineon eingesetzt. Das X bedeutet, dass es sich um einen Kryptocontroller handelt. Die darauf folgende Zahl bezeichnet die EEPROM-Größe des Controllers (z. B. SLE 66CX160P: 16 KByte EEPROM). Wenn die Produktbezeichnung auf "P" oder "PU" endet, verfügt der Controller zusätzlich über eine Speicherverwaltung, eine Schutzeinheit und einen DES-Beschleuniger.

Ein weiterer Hersteller von Security Controllern ist Philips Semiconductors. Die 8-Bit-Controller der P8WE50- und P8WE60-Familien verfügen über bis zu 32 KByte EEPROM und einen integrierten DES-Koprozessor. Die Produktlinie P8WE50 ist als Kryptocontroller realisiert. Ein Kryptocontroller ist ein Security Controller mit zusätzlichen Fähigkeiten zur schnellen Ausführung kryptografischer Funktionen. Die Algorithmen werden auf einem zusätzlichen Prozessor, dem Krypto-Koprozessor, ausgeführt.

Die Infineon-Kryptocontroller der SLE 66CX-Serie enthält einen Koprozessor, der als Advanced Crypto Engine bezeichnet wird. Er kann alle heute bekannten Public-Key-Algorithmen ausführen, darunter RSA-Operationen mit einer Schlüssellänge von bis zu 2048 Bit.

Die 16-Bit-Kryptocontroller der neuen SmartXA-Serie besitzen eine integrierte Hardware-Firewall und können bis zu 16 MByte ausführbaren Code adressieren. Die Mikrocontroller Infineon SLE C164P, 66CX640P, -320P, -160M und -160S sowie Philips P8WE6017V1I und P8WE5032VOG haben das ITSEC-Zertifikat E4/hoch erhalten. Sie dürfen in Signaturkarten eingesetzt werden, mit denen qualifizierte elektronische Signaturen erzeugt werden.

[70] vgl. http://www.seccomerce.com/de/fachwissen/technologie/smartcards/smartcards_architektur.html

Die folgende Tabelle (Tabelle 2) zeigt, welche Mikrocontroller für signaturgesetzkonforme Smartcards verwendet werden:

Signaturkarte	Mikrocontroller
TeleSec PKS-Card ,Version 2.0	Infineon SLE 66CX160S
TeleSec PKS-Card, Version 3.0	Infineon SLE 66CX320P
Signtrust SEA-Card, Version 1.0	Infineon SLE 66CX160S
Signtrust SEA-Card, Version 2.0	Infineon SLE 66CX320P
DATEV e:secure-Card, Version 1.0	Infineon SLE 66CX320P
STARCOS SPK 2.3-Signaturkarte	Philips P8WE5032V0G

Tabelle 2. Signaturkarten und verwendete Mikrocontroller[71]

4.1.1.3 Mikroprozessor und Koprozessoren

Der Mikroprozessor ist das Herz des Controllers, auch als CPU (Central Processing Unit) bezeichnet.

Fortgeschrittene Karten können über zusätzliche Komponenten, die Additional Units (AU), verfügen. Ein Beispiel ist ein Koprozessor zur beschleunigten Ausführung modularer Arithmetik oder zur Beschleunigung der Exponentationen, die beim RSA-Verfahren benötigt werden.

Für kryptografische Algorithmen haben möglichst gute, d. h. möglichst zufällige Zufallszahlen eine große Bedeutung. Die Generatoren auf Smartcards nutzen z. B. das Rauschen einer Diode zur Gewinnung zufälliger Werte.

4.1.2 Kontakte einer Smartcard

Wie man in Abb. 14 sehen kann, ist die goldene Fläche auf der Oberseite einer Smartcard in acht Kontaktfelder[72] unterteilt.

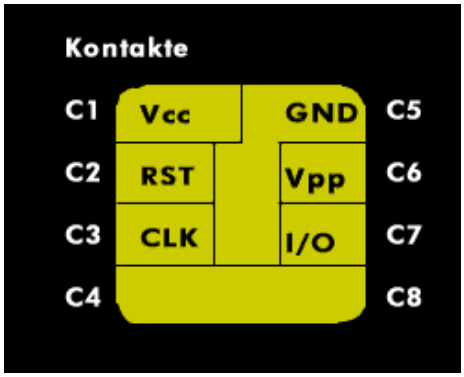

Abb. 14. Kontakte einer Smartcard

[71] Quelle: http://www.seccomerce.com/de/fachwissen/technologie/smartcards/smartcards_architektur.html - Tabelle
[72] vgl. http://www.seccomerce.com/de/fachwissen/technologie/smartcards/smartcards_architektur.html

Das Unternehmen Sec-Commerce[73] beschäftigt sich mit den Kontaktfeldern und Speicherbausteinen einer Smartcard und definiert diese wie folgt:

4.1.2.1 C7 - I/O-System

Die Kommunikation zwischen der CPU und dem Lesegerät erfolgt über das I/O Kontaktfeld Bei der Übermittlung von Daten von der Smartcard zum Lesegerät werden die Daten an eine bestimmte Speicheradresse geschrieben. Diese Adresse wird jedoch nicht durch ein wirkliches Speichermodul, sondern durch das I/0-System belegt, das mit den Kontakten der Smartcard verbunden ist. Die Datenübertragung erfolgt seriell im Halbduplex-Verfahren, da nur ein I/0-Kontakt[74] vorhanden ist. Das heißt, dass Karte und Lesegerät nicht gleichzeitig Daten austauschen können, sondern es kann nur ein Bit übertragen werden.

4.1.2.2 C6 – Vpp – Programmierspannung

Frühere Karten wurden für das Beschreiben des EEPROM-Moduls mit einer Programmierspannung von ca. 20 V versorgt. Heutige Smartcards erzeugen die Programmierspannung über kaskadierende Spannungsverdopplung aus der Vcc-Spannung. Auf diese Weise werden Angriffe verhindert, bei denen der Schreibvorgang durch eine Änderung der Programmierspannung manipuliert wird.

4.1.2.3 C1 - Vcc – Versorgungsspannung

Über diesen Kontakt wird die Smartcard mit der für den Betrieb nötigen Spannung versorgt. Moderne Smartcards arbeiten mit Spannungen von 2,7 bis 5,5 V. Die Stromstärke beträgt maximal 10 mA. Bei 5 V und 10 mA beträgt die Leistungsaufnahme 50 mW.

4.1.2.4 C3 - CLK – Takt

Normalerweise sind Smartcard-Controller auf eine externe Taktquelle angewiesen, da der Quarz aufgrund seiner Größe nicht auf der Karte untergebracht werden kann. Moderne Controller können mit externen Taktfrequenzen von ca. 1 bis 8 MHz betrieben werden. Einige Controller verdoppeln diese Rate und arbeiten mit internen Taktraten von bis zu 15 MHz.

[73] vgl. http://www.seccomerce.com/de/fachwissen/technologie/smartcards/smartcards_architektur.html
[74] vgl. http://www.cosy.sbg.ac.at/~uhl/crypto/Asmartcards.pdf.gz

4.1.2.4 C2 - RST – Reset

Das Reset-Signal wird für die Bootsequenz und zum Zurücksetzen der Karte in den Ausgangszustand verwendet. RST ist aktiv, wenn keine Spannung anliegt.
Die Kontakte C4 und C8 sind für zukünftige Ausprägungen reserviert.

4.1.3 Speicherbausteine einer Smartcard

Die Speicherbausteine[75] einer Smartcard sind wie auch von der Firma Sec-Commerce[76] beschrieben wie folgt aufgebaut:

4.1.3.1 ROM (Read Only Memory)

Auf ROM-Bausteine kann nur lesend zugegriffen werden. Das Betriebssystem der Smartcard wird in einem ROM-Modul gespeichert. Alle Karten einer Baureihe besitzen das gleiche Betriebssystem, d. h. der Inhalt der Betriebssystem-Bausteine ist identisch. Moderne Controller besitzen bis zu 136 KByte ROM. Dieser Speicher kann teilweise für Anwendungsprogramme genutzt werden, die bei der Chipherstellung integriert werden.

4.1.3.2 RAM (Random Access Memory)

Der Arbeitsspeicher einer Smartcard wird durch RAM-Module realisiert. Der Inhalt dieser Module ist flüchtig, d. h. die Daten gehen nach dem Beenden der Sitzung verloren. Da RAM-Bausteine recht groß sind, besitzen auch moderne Controller nur bis zu 5 KByte RAM. Die Zugriffszeit beträgt ca. 70 ns. Smartcard-Controller verwenden statische RAM. Diese Bausteine müssen nicht ständig mit einem Takt versorgt werden, das Abschalten des Taktsignals bedeutet keinen Datenverlust.

4.1.3.3 EEPROM

EEPROM-Bausteine (Electrically Erasable Programmable Read Only Memory) können im Unterschied zu ROM-Bausteinen beschrieben werden. Allerdings ist die Anzahl der Schreibzyklen begrenzt, eine moderne EEPROM-Speicherzelle kann zwischen 100.000 und 500.000 Mal beschrieben werden. Die Stabilität der gespeicherten Daten ist zeitlich begrenzt. Die meisten Hersteller garantieren eine Speicherdauer von 10 Jahren.

[75] vgl. Heinrich, Volker : Handy global
[76] vgl. http://www.seccomerce.com/de/fachwissen/technologie/smartcards/smartcards_architektur.html

Aufgrund der relativ hohen Zugriffszeit von ca. 3-5 ms können EEPROM-Module nicht als Arbeitsspeicher genutzt werden. Zur Speicherung von Kundendaten wie Signaturschlüssel und Zertifikate sind sie dagegen sehr gut geeignet. Die Funktion eines EEPROM-Bausteins entspricht der einer Festplatte in einem Desktop-Computer. Security Controller besitzen normalerweise einen nur einmal beschreibbaren EEPROM-Bereich ("write once area", "security area"), der zur sicheren Aufbewahrung von Daten, z. B. von Signaturschlüsseln, genutzt werden kann.

4.2 SIM - subscriber identity module

Die SIM Karte entspricht im Aufbau einer Smartcard mit CPU, Festwertspeicher, Arbeitsspeicher, Bussystem und Schnittstellen über ein Kontaktfeld.

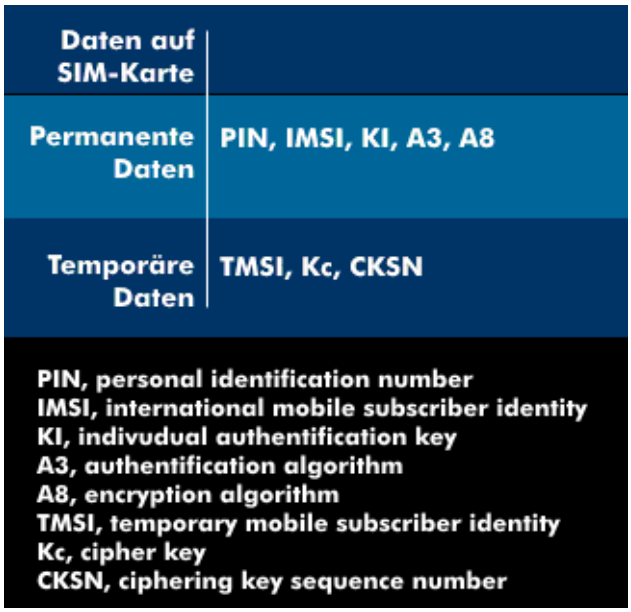

Abb. 15. Daten auf der SIM Karte[77]

Trotz ihrer geringen Größe ist die SIM Karte ein wichtiger Bestandteil des GSM Netzwerkes. Da sie alle Daten eines Teilnehmers, wie in Abb. 15 aufgelistet, enthält, kann der Teilnehmer mit seiner SIM Karte jedes beliebige GSM Endgerät verwenden. Die wichtigsten Informationen auf der SIM Karte sind die internationale Teilnehmernummer (IMSI – International Mobile Subscriber Identity), die internationale Identifikationsnummer für das Mobilgerät (IMEI), die persönliche Identifikationsnummer (PIN) sowie dessen geheimer Schlüssel (Ki), der für die Authentifizierung und Generierung des Verschhlüsselungskeys (Kc) benötigt wird.
Mit diversen im Internet kostenlos erhältlichen Tools können alle nicht lesegeschützten Informationen herausgelesen werden. Abbildung 16. zeigt ein solches Tool.

[77] http://www.itwissen.info/media/lex_pics/small/cc33t15.png

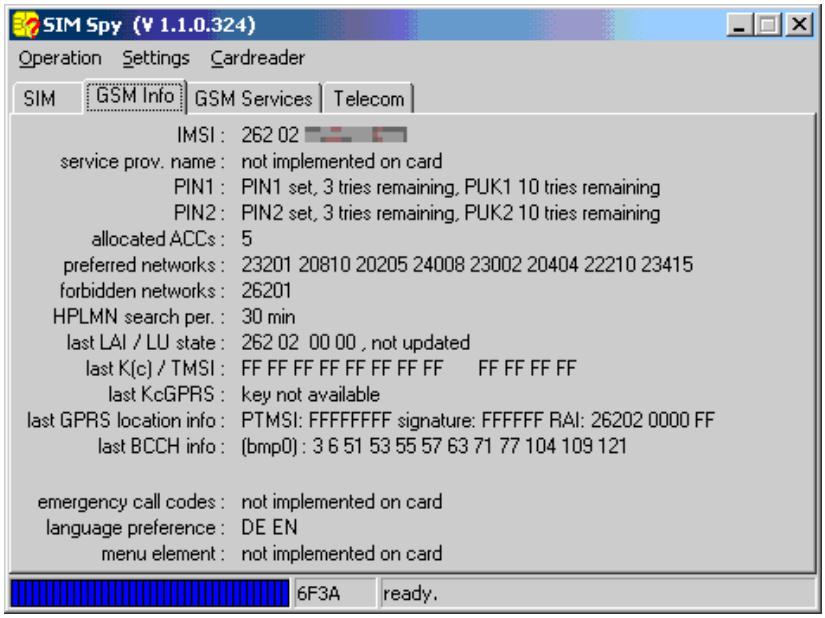

Abb. 16. Sim Spy (Herauslesen der Sim Daten)[78]

Mit der SIM Karte für das GSM-Netz identifiziert sich der Teilnehmer mit seiner Funktelefon-Rufnummer, der MSISDN. Mit Hilfe der Authentifikation stellt das Netz sicher, dass es sich tatsächlich um einen autorisierten GSM-Teilnehmer handelt. Das Authentifizierungsverfahren wird parallel auf der SIM Karte und im Netz durchgeführt und im Ergebnis verglichen. Bei Ergebnisgleichheit ist die Teilnehmerauthentizität gewährleistet.

4.2.1 Signatur auf der SIM-Karte (mSign)

Im Mobilfunkbereich ist die Smartcard nicht unbedingt der ideale Träger für die digitale Signatur. Man bräuchte immer ein zusätzliches Mobilgerät[79] bei sich. Bei Handys bietet sich deshalb die ohnehin im Mobiltelefon vorhandene SIM Karte (Subscriber Identification Module) als Speichermedium für den geheimen Schlüssel an. Der Vorteil ist dass jedes Mobil-Telefon seine eigene Karte mit einem identifizierbaren Code besitzt, so verlässt der Schlüssel die Karte nicht und erzeugt damit eine hohe Sicherheit.

Noch eine Zusatzoption dabei ist, dass bei Verlust die Karte in kürzester Zeit (d.h. in wenigen Sekunden) gesperrt werden kann und dadurch vor unbefugtem Zugriff geschützt werden kann.

[78] http://www.nobbi.com/simspy/sisp_gsm01.png
[79] siehe auch http://allpr.de/16210/Finnland-setzt-auf-mobile-Signatur-bei-eGovernment-Diensten-Giesecke-Devrient-liefert-die-SIM-Karten-mit-Sicherheitszertifikat.html

Ziel des Konsortiums ist es, einen weltweiten De-facto-Standard für den Einsatz von Signaturen über Mobiltelefone zu definieren. Die Mitglieder einigten sich auf ein Protokoll, das diese Schnittstelle zwischen E-Commerce-Anbietern und dem Mobilfunkbetreiber definiert. Für die Signatur mit Mobiltelefonen wird dazu eine generische Signaturapplikation[80] auf der SIM Karte installiert.

Mit Hilfe des Brokat-M-Trust-Server [81] können Mobilfunkbetreiber einen Service anbieten, der es Dienstleistern ermöglicht, mobile Signaturen zur einfachen und sicheren Authentifizierung von Kunden zu nutzen.

Durch ein so genanntes Trustcenter wird der User identifiziert. Dabei spielt ein unabhängiger Dritter eine große Rolle, der die Codes von Händler und Kunde mit seiner eigenen Signatur (diese Signatur muss mit qualifizierten Tools hergestellt werden) beglaubigt. Eine Lösung ist das so genannte Instant Contracting. Vertragspartner, die sich nicht persönlich kennen, können auf diese Weise ad hoc gültige Verträge abschließen und digital signieren.

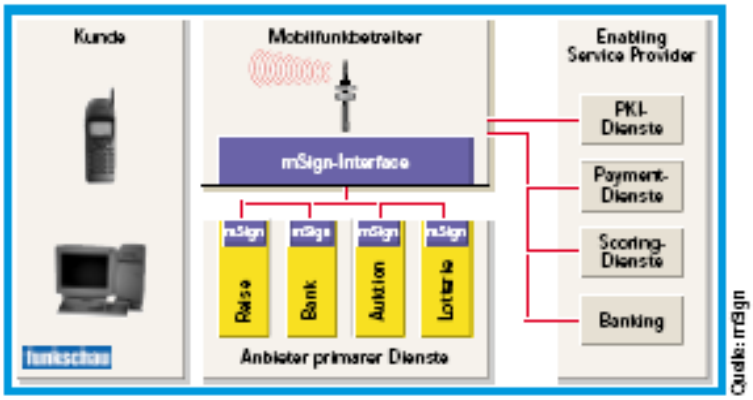

Abb. 17. Das m-Sign Interface[82]

Das Konsortium hat bereits ein Protokoll zur Nutzung der mobilen digitalen Signatur erstellt, das die Schnittstellen zwischen den Mobilfunkbetreibern und den Dienstanbietern definiert. Das mSign-Protokoll ist ein standardisiertes Interface, das die Kommunikation zwischen Mobilfunk-Anbietern und Servicediensten wie Banken oder Behörden regelt. Abbildung 17 zeigt das Interface mit den Verbindungen.

[80] vgl. Mobile digitale Kommunikation : Standards, Netze und Applikationen , Helge Grote
[81] siehe http://en.wikipedia.org/wiki/Brokat
[82] http://funkschau.de/heftarchiv/pdf/2001/fs1301/fs0113060.pdf

Das Mobile Electronic Signature Consortium (mSign), dessen Aufgabe es war, eine sichere applikationsübergreifende Infrastruktur für den Einsatz mobiler Signaturen zu entwickeln, hat im Jahre 2000 eine Lösung für mobile Signaturen vorgestellt. Hierbei handelt es sich um einen Dienst, der die eigentliche Signaturerstellung an einen Signierserver delegiert.

Die mSign Lösung ist zusätzlich an unzureichender Technik gescheitert und mittlerweile in Raddiccio integriert. Vielversprechender erscheint hier der Ansatz zu sein, eine Lösung auf Basis einer signaturfähigen SIM Karte anzustreben. Mit der WIM Spezifikation der Open Mobile Alliance (OMA) existiert bereits ein technisch ausgereifter Standard und im Rahmen des EU-Projektes „Wireless Trust for mobile Business“ (WiTness) wurde eine solche signaturfähige SIM Karte entwickelt. Eine mobile Signatur auf Basis einer signaturfähigen und nach Common Criteria evaluierten SIM Karte würde die Anforderungen durch das SigG erfüllen. Bisher konnte sich die WIM aufgrund fehlender Geschäftsmodelle noch nicht am Markt etablieren, aber es wurde eine flexible Zertifizierungsmöglichkeit vorgestellt, die im Folgenden kurz dargestellt wird.

4.2.2 Certification on Demand (CoD)

Herr HeikoRossnagel und Hr. Lothar Fritsch geben in einer Publikation unter dem Titel: „Die Krise des Signaturmarktes: Lösungsansätze aus betriebswirtschaftlicher Sicht“[83] folgenden Beitrag ab:
Bei diesem Konzept wird der Vertrieb von signaturfähigen Smartcards in die Vertriebsstruktur der Mobilfunkprovider eingegliedert, ohne dass die Kunden an ein bestimmtes Trust Center gebunden werden. Dazu werden beim Smartcard-Hersteller, zusätzlich zur Teilnehmerkennung IMSI und dem individuellen Schlüssel Ki, ein Schlüsselgenerator für Signaturschlüsselpaare und der öffentlichen Schlüssel der RootCA auf die SIM Karte aufgebracht. Der Mobilfunkprovider übergibt dann die Karte zusammen mit einem Nullpin zur Aktivierung der Signierfunktion, seinem Kunden, der sofort nach Erhalt die Telefon- und Datenübertragungsfunktion nutzten kann. Interessiert sich der Kunde auch für die Signaturfunktion, kann er sich bei einer Registrierungsstelle identifizieren lassen und seinen öffentlichen Schlüssel hinterlegen. Außerdem übermittelt der Kunde seine mit dem privaten Schlüssel chiffrierten

[83] Quelle: http://www.is-frankfurt.de/publikationenNeu/DieKrisedesSignaturmarktesLoes1143.pdf

Identifikationsdaten an das Trust Center. Gleichzeitig übermittelt die Registrierungsstelle den öffentlichen Schlüssel und die Identifikationsdaten des Kunden an das Trust Center. Stimmen die von der Registrierungsstelle übermittelten Daten mit den vom Kunden übermittelten Daten überein, stellt das Trust Center ein Zertifikat aus und sendet es direkt an das mobile Endgerät.

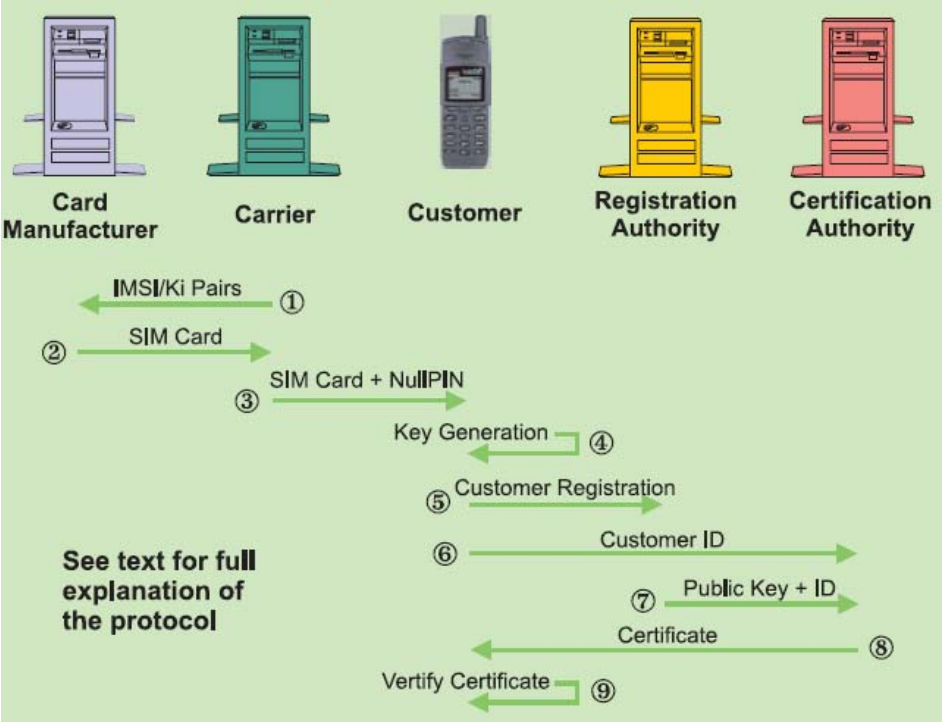

Abb. 18. Certification on Demand (CoD)[84]

Durch das von der RootCA für das Trust Center ausgestellte Zertifikat kann der Kunde die Gültigkeit seines Zertifikates überprüfen. Dadurch könnten auch völlig neue Geschäftsfelder erschlossen werden, beispielsweise im Zusammenhang mit Location Based Services. Daher ist für Kunden von mobilen Signaturen ein kundenspezifischer Nutzen vorhanden (Mobilität des Signiermittels). Auch die Rüstkosten sind als relativ gering zu betrachten, da lediglich eine neue SIM Karte mit Kryptofunktionalität, sowie eine Signatursoftware zusätzlich zum vorhandenen Mobiltelefon notwendig sind. Diese Anschaffungskosten könnten wiederum vom Mobilfunker subventioniert werden, der durch den durch mobile Signaturapplikationen entstehenden Traffic Gewinne erzielen kann.

Durch die nachträgliche Zertifizierung mit COD[85] entstehen beim Wechsel zu einem anderen Zertifizierungsanbieter kaum Wechselkosten. Auch die Eigenschaft der

[84] http://www.wiiw.de/publikationen/EnablingMobileQualifiedElectro1125.pdf
[85] vgl. http://www.is-frankfurt.de/publikationenNeu/EnablingMobileQualifiedElectro1125.pdf

Ausprobierbarkeit ist mittels Certification on Demand, wie Abb. 18 zeigt, gegeben, da der potentielle Nutzer die Signaturfunktionalität erproben kann, bevor Kosten für die Zertifizierung entstehen.

4.2.2 (U)SIM Plattform

STARSIM und UniverSIM, wie in Abb. 19 dargestellt, sind G&D's SIM Karten für die zweite und dritte Generation der mobilen Kommunikation.

Abhängig von seinem Netzwerk (GSM, UMTS, GPRS) kann der Netzbetreiber aus einer breiten Palette an Karten mit unterschiedlichen Speichergrößen, Sicherheitsmerkmalen und weiteren Komponenten wie zum Beispiel Micro-Browsern und der WIM seine ganz spezielle Auswahl treffen.

Sowohl STARSIM als auch UniverSIM sind auf G&Ds nativem Betriebssystem und auch auf Basis der Java™ Card Technologie verfügbar.

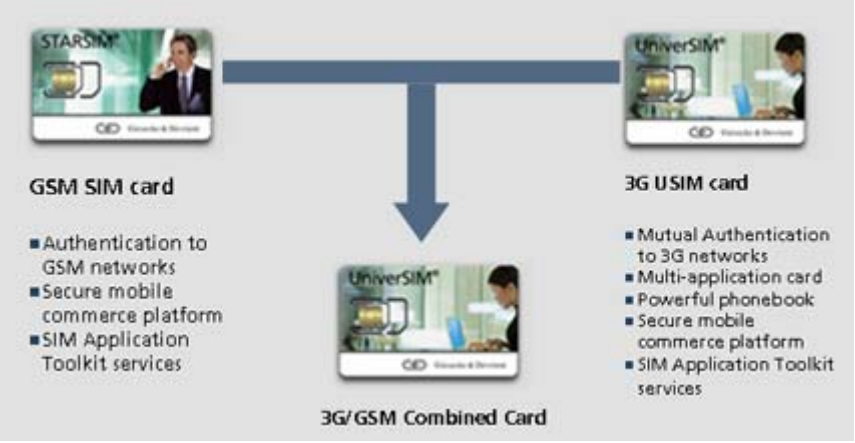

Abb. 19. Sim Karte vs Usim Karte[86]

Die Java-Card-Technologie [87] ermöglicht es, Java-Programme auf Smartcards zu installieren und auszuführen. Auch andere Geräte, die mit vergleichsweise wenig Speicher und CPU-Leistung auskommen müssen, gehören zur Zielgruppe von Java Card.

Sun Microsystems entdeckte das Potenzial von Smartcards und entwickelte eine Applikation für Smartcards, nämlich Java Card Applets. Dieses wird durch Java Card

[86] siehe G&D Homepage, http://www.gi-de.com
[87] vgl. Knuth, Michael : Web Services

Plattform unterstützt. Auf diese Plattform können unterschiedliche Applikationen abgespielt werden.

Ein Java Card Gerät besitzt eine 8- oder 16-bit CPU mit 3.7MHz, 1K RAM und über 16K EEPROM oder Flash (non-volatile memory). High-Performance Smartcards besitzen separaten CPU mit einem kryptografischen Chip und Speicherplatz zur Verschlüsselung, und andere mit 32-bit CPU.

Die Java Card Technologie Version 2.2 besteht aus drei Komponenten:

- Java Card Virtual Machine (VM): definiert eine Untergruppe für die Java Programmierungssprache und eine virtuelle Umgebung (VM) für Smartcards.
- Java Runtime Environment: definiert die Laufzeit für Java basierte smart cards.
- Java Card API: definiert die Hauptrahmenbedingung und die Erweiterung Java Packages und Klassen für Smartcard Applikationen.

Vergleich zwischen Java Card and J2ME Plattformen:

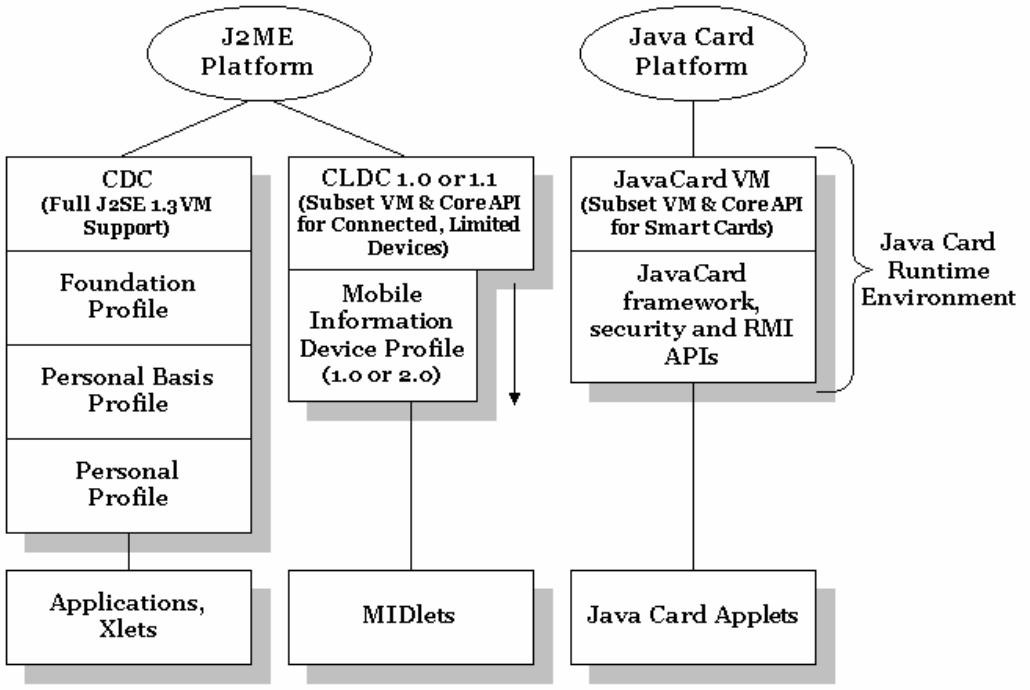

Abb. 20. Vergleich Java Card and J2ME Aufbau [88]

[88] Quelle: http://developers.sun.com/mobility/javacard/articles/javacard1/fig-3.gif

Im Gegensatz zu einer J2ME Plattform, besitzt eine smart card Umgebung ein eigene Plattform, wie man in Abb. 20 sehen kann, nämlich die Java Card Plattform.

Java Card Technologie ermöglicht die Ausführung von so genannten Applets, die die Java Technologie implementieren. Smartcard Hersteller bekommen eine gesicherte Plattform zur Ausführung und Speicherung unterschiedlicher Applikationen auf einem Gerät. Die Java-Card-Technologie ist mit existierenden Smartcard-Standards kompatibel. Diese Technologie bietet Entwicklern die Möglichkeit Applikationen und Services in einer geschützten Umgebung schnell zu entwickeln, zu testen und zu implementieren. Die Vorteile sind: reduzierte Entwicklungskosten, erhöhte Differenzierung von Produkten sowie Erhöhung des Kundennutzens. Java Card Technologie erleichtert die Integration von Sicherheitstokens in eine komplette Java Software Lösung.

Daraus ergeben sich folgende Nutzen:
Vollständige Kompatibilität: Applets mit Java-Card-Technologie ausgestattet, laufen auf alle Java Card Technologie basierte Smartcards, abhängig davon, wer der Hersteller ist.

Sicherheit: Java Card Technologie bietet eine sichere Umgebung. Der Einsatz dieser Technologie bestätigt ihre Fähigkeit und Sicherheit.

Multi-Applikation fähig: Java Card Technologie bietet unterschiedlichen Applikationen Platz auf einer Smartcard.

Dynamisch: neue Applikationen können problemlos auf Smartcards installiert werden. Dies gibt den Herstellern der Smartcard die Möglichkeit schnell auf Kundenanforderungen zu reagieren.

Kompatibilität mit vorhanden Standards: das Java Card API ist mit internationalen Standards (z.B. ISO 7816, EMV, Global Platform, ETSI) für Smartcards kompatibel.

4.2.3 STARSIM für GSM

STARSIM und STARSIM Java™ sind G&Ds SIM Karten für GSM Netze. STARSIM bildet die ideale Basis für flexible, maßgeschneiderte Services und gewährleistet gleichzeitig höchste Sicherheitsstandards.

SIM Application Toolkit (SAT) für STARSIM und die Java™ Card Technologie bieten ein mächtiges Instrumentarium für die Generierung und Implementierung von mobilen Services, die der Netzbetreiber selbst managen kann.

Die Interoperabilität von STARSIM Java™ verleiht Netzbetreibern eine einzigartige Flexibilität. Unabhängig davon, ob eine Java™ Card Anwendung von ihnen selbst geschrieben wurde, von G&D oder von einem Applikationslieferanten, sie läuft auf einer STARSIM Java™ Karte. Die Vorteile sind beträchtlich:

- Kurze Markteinführungszeit für neue Services
- Einfache Applikationsentwicklung
- Kostenreduzierung für das Management von Applets
- An Kundenwünsche anpassbar, auch wenn die SIM Karte schon beim Kunden ist
- Wichtig für Direktmarketing

4.2.4 UniverSIM® für UMTS

UniverSIM und UniverSIM Java™ sind unsere Multiapplikations-Karten für die dritte Generation (3G) der mobilen Telekommunikation. UniverSIM schlägt die Brücke zwischen den verschiedenen Mobilkommunikations-Standards, denn UMTS Nutzer können die UniverSIM Karte in ihren heutigen GSM Handies genauso einsetzen wie in 3G Handies.

UniverSIM (Abb. 21) bietet mächtige kryptografische Funktionen, um die unerlässliche gegenseitige Authentisierung zwischen dem Teilnehmer und dem Netzwerk als innovative 3G Sicherheitskomponente zu liefern.

Abb. 21. USim von G&D[89]

[89] siehe G&D Homepage, http://www.gi-de.com

4.2.3 Vergleich von SIM-Karten

Diese Abbildung (Abb. 22) zeigt einen Vergleich der verschiedenen Sim-Karten. Dabei kann man die Hauptfunktionalitäten, Speichergröße, Unterstützte Netze und Protokolle und die Sicherheit, die von den Karten angeboten wird vergleichen.

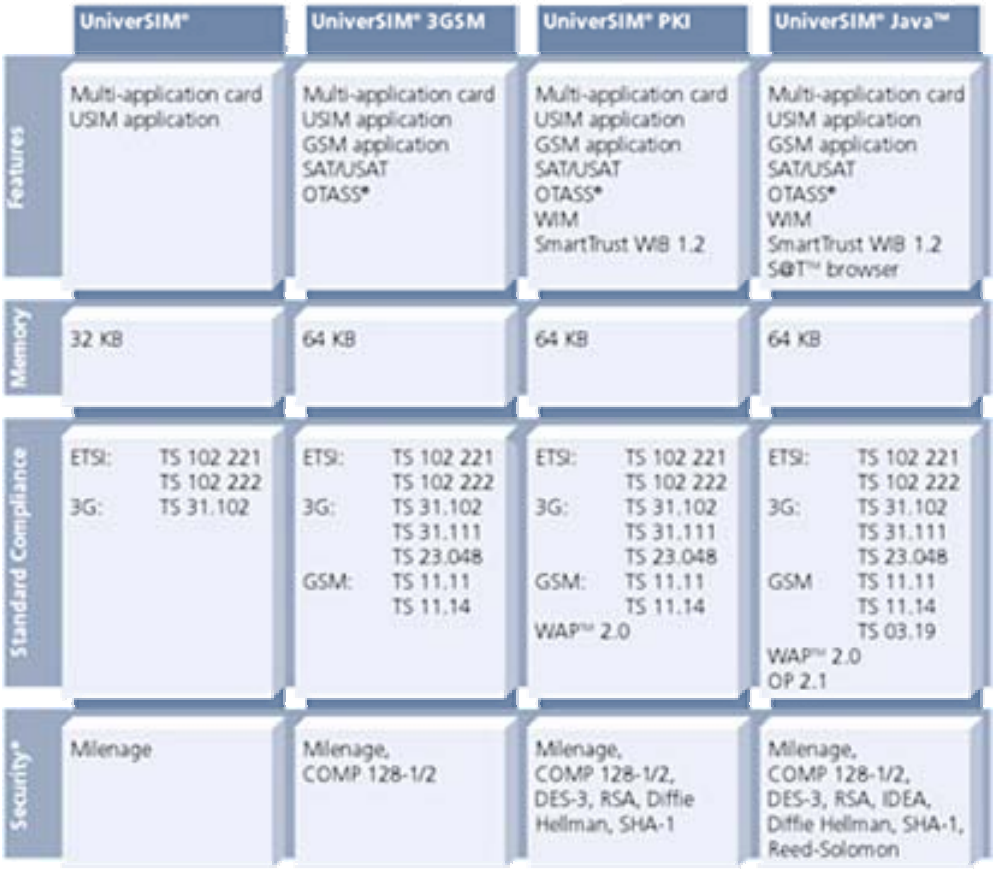

Abb. 22. Vergleich der SIM-Karten[90]

[90] siehe G&D Homepage, http://www.gi-de.com

4.3 Systeme der Mobilkommunikation

Die rapide Entwicklung der Kommunikationstechnologie führt zu einem stetig wachsenden Anstieg der Teilnehmerzahl und der übertragenen Datenvolumina. Im Bereich der Telekommunikation ist die Entwicklung gekennzeichnet durch einen Übergang von einfachen Vermittelungs- und Verbindungsdiensten hin zu mobilen multimedialen Diensten über verschiedene Netzwerke hinweg.

4.3.1 GSM (Global System for Mobile Communications)

Das GSM-System (Global System for Mobile Communication) war die erste weltweite Anwendung chipkartenbasierter Authentifikation. Das GSM-System kann man heutzutage als die größte Sicherheitsinfrastruktur weltweit betrachten. Das GSM ist ein paneuropäischer Mobilfunkstandard, der von 1982 bis 1990 entwickelt wurde. Im März 2004 verzeichnete die GSM Association, wie in Abb. 23 in einer grafischen Darstellung ersichtlich, über 1046,8 Millionen Benutzer des GSM Netzes in mehr als 124 Ländern. Die zellularen GSM-Netze überspannen heute bereits alle Kontinente und werden von mehr als 110 Ländern unterstützt. Damit ermöglichte man ein weltweites Roaming zwischen verschiedenen Mobilfunkbetreibern.

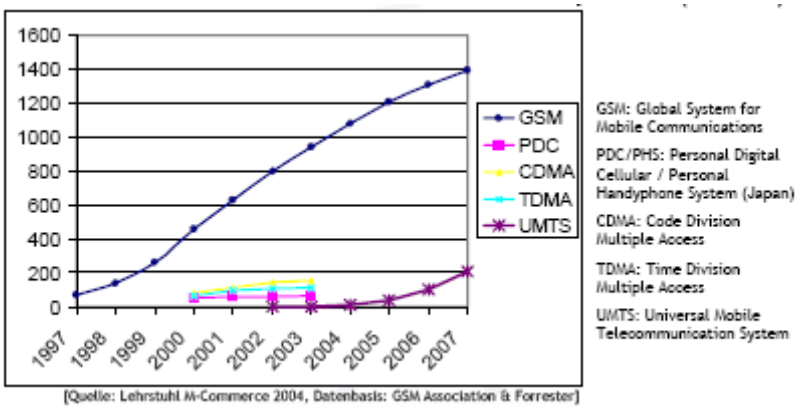

Abb. 23. Mobile Kommunikationsysteme

4.3.1.1 GSM-Dienste

Es bestehen drei Subunterteilungen von Diensten, die von GSM[91] bereitgestellt werden:
1. Trägerdienste dienen zur Übertragung von Daten über das GSM-Netz. Die maximale Datenübertragungsrate beträgt laut dem GSM-Standard 9,6 kbit/s. Der Standard hat keine Multimediaanwendungen vorhergesehen.

[91] vgl. Sauter, Martin : Grundkurs Mobile Kommunikationssysteme

2. Teledienste dienen zur Sprachübermittelung und unterstützen die mobile Kommunikation zwischen den Nutzern. Außerdem spielen sie eine zentrale Rolle im GSM-Standard.

Diese wären z.B.: Hochqualitative Telefongespräche, Kurz-Mitteilungen (SMS), Fax, und von allen Betreibern kostenlose europaweite Notfallnummer 112 (mit höchster Priorität).

3. Zusatzdienste sind abhängig vom Netzbetreiber. Dies können folgende Dienste sein:

- Identifikation des Anrufers (Rufnummerübermittlung)
- Unterdrückung der Identifikation (im Endgerät)
- Rufumleitungen
- Konferenzschaltungen mit bis zu 7 Teilnehmern
- Geschlossene Benutzergruppen

Die Integration von Sicherheitsdiensten war ein explizites Ziel bei der GSM-Entwicklung, wobei der Schutz der Luftschnittstelle im Mittelpunkt stand. Die Luftschnittstelle ist die Strecke, die per Funk überbrückt werden muss, bis die Daten in ein Festnetz eingespeist werden.

Die Sicherheitsdienste werden durch drei Systemkomponenten der GSM-Architektur realisiert. Diese sind die SIM Karte, das mobile Endgerät und das Network and Switching Subsystem.

4.3.1.2 GSM – Architektur

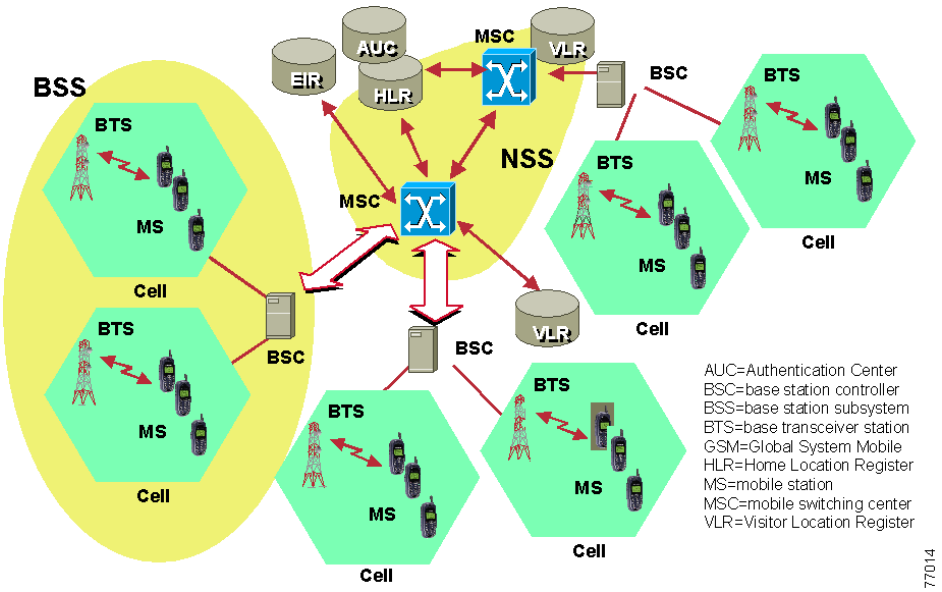

Abb. 24 GSM – Architektur[92]

4.3.1.2.1 Network und Switching Subsystem (NSS)

Das Network und Switching Subsystem (NSS), wie Abb. 24 zeigt, eine Menge von Verwaltungskomponenten der Netzbetreiber zusammen. Dazu gehört das Mobile Switching Center (MSC), das als Vermittlungsstelle für Aufbau, Abbau und Übergabe von Verbindungen zuständig ist. Außerdem realisiert es den Übergang ins Festnetz. Eine zweite Komponente ist die Home Location Register (HLR). Hier sind in der zentralen Datenbank alle Teilnehmerdaten wie Rufnummern, Schlüsseln, und aktuellen Standorte gespeichert. Ein zweites Register, das Besuchsortregister VLR (Visitor Location Register), ist jedem MSC zugeordnete Datenbank mit Teilnehmerdaten (HLR-Teilkopien) mit aktiven Teilnehmern im MSC-Einzugbereich, das heißt Teilnehmern, die sich temporär in dem geografischen Bereich einer Funkzelle aufhalten.

Zwei weitere wichtige Komponentevon NSS sind:

- Authentication Center (AC): Das Authentifizierungs-Zentrum (AC) übernimmt den Schutz der Teilnehmerdaten und der Datenübertragung und verwaltet die Schlüssel.
- Equipment Identity Register (EIR): Im Geräte-Identifikationsregister (EIR) sind die Daten für die Identifikationen aller Endgeräte eingetragen. Dazu führt das EIR bis zu drei Listen, nämlich die schwarze für gesperrte Endgeräte, die gestohlen sind oder

[92] http://www.cisco.com/univercd/illus/7/14/77014.gif

technische Mängel aufweisen, die graue, für fehlerhafte Geräte, und die weiße mit den Seriennummern aller zugelassenen Geräte.

4.3.1.2.2 Basisstationsubsystem (BSS)

Dieses System besteht aus funkspezifischen Komponenten. Diese sind mobile Endsysteme, MS (Mobile Station), die sich durch zellulare Systeme bewegen können. Beispiele für solche mobilen Endgeräte sind Autotelefone, portable Geräte und natürlich Mobiltelefone. In solchen mobilen Endgeräten befindet sich eine Sim Karte, die die Identifikations- und Authentifikationsdaten eines Mobilfunkteilnehmers enthält.

Die Funkübertragung erfolgt durch das Basisstationsubsystem (BSS), das das mobile System mit dem NSS verbindet. Das Basisstationssubsystem besteht aus zwei Teilen. Erstens aus der Sende- und Empfangseinheit einer Zelle, auch Base Transceiver Station (BTS) oder auch kurz Basisstation genannt. Zweitens aus einer Kontrolleinheit, der Base Station Controller (BSC), die angrenzende BTS verwaltet und überwacht. Dies wird beispielsweise für die Frequenzvergabe sowie Verbindungsübergabe zwischen den Zellen benutzt. Mehrere Basisstationen können über einen gemeinsamen Controller in einem RSS zusammengefasst sein. Eine BTS versorgt jeweils eine GSM-Zelle (~100m bis ~30km Radius). Die genauen Unterteilungen sind in Abb. 24 auf der vorigen Seite genau zu sehen.

4.3.1.3 Roaming

Roaming[93] beschreibt den Wechsel des Netzzuganges. Diese wären z.B.:

- Wechsel von GSM-Netzbetreibern
- Wechsel zwischen verschiednen Netzsystemen
  (UMTS, GSM, WLAN, CDMA, PDC)
- Wechsel zwischen den Zellen innerhalb eines GSM-Systems

Der Wechsel geschieht, indem die Verbindung unterbrochen und wiederaufgebaut wird. Roaming dient dazu, fremde GSM-Netze im Ausland zu nutzen, wie in Abb. 25 global dargestellt, aber auch national wird es genützt um einen besseren Empfang zu erhalten.

[93] vgl. Heinrich, Volker : Handy global

Abb. 25. Roaming[94]

Eine wichtige Rolle wird Roaming in Zukunft in heterogenen Netzwerken(GSM, WLAN, UMTS) und lokal unterschiedlichen Netzversorgung spielen. Zum Beispiel trägt sich das Endgerät automatisch in das bereitgestellte WLAN ein, sobald es in dem Bereich des Hotspots eingetreten ist (Flughafen, Konferenzen, Firmennetze).

Bewegt sich ein Nutzer vom Abdeckungsbereich einer Funkzelle in den einer anderen, muss eine möglichst „weiche“ Verbindungsübergabe erfolgen. Daher erfolgt die Verbindungsübergabe zwischen den Funkzellen im Bereich von 100ms, und es kommt nur zu einer kurzen Verbindungsunterbrechung. Der Grund für diese Unterbrechung ist, dass die Daten im VLR aktualisiert werden müssen.

Folgende Sicherheitsdienste sind zu beachten:

- Authentifizierung und Zugangskontrolle:

Die Authentifizierung des Nutzers gegenüber SIM erfolgt durch die Eingabe des PINS, und gegenüber dem GSM-Netz durch ein so genanntes Challenge-Response-Verfahren.

- Vertraulichkeit:

Die über Funk übertragene Daten & Sprache zwischen Mobile Station und Base Transciever Station werden verschlüsselt.

- Anonymität:

Nutzeridentifizierenden Daten werden über Funk nicht übertragen sondern stattdessen wird eine temporäre Kennung (Temporary Mobile Subscriber ID, TMSI) verwendet.

[94] http://www.dsltarife.net/images/mobilfunk/mobil-info-roaming.gif

4.3.1.3.1 Erweiterte GSM-Dienste

Die erweiterte GSM- Dienste sind Circuit Switched Data (CSD) und High Speed Circuit Switched Data (HSCSD).

CSD ist ein leitungsvermitteltes Übertragungsverfahren im GSM-Mobilfunknetz mit einer Datenrate von 9,6 kBits/s. Der Verbindungsaufbau einer leitungsvermittelten Datenübertragung unterscheidet sich nur unwesentlich von der Sprachübertragung. Als Adressierung dient eine Telefonnummer. Die Leitungsvermittelung erfolgt zwischen einer Mobile Station (MS), also einem GSM-Mobiltelefon bzw. einer Datenkarte, und dem G-MSC (Gateway – Mobile Services Switching Center), das die Verbindungen in andere Netze herstellt.

HSCSD [95] arbeitet auch wie das bisherige GSM-Dienst verbindungsorientiert. Eine höhere Übertragungsrate wird durch Bündelung mehrerer Kanäle erreicht (d.h. mehrere Zeitschlitze). Theoretisch erreicht man eine achtfache Übertragungsrate, wenn 8 Zeitschlitze verfügbar wären.

Da gleichzeitiges Senden/Empfangen nicht von der Mobile Station unterstützt werden muss, sind Zeitschlitze für Auf- und Abwärtsrichtung getrennt zu reservieren.
Meistens werden mehr Daten empfangen als gesendet, daher gibt es die Möglichkeit mehr Zeitschlitze für den Empfang zu reservieren. Dies wird als Asymmetrischer Datendienst bezeichnet. Auch wenn keine Übertragung stattfindet, sind die Zeitschlitze geblockt.

Abb. 26. Asymetrische Kanalaufteilung

HSCSD bietet eine asymmetrische Kanalaufteilung hinsichtlich der Up- und Downloadgeschwindigkeit an. Wie Abb. 26 zeigt ist im Moment die Bündelung von gleichzeitig 4 Kanälen möglich. Mit Hilfe der neuen Kodierungstechnik wurde die Übertragungsrate pro Kanal von 9.6 KBit/s auf 14.4 KBit/s gesteigert.

[95] vgl. Heinrich, Volker : Handy global

4.3.1.3.2 General Packet Radio Service (GPRS)

Ein Schritt in Richtung Mobilkommunikation der dritten Generation (UMTS) ist der paketvermittelnde Dienst GPRS[96], der theoretisch eine Datenrate bis zu 115 Kb/s erlaubt. In der Praxis muss man sich aber mit weit geringeren Datenraten von 14,4 Kb/s im Upstream und 40 Kb/s im Downstream zufrieden geben. Auch bei GPRS werden mehrere Kanäle (bis zu acht) für einen einzelnen oder mehrere Benutzer gemeinsam benutzt.

Die Kanäle werden bei GPRS dynamisch aufgeteilt, woraus sich eine flexible Ressourcennutzung ergibt, aber die Datenraten auch variieren können. Die über GPRS angebundenen Geräte besitzen eine IP Adresse. GPRS baut auf dem GSM Standard auf und Abb. 27 zeigt die Grobarchitektur eine GPRS Systems.

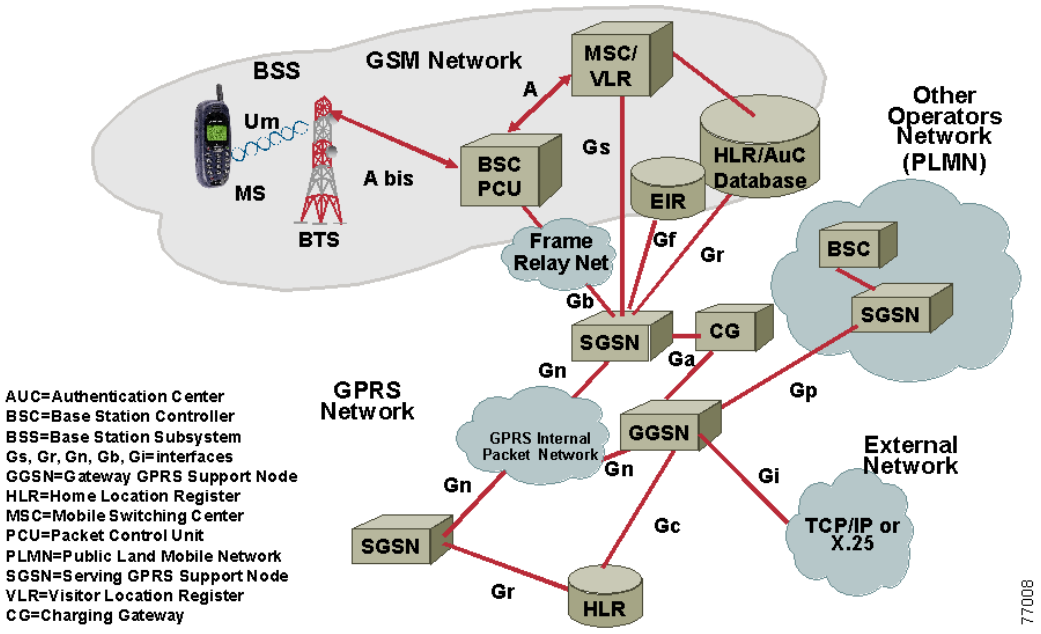

Abb. 26. GPRS - Architektur[97]

Der GGSN (Gateway GPRS Support Node) stellt die Verbindung zum Internet her und der SGSN (Service GPRS Support Node) vermittelt IP-Pakete über GSM an das Endgerät.

IP-Pakete werden dazu, wie üblich, vor dem Versenden in eine Folge von Datenframes aufgespaltet und beim Empfänger wieder zum kompletten Paket zusammengefügt. Im Gegensatz zu GSM werden unter GPRS die einzelnen Datenframes aber nicht bereits von der Basisstation ver- und entschlüsselt, sondern erst durch das SGSN.

[96] vgl. Heinrich, Volker : Handy global
[97] http://www.cisco.com/univercd/illus/7/08/77008.gif

GPRS ermöglicht es den mobilen Teilnehmern, immer online zu sein. Daher wäre eine Etablierung eines VPN zur sicheren Ende-zu-Ende-Kommunikation hier sinnvoll.

4.3.2 Universal Mobile Telecommunications System

Mit UMTS wird zurzeit das UMTS Mobilfunksystem der dritten Generation, basierend auf GSM, als weltweiter Standard etabliert. Mobilfunksysteme der dritten Generation (3G) sind wesentlich komplexer und bieten zusätzliche Operationen und komplexe Roaming-Szenarien. UMTS bietet in Pikozellen, die nicht größer als 50 Meter sind, Datenraten von bis zu 2Mb/s. Diese Datenrate nimmt aber mit der Größe der Zelle sehr schnell ab, sodass man bei Mikrozellen (Größe = einige Kilometer) nur noch eine Datenrate von bis zu 384Kb/s messen kann.

Die Kommunikation der 3G-Systeme basiert auf verschiedene Netzwerktypen und drahtlosen Netzen. Daher steht die Frage der UMTS-Sicherheit bei der Entwicklung des Standards groß im Mittelpunkt.

Die UMTS-Sicherheitsarchitektur übernimmt einige der Basis-Sicherheitsdienste von GSM und erweitert diese. Dazu gehören Vertraulichkeit der Teilnehmeridentität, die Authentifizierung des Teilnehmers gegenüber dem Netz, die verschlüsselte Kommunikation auf der Luftschnittstelle, die SIM Karte als persönliches Sicherheitsmodul sowie die Authentifikation des Teilnehmers gegenüber der SIM Karte.

Analog zur SIM Karte wird das USIM (UMTS Subscriber Identity Module) eingeführt. Die Aufgaben des Networks and Switching' Subsystem (NSS) werden unter UMTS auf die Heimatumgebung, die von dem Netzbetreiber betreut wird, und auf das Service Netzwerk (SN) aufgeteilt.

Das SN verwaltet die Basisstationen eines geografischen Bereichs, kontrolliert Verbindungen, leitet sie weiter und verwaltet das VLR (Visitor Location Register). Zur Heimatumgebung gehört das Authentifizierungs-Zentrum AC, das die Aufgaben der GSM-Komponente um zusätzliche Dienste ergänzt.

Unter UMTS erfolgt der Austausch der Authentifizierungs-Vektoren über IP-basierte Netze, wie GTP, dem Tunneling Protokoll für GPRS. IP-basierteNetze können durch

die Verwendung von IPSec und IPSec Tunnels zwischen Netzwerkkomponenten abgesichert werden.

4.4 Anwendungsbeispiele

Auch wenn die Bedeutung digitaler Signaturen der breiten Öffentlichkeit nicht bewusst ist, so dringen diese doch in zunehmendem Maße in immer mehr Lebensbereiche ein. Der Bogen reicht vom immer beliebter werdenden Internet-Shopping über problemlos abzuwickelnde Behördenwege bis hin zur sicheren E-Mail-Kommunikation[98]. Dem Einsatz dieser Techniken in unterschiedlichsten Anwendungsbereichen sind keine Grenzen gesetzt.

Das Signaturgesetz liefert dabei lediglich die Rahmenbedingungen für die Erstellung von elektronischen Signaturen.

Im nachfolgenden Kapitel sollen anhand einiger Beispiele bereits existierende oder sich in Entwicklung befindliche Systeme beschrieben werden.

4.4.1 e-Government

Der Begriff "E-Government" (electronic Government) steht heute als Synonym für eine moderne und effiziente Verwaltung.
Auf EU-Ebene wird E-Government [99] als "Einsatz der Informations- und Kommunikationstechnologien in öffentlichen Verwaltungen in Verbindung mit organisatorischen Änderungen und neuen Fähigkeiten" definiert, "um öffentliche Dienste und demokratische Prozesse zu verbessern und die Gestaltung und Durchführung staatlicher Politik zu erleichtern."

Mit Hilfe von neuen Medien und aktueller Technologie ist es den Behörden nun möglich, Dienstleistungen dem Großteil der Bevölkerung über traditionellem Weg hinaus zugänglich zu machen. An oberster Stelle steht das Internet, welches den Weg zu einem qualitativen Fortschritt in der Kommunikation zwischen Amt und Bürgern ebnete.

[98] siehe auch http://www.bmwa.gv.at/NR/rdonlyres/B3AEAF97-40F8-41F2-B1C3-04DA00C875FF/12408/EndberichtelektonischeSignatur.pdf
[99] vgl. http://www.digitales.oesterreich.gv.at/site/5230/default.aspx

Die meisten Informationen werden heutzutage im Web angeboten und auch die öffentliche Verwaltung geht schrittweise dazu über, alle Ihre Prozesse, d.h. die Transaktionen vom Antrag bis zur Erledigung eines Anbringens, online anzubieten. In Zukunft wird es auch nicht mehr notwendig sein, Formular herunterzuladen, sondern diese können in Form von Onlineformularen direkt am Server des Anbieters (z.B. Finanzonline) ausgefüllt, elektronisch signiert und abgesendet werden. Dies soll, wie beschrieben, dann auch über das Handy [100] signiert werden können. Auch in entgegengesetzter Richtung sollen Bescheide, Erledigungen der Verwaltung und sonstige Schriftstücke nicht mehr auf dem Postweg zugestellt werden, sondern auf Wunsch auch elektronisch erfolgen.

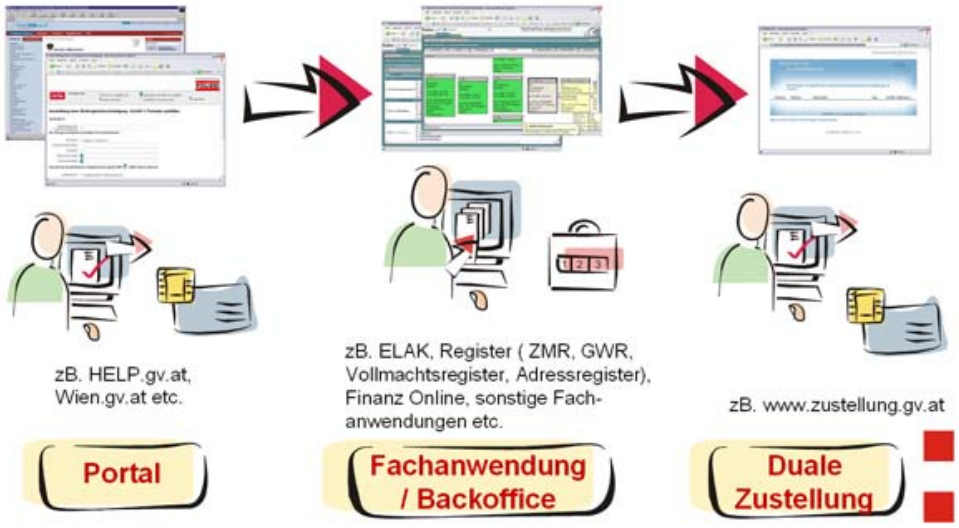

Abb. 28. Antrag bis zur Erledigung (E-Goverment)[101]

Internet-Portal: Informationen zu und Erledigung von Amtswegen (z.B. Help.gv.at, wien.gv.at) - (wie in Abb.28 ersichtlich).

Fachanwendung: elektronische Bearbeitung des Amtsverfahrens (z.B. elektronischer Akt, Zentrales Melderegister, Finanz Online)
Duale Zustellung: elektronische Zustellung der Amtspost (z.B. zustellung.gv.at)

Nicht nur für die BürgerInnen entstehen durch die elektronische Abwicklung von Amtswegen Veränderungen, auch innerhalb der Verwaltung ist eine Reorganisation der Prozesse und Kommunikationswegen erforderlich. Die Anforderungen an den Mitarbeitern der öffentlichen Verwaltung steigen, da diese eine hohe Flexibilität im

[100] siehe auch http://www.tecchannel.de/news/themen/business/407509/
[101] Digitales Österreich, 2008

Umgang mit den neuen Technologien vorweisen sollten. Laut „digitales Österreich“ wurde in Österreich im Rahmen der Neuausrichtung der IT-Strategie des Bundes, damals das IKT-Board, nun IKT-Bund genannt, eingerichtet.
Aufgabe des IKT-Bund ist es, übergreifende Aspekte im Bereich der Informations- und Kommunikationstechnologien zu regeln sowie die Abstimmung mit Projekten auf Landes-, Gemeinde- und Städteebene vorzunehmen.

Um unnötige Behördenweg und Zeit zu sparen, ist man bemüht für BürgerInnen und Unternehmen eine einzige Anlaufstelle zu schaffen. Diese wird auch als One Stop Prinzip bezeichnet und wieder werden diese zu den Dienstleistungen der öffentlichen Verwaltung über das jeweilige Behördenportal bzw. dem Amtshelfer HELP herangeführt.

Ein positiver Aspekt im Gegensatz zu früher ist, dass die Verwaltungskunden nicht mehr wissen, wie die Zuständigkeitsverteilung der Behörden organisiert ist, da die Beendigung durch ein elektronisches Zustellservice an den Kunden weitergeleitet wird.
Durch die neuen elektronischen Verfahren wird es in der Zukunft auch möglich sein eine Statusabfrage zu tätigen, d.h. BürgerInnen können jederzeit elektronisch den Bearbeitungsstand ihres Verfahrens prüfen.

4.4.1.1 Zielsetzungen für e-Government

Angestrebt wird, dass alle Bürgerinnen, Bürger und Unternehmen sämtliche Verfahren der öffentlichen Verwaltung problemlos und schnell ausführen können, ohne dafür spezielles technisches Wissen benötigen zu müssen.

Der erste Schritt, um sich diesem Ziel nähern zu können, ist, dass man die Kommunikationswege der öffentlichen Verwaltung mit den Bürgerinnen, Bürgern und Unternehmen an die neuen elektronischen Medien anpasst. Aber nicht nur nach außen hin, sondern auch verwaltungsintern müssen die Prozesse auf den neuesten Stand gebracht werden.

Einerseits die Einbindung aller Handelnden und andererseits die enge Zusammenarbeit zwischen Bund, Ländern und Gemeinden stellen österreichische E-Government-Strategien dar, sie liegen dem föderalen Prinzip zu Grunde, und nur dadurch können diese Ziele auch verwirklicht werden.

Kompetenzen und Zuständigkeiten werden auf unterschiedlichste Ebenen verteilt, doch um eine schnelle Bearbeitung und Erledigung von Verfahren zu erreichen, müssen die mitwirkenden Behörden noch besser zusammenarbeiten.

Damit es keinen Unterschied machen soll, auf welche Ebene die Kommunikation erfolgt, muss diese optimiert werden, das bedeutet, dass sowohl gemeinsame Standards verwendet werden müssen als auch, dass man die technischen Systeme aufeinander abstimmt, sodass eine Kommunikation problemlos erfolgen kann.

4.4.1.2 Herausforderungen

Damit man E-Government umsetzten kann, ist ein koordiniertes Vorgehen erforderlich. Zu berücksichtigen sind folgende Prinzipien: Datenschutz, Informations- und Netzwerksicherheit, Transparenz und vor allem die Zusammenarbeit.

Auf der einen Seite wird nun versucht, die BürgerInnen und Unternehmen an die elektronischen Behörden-Services heranzuführen, und auf der verwaltungsinternen Seite bemüht man sich die technischen Systeme aneinander anzupassen und einheitliche Standards zu schaffen, um einen Erfolg garantieren zu können.

Voraussetzungen für ein erfolgreiches E-Government: [102]

- effizientes Service, Transparenz und Kundenorientierung,
- Reorganisation von Arbeitsabläufen und Kommunikationswegen,
- Schaffung universaler Anlaufstellen (One Stop Shop-Prinzip),
- ein flexibles, interaktives, schnelles und sicheres Verwaltungssystem,
- gemeinsames Vorgehen und Kooperation der Verwaltungen von Bund, Ländern, Städten und Gemeinden,
- Interoperabilität und offene Schnittstellen.

[102] vgl. Digitales Österreich, http://www.digitales.oesterreich.gv.at/site/5237/default.aspx

4.4.1.3 e-Government per Handy

Online Formulare im Internet können heutzutage auch mit einem Mobiltelefon elektronisch signiert werden. Das Mobiltelefon muss sms empfangen können, dies stellt einen Standard dar.

Mobilkom Austria bietet allen Mobiltelefonbesitzern eine Handy Signatur, auch A1-Signatur [103] genannt, unabhängig davon von welchen Mobiltelefonanbieter sie betreut werden. Die A1 – Signatur [104] wird auch als Verwaltungssignatur bezeichnet und ist eine vollwertige elektronische Signatur via Mobiltelefon, sie ist der sicheren elektronischen Signatur im Rahmen der Bürgerkartenfunktion gleichgestellt.

Vorteile der Handy-Signatur [105]
Ein hervorragender Vorteil ist, dass man seine E-Goverment Anwendungen zeit- und ortsunabhängig ohne zusätzliche Geräte oder Programme von jeder Internet Station aus erledigen kann. Das heißt, man kann von jedem internetfähigen PC aus mittel Signatur Pin und sms Code, welcher nur einmalig gültig ist, seine Unterlagen elektronisch unterschreiben. Es ist auch zu erwähnen, dass es egal ist ob es sich hierbei um ein Vertrags- oder Wertkartenhandy handelt.

[103] http://www.jurpc.de/aufsatz/20040253.htm
[104] vgl. http://www.signatur.rtr.at/de/providers/services/mobilkom-a1signatur.html
[105] siehe auch http://www.tecchannel.de/news/themen/business/407509/

4.4.2 E - Wahlen

Die Teilnehmer verwenden bei der elektronischen Wahl eine lange Zufallszahl als Wahlkarte, die mit Hilfe der e-voting Applikation generiert wird. Die Wahlkarte wird vom e-voting Server versiegelt und blind signiert. Am PC des Wählers wird die Versiegelung entfernt, der Wähler verfügt über eine Wahlkarte, die doppelt signiert ist. Und das Wichtigste ist, dass dies zum Wähler nicht zurückverfolgt werden kann.

Einer der Hauptprobleme im e-voting System ist die mögliche Manipulation von abgegebenen Stimmen durch die Administration des e-voting-Systems.

Durch Verschlüsselung der abgegebenen Stimmen mit den öffentlichen Schlüsseln der Wahlkommission dezentral am PC des Wählers kann dies verhindert werden.
Zum Schutz vor einer übereilten Entscheidung (oder einem Fehler bei der Auswahl) des Wählers wird die getroffene Wahl nochmals angezeigt.

Der Wähler kann bis zu diesem Punkt seine Auswahl beliebig oft ändern, bis die Stimme schließlich endgültig abgegeben wird. Danach wird diese mit den öffentlichen Schlüsseln der Wahlkommission verschlüsselt und an den e-voting-Server gesendet, wie es in Abb. 29 dargestellt ist.

Nach Ende der Stimmabgabe entnehmen die Mitglieder der Wahlkommission ihre privaten Schlüssel dem sicheren Key Store. Die Stimmen können nur bei Vorliegen der Schlüssel aller Kommissionsmitglieder entschlüsselt und gezählt werden.

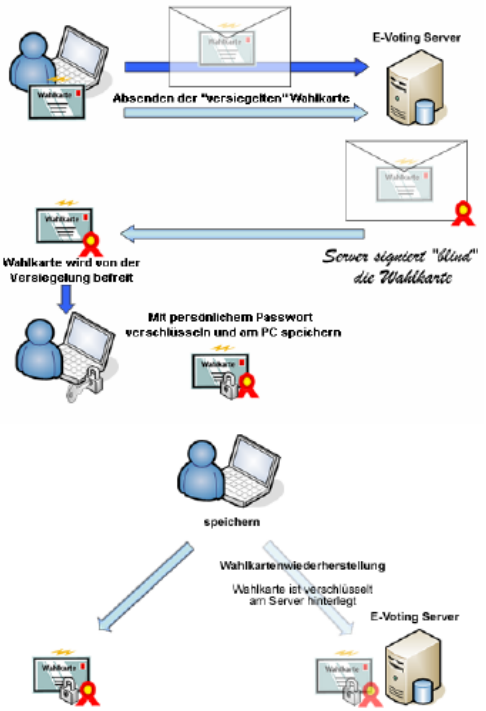

Abb. 29. Prozessverlauf – E Wahlen

Die elektronische Wahl, also die Wahl über das Internet, ist, eines der Ziele für die Zukunft. Wie diese Wahlen genau aussehen sollen, ist noch nicht geklärt. Viele sind aber jetzt schon der Meinung. dass e-Wahlen die herkömmlichen Wahlen einmal ganz verdrängen werden und damit auch quasi ein neues Zeitalter eingeleitet wird.

Folgender Beitrag[106] von Hr. Nicolas Wolz analysiert, wie sicher Wahlcomputer sind:
Wie sicher sind Wahlcomputer?
(Nicolas Wolz, Wie Sicher sind Wahlcomputer; FAZ.NET, Link, Datum)

Abb. 30. „Black Boxes“, mit denen man Schach spielen kann

03. Januar 2007 Die Bundestagswahl 2005 ist ungültig. Das meint zumindest Ulrich Wiesner, ein 38 Jahre alter Informatiker aus Frankfurt am Main. Gemeinsam mit seinem Vater, einem emeritierten Politikwissenschaftler, hat Wiesner beim Wahlprüfungsausschuss des Bundestags Einspruch gegen das Wahlergebnis eingelegt, weil in etwa 2000 Wahlbezirken knapp zwei Millionen von insgesamt 62 Millionen Wahlberechtigten in Deutschland mit Hilfe von Wahlcomputern abgestimmt hätten.

Das Zustandekommen des Wahlergebnisses, so die Wiesners in der Begründung zu ihrem Einspruch, sei beim Einsatz von Computern nicht öffentlich nachvollziehbar und damit gesetzeswidrig. Die Kontrollmöglichkeit der Öffentlichkeit ist ihrer Ansicht nach „die wesentliche Voraussetzung für demokratische Wahlen“. [107]

[106] Nicolas Wolz, 2007.
[107] siehe http://www.faz.net/s/Rub594835B672714A1DB1A121534F010EE1/Doc~ED7BB8B33DC2A4CCC8701C8B0672E58FF~ATpl~Ecommon~Scontent.html

4.4.3 e-Commerce

Beim E-Commerce[108] geht es um eine Abwicklung von Geschäften via Internet. Das virtuelle Geschäft - oft auch als Onlineshop bezeichnet - übernimmt dabei die Rolle des Verkäufers und Beraters. Via Internet wird ein Dialog zwischen Verkäufer und Käufer aufgebaut.

Folgende Anwendungsgebiete des E-Commerce sind für den Einsatz elektronischer Signaturen geeignet:
Business-to-Consumer (B2C): Geschäftsbeziehungen zwischen Unternehmen und Konsumenten. Die Konsumenten müssen sich nicht bei jedem Geschäft neu identifizieren, sondern können Bestellungen oder Reservierungen noch schneller und sicherer vornehmen (siehe Abb. 31).

Die Rechtssicherheit beim Online Shopping kann durch elektronische Signatur verbessert werden, zumal die Anbieter die Identität des Bestellers sofort online überprüfen können.

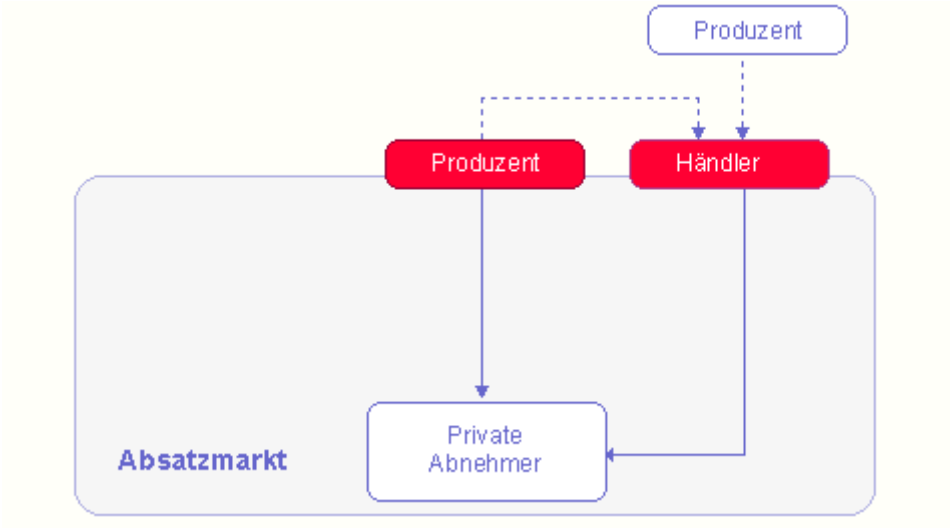

Abb. 31. Business-to-Consumer (B2C)[109]

Business-to-Business (B2B): Dies steht für die Kommunikationsbeziehungen zwischen Unternehmen. Im B2B ereich geht es um die bestmögliche Unterstützung der Absatzmittler durch das Medium Internet (siehe Abb.32).

[108] Quelle: http://www.echonet.at/de/wissen/e-commerce/25#nav
[109] E-Commerce Fachbegriffe Online Lexikon, B2C, http://www.at-mix.de/b2c.htm, Juni 2008

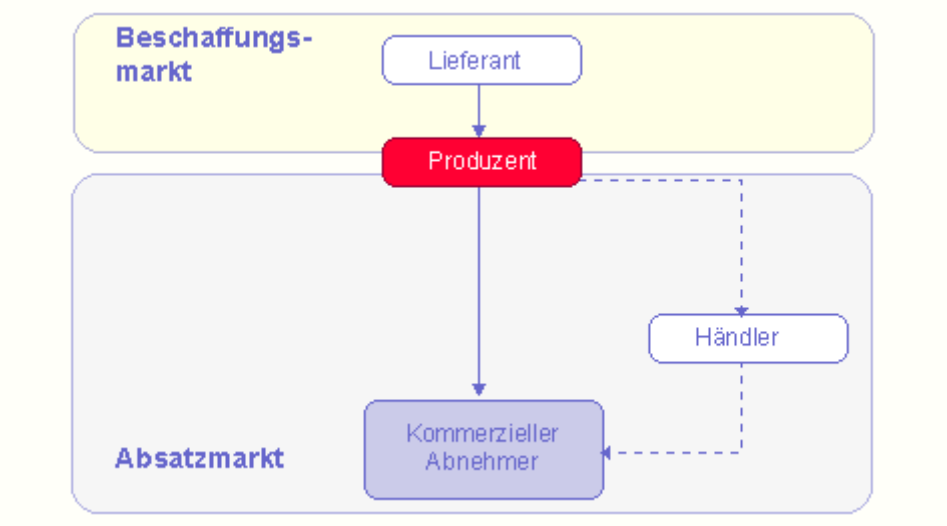

Abb. 32. Business-to-Business (B2B)[110]

Consumer-to-Consumer (C2C): C2C beschreibt den Handel zwischen Privatpersonen über multimediale Medien. Größtes und erfolgreichstes Beispiel dafür ist „EBay"-Plattform zur Ersteigerung von Waren aller Art.

[110] E-Commerce Online Lexikon, http://www.at-mix.de/images/glossar/business_to_business.gif, Juni 2008

4.4.4 e-Mail

4.4.4.1 Signieren von E-Mails

Aktuelle E-Mail-Programme bieten bereits integrierte Signaturfunktionen nach den vorgeschriebenen Standards. In den meisten Fällen wird der Standard S/MIME eingesetzt.

Das Zertifikat mit dem privaten Schlüssel muss in ihr E-Mail -Programm bzw. in die Signatursoftware importiert werden. Das Zertifikat wird im Normalfall mit dem öffentlichen Schlüssel den signierten E-Mails als Anhang beigefügt. Das heißt, um ein Signaturverfahren durchführen zu können, muss man im Besitz eines privaten Schlüssels samt Zertifikat sein.

In heutigen E-Mail-Programmen wie in Abb.33 ersichtlich kann über die Einstellungen die Signatur automatisch allen E-Mails beim Versenden angehängt werden. Man kann aber auch bei jeder E-Mail einzeln entscheiden, diese zu signieren. Unter Verwendung der Schlüsselpaare und Zertifikate können vertrauliche E-Mails auch verschlüsselt werden.

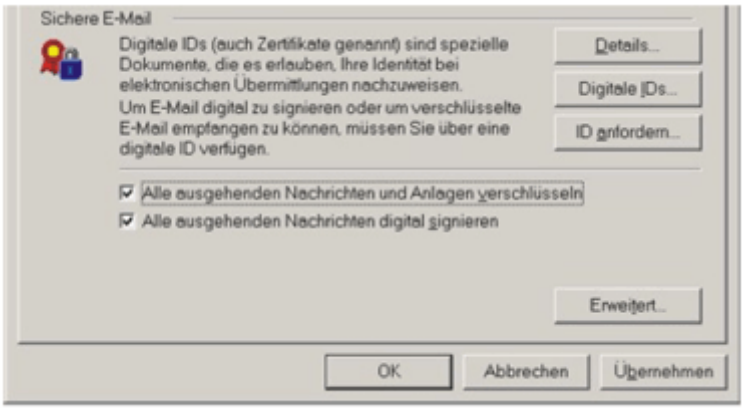

Abb. 33. E-mail-Signatur

4.4.4.2 Prüfung von signierten E-Mails

Die Signaturprüfung findet in zwei Teilen statt. Im ersten Schritt wird unter Verwendung des öffentlichen Schlüssels des Signators die kryptografische Prüfung der Signatur durchgeführt. Im zweiten Schritt wird überprüft, ob das Zertifikat des Signators von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde und ob es noch gültig ist.

Zur Prüfung der Signatur muss der Empfänger das Zertifikat mit dem öffentlichen Schlüssel des Signators besitzen. Dieses ist typisch dem signierten E-Mail angehängt. Dabei ist es sehr wichtig und vorteilhaft, wenn der Empfänger auch die Zertifikate der ausstellenden Zertifizierungsstelle besitzt und diese als vertrauenswürdig einstuft. Auf diese Art und Weise kann der gesamte Zertifikatsbaum wie in Abb.34 dargestellt - vom Zertifikat der Zertifizierungsstelle bis zum Zertifikat des Signators - geprüft werden.

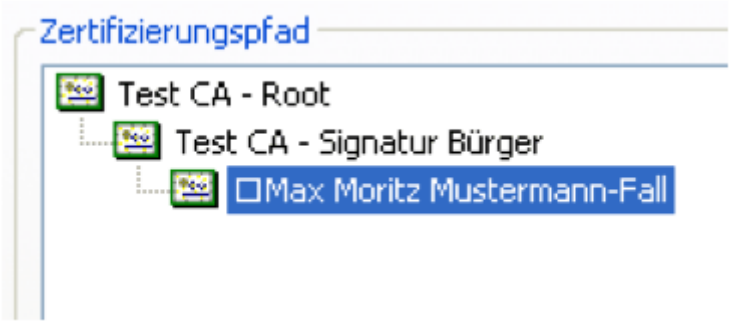

Abb. 34. Zertifizierungspfad im Windows

Wenn ein Wurzel-Zertifikat noch nicht als vertrauenswürdig eingestuft ist, so erscheint beim Empfang eines signierten E-Mails eine entsprechende Warnung. Beim Einstufen der Zertifikate sollte man nur jene Zertifikate als vertrauenswürdig einstufen, denen man auch wirklich vertrauen will.

In den meistverwendeten E-Mail-Programmen werden eingehende signierte E-Mails bereits automatisch überprüft.

Abb. 35. Automatische Zertifizierung

In der folgenden Abbildung (Abb. 36) sieht ein Beispiel für eine Nachricht im S/MIME Format. Wie man an diesem Beispiel erkennen kann, muss man sich gegenseitig signierte Mails zusenden, um die Schlüsseln auszutauschen. Weiters werden Mails in S/MIME Format von den gängigsten E-Mail-Programmen automatisch entschlüsselt.

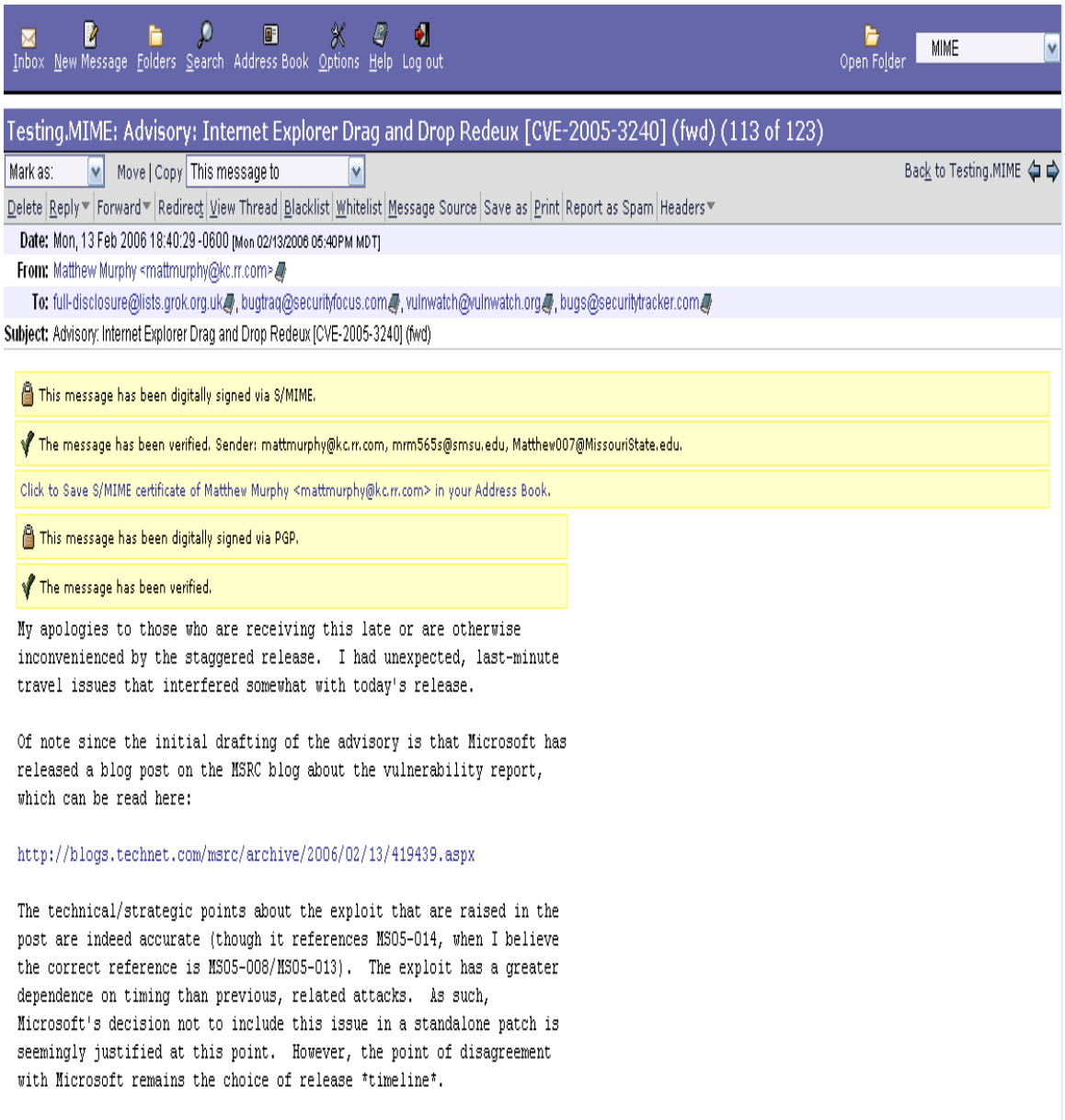

Abb. 36. Beispiel für S/MIME Zertifikat

Die nachfolgende Abbildung (Abb. 37) zeigt eine signierte Nachricht in PGP Format. Es ist eine empfangene signierte Nachricht, die man mit Hilfe der PGP-Plugins auf eine einfache Art und Weise entschlüsseln kann. Wie man hier sehen kann, funktioniert das Verschlüsseln einer Nachricht auf die gleiche Art und Weise.

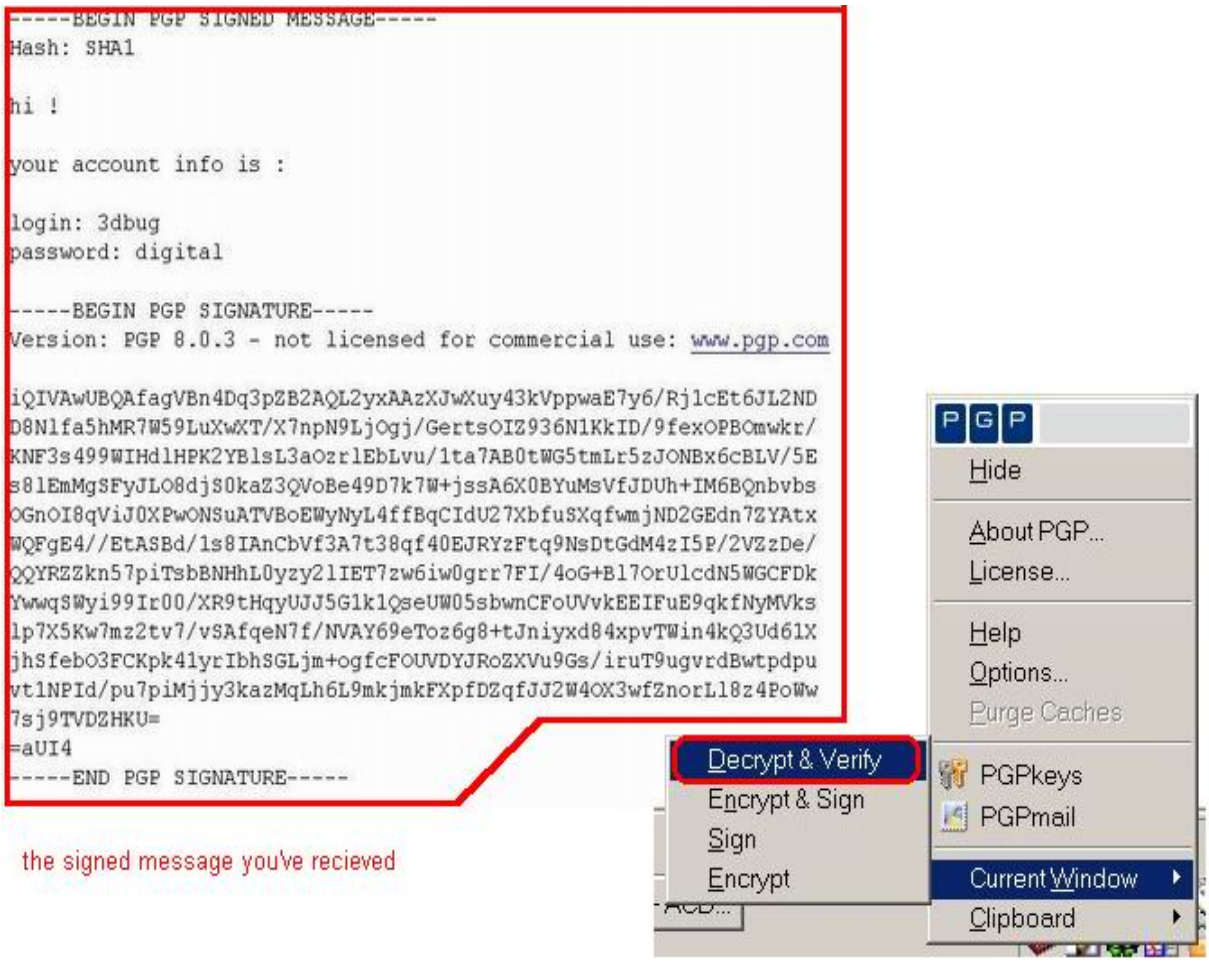

Abb. 37. Beispiel für PGP Signatur [111]

[111] vgl. http://www.emailprivacy.info/uploads/images/102/dig_sign_0041.jpg

4.4.5 e-Medical

Maßnahmen zur Erhöhung der Effizienz der Verwaltung in medizinischen Bereichen zu ergreifen, stellt für die Zukunft eine große Herausforderung dar. Auch hier können elektronische Signaturen vieles erleichtern oder überhaupt erst möglich machen.
So gibt es schon die e-card; vertrauliche, medizinische Daten werden in zunehmendem Ausmaß nun elektronisch gespeichert.

Die e-card[112] ist ein elektronischer Schlüssel zum Datensystem der Sozialversicherungen und besitzt zurzeit relativ wenige Funktionalitäten. Es gibt viele Pläne und Projekte, die Funktionen dieser Chipkarte auszubauen. Kaum ein Gesundheitsprojekt ist so umstritten wie die lebensbegleitende elektronische Gesundheitsakte (ELGA), die ab dem Jahr 2012 in Österreich eingeführt werden soll.

Darin sollen alle Gesundheitsdaten für Ärzte, Spitäler und andere Leistungsanbieter jederzeit per EDV zugänglich sein. Nicht nur Datenschützer, sondern auch die Österreichische Ärztekammer ist gegen das Projekt. Als Argumente werden der gläserne Patient und das Ende der Privatsphäre angeführt.

Mit der e-card Infrastruktur wurden die Meilensteine für viele zukunftsweisende Folgeprojekte gelegt. Die e-card ist für den Patienten nicht nur ein Krankenschein in Scheckkartenformat, sondern viel mehr. Sie dient als Lösung für das Gesundheitssystem und eröffnet den Besitzern der e-card durch die Bürgerkartenfunktion auch die Benützung der E-Govermnet Services.

Unbegrenzt gültig
Die e-card ist zeitlich unbegrenzt gültig und gilt für jeden Vertragsarzt. Das heißt, in Zukunft wird für den Arztbesuch nur die e-card benötigt.

Jederzeit Verfügbar
Die e-Card hat man immer bei sich und muss sich nicht im Falle einer Erkrankung, wie in der Vergangenheit einen Krankenschein besorgen.

Die e-card gilt in ganz Österreich bei allen Vertragsärzten und Vertragseinrichtungen, die bisher auch Krankenscheine akzeptiert haben. Aber nicht nur in Österreich, sondern auch innerhalb der EU-Mitgliedsstaaten ist sie gültig. Von EWR-Staaten und der Schweiz wird die europäische Krankenversicherungskarte anerkannt.

[112] siehe auch http://www.datenschutzzentrum.de/sommerakademie/2005/somak05_engel.pdf

Datenschutz

Persönliche Daten, die auf der e-card gespeichert sind, werden durch den Einsatz modernster Technologie geschützt. Unternehmen, Ärzte, Sozialversicherung und das Arbeitsmarktservice sehen die e-card als unbürokratisch, zeitsparend und kostengünstig in der Verwaltung.

Die e-card ist nicht nur eine Krankenversicherungskarte. Sie ist in Zukunft auch in anderen Zusammenhängen - z.B. für Datenabfragen im Internet, als persönlicher elektronischer Ausweis, als Bürgerkarte[113] - verwendbar.

Auf der e-card sind folgende Daten gespeichert:

- Vorname , Familienname und Akademischer Grad
- Sozialversicherungsnummer und Kartennummer

Die e-card enthält keine Gesundheitsdaten, sondern dient nur als Schlüsselkarte. Sie enthält nur wenige persönliche Angaben, und ermöglicht den Zugang zu den persönlichen Daten. Beim Arzt wird mit Hilfe eines Lesegerätes über gesicherte Datenleitungen der Krankenversicherungsträger und eine eventuelle Rezeptgebührenbefreiung abgefragt.

Die Funktionalitäten der e-card sind sehr erweiterbar. Das Problem, das dabei entsteht, ist folgendes: je mehr Funktionen die e-card erfüllen würde, desto schwerer wäre es nachzuvollziehen, wer wirklich Zugang zu den Daten hat. Die e-card könnte für folgende Aufgaben bzw. Funktionen erweitert werden:

- Die Verwendung als Bürgerkarte, diese ist auch schon möglich und individuell jedem Kartenbesitzer überlassen.
- Eine genaue Arztbesuchsprotokollierung und administrative Sonderlösung
- Auch die Speicherung der Notfalldaten wäre möglich
- Die e-card könnte man auch als Multifunktionskarte verwenden, wie z.B: als Bankomatkarte oder Quickfunktion

Als letzten Punkt möchte ich die E-Medikamentation erwähnen. Mit diesem System will man in Zukunft das klassische Rezept ersetzen. Dazu benötigt der Apotheker ein Lesegerät, mit Hilfe dessen er erkennen kann, welches Medikament vom Arzt

[113] siehe http://mediakomm.difu.de/documents/forschung/mobile---signatur.pdf

verschrieben wurde. Kritik besteht insofern, dass der Apotheker somit Einblick in die Medikation des Arztes und der gesamten Gesundheitszustandes des Patienten erhält.

Doch meiner Meinung sollte dieses Problem leicht zu lösen sein. Dazu bräuchte man nur einen speziellen Ordner auf der e-card anzulegen, welcher nur die aktuellen und nicht die ausgehändigten Medikamente dem Apotheker anzeigt.

Doch bei dieser großen Vielfalt von Ideen haben die meisten e-card Besitzer ohnehin keine Vorstellung mehr, was dies im Konkreten für die Sicherheit Ihrer Daten bedeutet. Auch für die administrativen Mitarbeiter ist es wichtig, die technischen Details zu kennen, um sich ein Bild über die Sicherheit der Daten zu verschaffen. Doch im Moment ist der genaue Prozessablauf noch offen.

4.5 Future Net

Ideen und Vision über die Weiterentwicklung des Internets in Richtung Future Net werden unter Bezeichnungen wie Next Generation Network (NGN), all-IP oder auch beyond 3G Networks (B3G) durchgeführt.

Im Grunde geht es darum EnablerTechnologien zu entwickeln, sodass heterogene Netze in einem integrierenden Netz zusammengeführt werden können, obwohl man in verschiedenen Forschungsbereichen unterschiedlichen Zielvorstellungen folgt.
Mit der „Future Net"-Architektur wird es möglich sein, heterogene Zugangs- und Kommunikationstechnologien gemeinsam zu betreiben und die einheitliche Benützung von unterschiedlichsten Content- und Diensteanbieter zu schaffen.

4.5.1 Next Generation Network – Entwicklung

Durch die Verschmelzung verschiedener Branchen, im Speziellen Telekom und Daten, entstehen neue Anforderungen wie die Notwendigkeit flexibler Anpassungen sowohl an die unterschiedlichen Netze als auch an die Bedürfnisse der User.

Im Zuge dessen werden künftig beispielsweise im Mobilfunk die Technologien GSM, UMTS und PDF/i-mode miteinander verschmelzen. Weiters ist auch ein Zusammenwachsen mit WLAN-Technologien, aber auch DAB (Digital Audio Broadcasting bzw. DVB Systemen angestrebt. Das daraus entstehende neue Netz ist unter dem Namen NGN (Next Generation Networks) bekannt.

Eine weitere Facette des NGN ist die Vereinheitlichung von IP Standards um beispielsweise Datendienste und Sprachtelefonie miteinander zu verbinden. Ziel dabei ist es sämtliche Dienste und Engeräte (PDAs, Telefone etc.) miteinander kompatibel zu machen.

4.5.2 Qualität

Hauptanforderungen der Verschmelzung ist es, dass diese sowohl unterbrechungsfrei, bequem als auch sicher sind. Weitere Anforderungen nach dem ABC (All best connected) Ansatz sind:

- Beste Bandbreite
- Geringste Verzögerungen
- Geringste Kosten
- Beste Verfügbarkeit
- Qualität
- Sicherheit

4.5.3 Realisierung

Zur Realisierung wird es notwendig sein, Endgeräte schnell softwarebasiert an die entsprechenden Netzgegebenheiten anzupassen. Die dazu notwendige Technologie SDR (Software Defined Radio) wurde bereits entwickelt und steht vor ihrem Einsatz. Die noch zu lösenden Probleme betreffen vorwiegend die Vereinheitlichung unterschiedlicher Sicherheitsstandards in den verschiedenen heterogenen Netzen.

4.5.4 Interworking, Handover, Roaming

Ähnlich wie beim Roaming (Nutzung fremder Netze mit gleichem Endgerät) soll auch bei NGN ein Handover-Szenario entworfen werden (siehe dazu www.etsi.org) um die Übergabe aus heterogenen Netzen zu ermöglichen.

Beim Roaming werden alle notwendigen Informationen, wie z.B. Aufenthaltsort des Users, automatisch bestimmt und verwaltet. Die automatische Weiterreichung wird in diesem Zusammenhang auch mit „seamless“ bezeichnet.

Um eine korrekte Abrechnung genutzter Dienste zu gewährleisten, müssen Sicherheitsaspekte wie Authentifizierung, Autorisierung und Accounting (AAA-Dienste) ermöglicht werden. Die Übergabe dieser Informationen stellt allerdings wieder ein Sicherheitsrisiko dar.

Zusammenfassend ist festzuhalten, dass das Netz der Zukunft durchgehend IP- basiert sein wird, selbstorganisierende Funknetze und adaptive softwarebasiert (re)konfigurierbare Luftschnittstellen bereitstellen und zur Erhöhung der Leistungsfähigkeit über optische Netzkomponenten, intelligente Antennen und Sensoren verfügen wird.

Auch die Endgeräte, die die Nutzung des Netzes der Zukunft ermöglichen sollen, müssen sehr viel flexibler und leistungsfähiger werden.
Mit neuen multi-modalen Schnittstellen, neuen Werkstoffen für die Displays und mit flexibel anpassbaren Software- und Hardwarearchitekturen werden zukünftige Endgeräte eine Vielzahl von Funktionen in sich vereinen.

Auch wenn für das technologische Zusammenwachsen von Netzen bereits Lösungsvorschläge erarbeitet wurden, wird in der Praxis nicht jede technisch machbare Netz-Kopplung sinnvoll einsetzbar sein. Hier spielen weitere Faktoren wie Kosten, Sicherheit und Qualität von Diensten eine Rolle.

Um den Nutzern die geforderten und ausgehandelten bzw. auch bezahlten Sicherheits- und sonstigen Qualitätsattribute durchgehend garantieren zu können, sind dringend noch weitere Forschungs- und Entwicklungsarbeiten notwendig.

5 Zusammenfassung

Im Rahmen dieser Diplomarbeit wurden die rechtlichen und technischen Aspekte der elektronischen Signatur transparent aufgearbeitet. Im Speziellen bin ich auf die mobilen elektronischen Signaturen eingegangen. In diesem Zusammenhang wurden die Grundlagen der Telekommunikation und verschiedene Dienste im Bereich des Mobilfunks erläutert.

Ziel dieser Arbeit war es, auf die Bedeutung elektronischer Signaturen und die Anforderungen, die an sie gestellt werden, einzugehen. Nach der Darstellung grundlegender Richtlinien wie der Signaturrechtlinie, der Unterschriften in Verbindung mit Zertifikaten und der Biometrie wurde auf technische Grundlagen elektronischer Signaturen ausführlich eingegangen, hierbei insbesondere auf symmetrische wie asymmetrische Verfahren und Verfahren zur Erzeugung elektronischer Signaturen.

Weitere Zielsetzung der vorliegenden Diplomarbeit war es, mobile elektronische Signaturen am Beispiel der SIM-Karte und verschiedener Systeme der Mobilkommunikation näher zu beleuchten und hierfür Anwendungsbeispiele zu geben.

Die Sim-Card bildet die Brücke zwischen elektronischen Signaturen und der mobilen Technologie. Die technischen Gegebenheiten ermöglichen es heutzutage theoretische Ideen zu implementieren, wie zum Beispiel das Mobil-Sign (mSign). In diesem Zusammenhang sind bereits viele Anwendungen im e-Government Bereich möglich, indem Formulare schon per Handy unterschrieben werden können.

Die vorliegende Diplomarbeit beleuchtet die zahlreichen Aktivitäten und Erweiterungen in den Bereichen e-Wahlen, e-Commerce und e-medical. Hierbei bekommt der Leser auch einen Überblick darüber, wie flächendeckend heutzutage mobile Signaturen bereits eingesetzt werden.

Im letzten Teil meiner Beschäftigung mit elektronischen Signaturen widme ich mich dem Future Net, indem ich dem Interessierten Einblicke in die Next-Generation-Network-Entwicklung, die Qualität sowie in die Bereiche Internetworking, Handover und Roaming gewähre. Die noch zu lösenden Probleme betreffen vorwiegend die

Vereinheitlichung unterschiedlicher Sicherheitsstandards in den verschiedenen heterogenen Netzen. Auch andere Aspekte, wie die Gewährleistung von korrekten Abrechnungen genutzter Dienste, spielen hier eine große Rolle. Ziel dabei ist es sämtliche Dienste und Endgeräte (PDAs, Telefone etc.) miteinander kompatibel zu machen.

Auch trotz der unbestrittenen Nutzenpotentiale und Kosteneinsparungen, welche Signaturtechnologien mit sich bringen, werden elektronische Signaturen von Unternehmen in der Praxis nach wie vor kaum eingesetzt.

In der Zukunft liegt das Hauptaugenmerk auf mobiler Kommunikation und es wird sich zeigen, dass durch die starke Weiterentwicklung der mobilen Endgeräte und der Sicherheit, die durch diese in Verbindung mit den SIM Karten gegeben ist, die mobile elektronische Signatur eine große Rolle spielen wird.

Wie auch immer die Verfahren aussehen werden, Signaturen werden auch in Zukunft ein wichtiger Teil unseres Lebens sein. Ob in Form von endlosen Zahlenreihen, der guten alten Unterschrift per Hand, eines biometrischen Merkmals oder einer sms (mobiler Signatur). Die Formen und Verfahren verändern sich, doch die Bedeutung bleibt.

Literaturverzeichnis

Ahmadi, Sanaz : 26 Jahre RSA-Kryptosystem / Sanaz Ahmadi, 2005. - 59 Bl.

Beutelspacher, Albrecht : Kryptografie in Theorie und Praxis : mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk / Albrecht Beutelspacher ; Heike B. Neumann ; Thomas Schwarzpaul. - 1. Aufl. . -Wiesbaden : Vieweg, 2005. – XIV

Beutelspacher, Albrecht : Moderne Verfahren der Kryptographie : von RSA zu Zero-Knowledge / Albrecht Beutelspacher ; Jörg Schwenk ; Klaus-Dieter Wolfenstetter. - 6., verb. Aufl. . - Wiesbaden : Vieweg, 2006. - X, 138 S. . - (Studium).

Beutelspacher, Albrecht : Kryptologie : eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen ; ohne alle Geheimniskrämerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums / Albrecht Beutelspacher. - 7., verb. Aufl. . - Braunschweig : Vieweg, 2005. - XII, 156 S. .

Eckert, Claudia : IT-Sicherheit : Konzepte - Verfahren - Protokolle / von Claudia Eckert. - 4., überarb. Aufl. . - München ; Wien : Oldenbourg, 2006. - XIV, 918 S. .

Eren, Evren : Mobile Security : Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit / Evren Eren ; Kai-Oliver Detken. - München ; Wien : Hanser, 2006. - XII, 660 S. .

Mobile digitale Kommunikation : Standards, Netze und Applikationen / [Funkwerk]. Helge Grote .... - [Landsberg] : Verl. Moderne Industrie, 2004. - 93 S. . - (Die Bibliothek der Technik ; 268).

Heinrich, Volker : Handy global - mit dem Handy im Ausland : [Netzstandards, Roaming, Kosten sparen, SMS, MMS, E-Mail, Fotografieren, WAP, Internet, Reiseinfos mobil] / Volker Heinrich. - 1. Aufl. . - Bielefeld : Reise-Know-How-Verl. Rump, 2006. - 160 S. . - (Reise-Know-how : Praxis).

Hühnlein, Detlef : Grundlagen der elektronischen Signatur : Recht - Technik - Anwendung / Bundeamt für Sicherheit in der Informationstechnik. [Autoren: Detlef Hühnlein und Ulrike Korte]. - Ingelheim : SecuMedia-Verl., 2006. - XII, 161 S.

Lockhart, Andrew : Network security hacks : [100 industrial-strength tips & tools] / Andrew Lockhart. - 1. ed. . - Bejing [u.a.] : O'Reilly, 2004. - XV, 298 S. .

Beweiskräftige elektronische Archivierung : bieten elektronische Signaturen Rechtssicherheit? Ergebnisse des Forschungsprojekts "ArchiSig - Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente" / hrsg. von Alexander Roßnagel ; Paul Schmücker. Unter Mitarb. von Norbert Anderl .... - Heidelberg [u.a.] : Economia, 2006. - XV, 267 S. . - (Gesundheitswesen in der Praxis).

Sauter, Martin : Grundkurs Mobile Kommunikationssysteme : von UMTS, GSM und GPRS zu Wireless LAN und Bluetooth Piconetzen ; [GSM, GPRS und EDGE, UMTS und HSDPA, WLAN, Bluetooth ; mit Online-Service zum Buch] / Martin Sauter. - 2. Aufl. . - Wiesbaden : Vieweg, 2006. - XIII, 368 S. .

Schnabel, Patrick : Systeme der Mobilkommunikation : [GSM GPRS, UMTS, Bluetooth, WLAN 802.11, WAP, DECT ...] / Patrick Schnabel. - Duderstadt : EPV Elektronik-Praktiker-Verl.-Ges., 2005. - 64 S. . - (IT-Praxis-Reihe für Aus- und Weiterbildung).

Schneier, Bruce : Angewandte Kryptographie : Protokolle, Algorithmen und Sourcecode in C ; [der Klassiker] / Bruce Schneier. [Übers.: Katja Karsunke und Thomas Merz]. - München [u.a.] : Pearson Studium, 2006. - XXII, 844 S. . - (Informatik : Kryptographie).

Steininger, Katharina : Elektronische Signaturen : ein Leitfaden zum erfolgreichen Einsatz von ektronischen Signaturen / Katharina Steininger. - Linz : Trauner, 2006. - 159 S. . - (Schriften der Johannes-Kepler-Universität Linz : Reihe B, Wirtschafts- und Sozialwissenschaften ; 100).

IT-Sicherheit geht alle an! : [Tagungsband zum 9. Deutschen IT-Sicherheitskongress] / Bundesamt für Sicherheit in der Informationstechnik. - Gau-Algesheim : SecuMedia-Verl., 2005. - 361 S.

http://download.microsoft.com/download/a/b/c/abc6dd0c-2f81-4678-8ca8-6883ff42fb45/Markus_Tak.pdf

http://www.jurpc.de/aufsatz/20040253.htm

http://www.ecin.de/sicherheit/bedeutung-signatur/index-2.html

http://www.computerwelt.at/detailArticle.asp?a=99728&n=4

http://www.bundesnetzagentur.de/enid/pi.html

http://bundesrecht.juris.de/sigv_2001/index.html

http://digitale-signatur.edulab.de/

http://www.bsi.bund.de/esig/index.htm

http://europa.eu.int/comm/enterprise/ict/policy/b2b-con2003/reply-de-bitkom.pdf

http://www.datenschutzzentrum.de/sommerakademie/2005/somak05_engel.pdf

http://mentana.de/cms/index.php

http://mediakomm.difu.de/documents/forschung/mobile---signatur.pdf

http://www.buergerkarte.at/download/Handbuch_Unternehmer.pdf

http://www.bmwa.gv.at/NR/rdonlyres/B3AEAF97-40F8-41F2-B1C3-04DA00C875FF/12408/EndberichtelektonischeSignatur.pdf

http://www.tecchannel.de/news/themen/business/407509/

http://allpr.de/16210/Finnland-setzt-auf-mobile-Signatur-bei-eGovernment-Diensten-Giesecke-Devrient-liefert-die-SIM-Karten-mit-Sicherheitszertifikat.html

Computers & Security 25 (2006) S. 45 – 51

Wirtschaftsinformatik (2005) 1, S. 55 – 62

IT – Fokus ¾ 2005, S. 40 – Drahtlos im Geschäft

Monitor , April 2006, S. 18 – Mobile Business Solutions 2006

Business & IT 5 / 2006 S. 102 – Nie ohne Umschlag

Weiterführende Literatur:

Brands, Gilbert : IT-Sicherheitsmanagement : Protokolle, Netzwerksicherheit, Prozessorganisation / Gilbert Brands. - Berlin [u.a.] : Springer, 2005. - XI, 728 S. . -(X.systems.press).

Campo, Markus a : Sicherheit total / Markus a Campo. - 1. Aufl. . - Bonn : Verl. Moderne Industrie, 2003. - 764 S. . - (Das bhv Taschenbuch).

Coulouris, George : Verteilte Systeme : Konzepte und Design / George Coulouris ; Jean Dollimore ; Tim Kindberg. - 3., überarb. Aufl. . - München : Addison-Wesley, 2002. -869 S. . - (Informatik : Verteilte Systeme) (Pearson Studium).

Gläßer, Lothar : IT-Lösungen im E-Business : die technischen Grundlagen: einfach, praxisnah, zukunftsorientiert / von Lothar Gläßer. - Erlangen : Publicis Corporate Publ., 2003. - 218 S. .

Janowicz, Krzysztof : Sicherheit im Internet : [Gefahren einschätzen, Risiken minimieren: fundiertes Hintergrundwissen rund ums Internet ; effektiver Schutz für den PC: Wissenswertes über Schädlinge und Angriffsszenarien ; mit zahlreichen Sicherheitstools auf CD-ROM] / Krzysztof Janowicz. - 2. Aufl. . - Köln [u.a.] : O'Reilly, 2006. - XIV, 325 S. . - (O'Reillys basics).

Knoedel, Walter : Sätze über Primzahlen : Teil 1 u. 2. / Walter Knödel. - Wien : Springer, 1953. - S. 63-75, S. 138-143

Knuth, Michael : Web Services : Einführung und Übersicht / Michael Knuth. - Frankfurt : Software-und-Support-Verl., 2002. - 313 S. . - (Java-Magazin)

Krispler, Heinrich : IT-Sicherheit in multinationalen militärischen Netzwerken anhand des Beispiels Combined Endeavor 2005 / Krispler Heinrich, 2005. - V, 117 S.

Lepschies, Gunter : E-commerce und Hackerschutz : Leitfaden für die Sicherheit elektronischer Zahlungssysteme / Gunter Lepschies. - 2., überarb. Aufl. . - Braunschweig [u.a.] : Vieweg, 2000. - VI, 242 S. . - (DuD-Fachbeiträge).

Martius, Kai : Sicherheitsmanagement in TCP-IP-Netzen : aktuelle Protokolle, praktischer Einsatz, neue Entwicklungen / Kai Martius. - Braunschweig [u.a.] : Vieweg, 2000. - X, 227 S. . - (DuD-Fachbeiträge).

Sicherheitskonzepte für das Internet : 5. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung / Günter Müller ... (Hrsg.). - Berlin [u.a.] : Springer, 2001. - X, 211 S. . - (Xpert.press).

Näf, Michael : Risiko Internet? : Sicherheitsaspekte bei der Internet-Benutzung / Michael Näf ; Patrick Streule ; Werner Hartmann. - Zürich : Orell Füssli, 2000. - 158 S. .

Poguntke, Werner : Basiswissen IT-Sicherheit : das Wichtigste für den Schutz von Systemen und Daten / Werner Poguntke. - Herdecke [u.a.] : W3L-Verl., 2007. - XII, 363 S. . - (IT lernen).

Tanenbaum, Andrew S. : Verteilte Systeme : Grundlagen und Paradigmen / Andrew S. Tanenbaum ; Maarten van Steen. [Übers.: Judith Muhr]. - München [u.a.] : Pearson Studium, 2003. - 878 S. . - (Informatik : Verteilte Systeme).

Tanenbaum, Andrew S.: Computernetzwerke / Andrew S. Tanenbaum. [Übers.: Angelika Shafir]. - 3. Aufl. . - München [i.e. Haar] [u.a.] : Prentice Hall, 1997. - 847 S. .

http://www.documanager.de/magazin/artikel_913_elektronische_signatur_cebit_2006.html

http://www.secunet.com/

http://www.s-trust.de/

http://www.pressetext.at/pte.mc?pte=060206023

http://www.cio.gv.at/faq/onlineServices/#top

http://www.ecin.de/recht/elektronische-rechnung/

http://europa.eu.int/comm/enterprise/ict/policy/b2b-con2003/reply-de-bitkom.pdf

http://www.artmob.at/ans/content.cfm?id=878&sessid=188826

http://www.fir.rwth-aachen.de/download/udz/udz3_2004_257.pdf

http://www.mobued.de/projekt/projektbeschreibung/endgeraete.html

http://truposign.sit.fraunhofer.de/TPS_SIT_Gesamtvorhaben_Kickoff_020131org.pdf

http://www.wiiw.de/publikationen/DieKrisedesSignaturmarktesLoes1143.pdf

http://www.monitortv.at/monitortv/website/mobilesignatur/mobilesignatur.asp

http://www.inside-handy.de/news/5544.html

http://business.telekom.at/telekom/news/bizmail/it_strategien/biz79_itstrat.php

http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/Signaturworkshop_2003.pdf

http://www.net-im-web.de/pdf/2004_07s28.pdf

Anhang

Signaturgesetz[114]

1. Abschnitt

Gegenstand und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

§ 1. (1) Dieses Bundesgesetz regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten.

(2) Dieses Bundesgesetz ist auch anzuwenden in geschlossenen Systemen, sofern deren Teilnehmer dies vereinbart haben, sowie im offenen elektronischen Verkehr mit Gerichten und anderen Behörden, sofern durch Gesetz nicht anderes bestimmt ist.

(3) Dieses Bundesgesetz ist auf Zertifizierungsdiensteanbieter (ZDA) anzuwenden, die qualifizierte Zertifikate ausstellen oder qualifizierte Zeitstempeldienste bereitstellen. § 6 Abs. 1, § 22 und § 24 gelten auch für die übrigen ZDA.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeuten

1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen;

2. Signator: eine Person oder eine sonstige rechtsfähige Einrichtung, der Signaturerstellungsdaten und Signaturprüfdaten zugeordnet sind und die im eigenen oder fremden Namen eine elektronische Signatur erstellt;

3. fortgeschrittene elektronische Signatur: eine elektronische Signatur, die

a) ausschließlich dem Signator zugeordnet ist,

b) die Identifizierung des Signators ermöglicht,

c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann, sowie

d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann;

3a. qualifizierte elektronische Signatur: eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wird;

4. Signaturerstellungsdaten: einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden;

5. sichere Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen dieses Bundesgesetzes sowie der auf seiner Grundlage erlassenen Verordnungen entspricht;

6. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;

7. Signaturprüfeinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturprüfdaten verwendet wird;

8. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird;

[114] Quelle: http://www.internet4jurists.at/gesetze/bg_signatur01.htm

9. qualifiziertes Zertifikat: ein Zertifikat einer natürlichen Person, das die Angaben des § 5 enthält und von einem den Anforderungen des § 7 entsprechenden ZDA ausgestellt wird;
10. ZDA: eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt;
11. Signatur- und Zertifizierungsdienste: die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs- und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen;
12. qualifizierter Zeitstempel: eine elektronische Bescheinigung, dass bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage erlassenen Verordnungen entspricht;
13. Signaturprodukt: Hard- oder Software bzw. deren spezifische Komponenten, die für die Erstellung und Überprüfung elektronischer Signaturen oder von einem ZDA für die Bereitstellung von Signatur- oder Zertifizierungsdiensten verwendet werden;
14. Kompromittierung: die Beeinträchtigung von Sicherheitsmaßnahmen oder Sicherheitstechnik, sodaß das vom ZDA zugrundegelegte Sicherheitsniveau nicht eingehalten ist;
15. Signaturrichtlinie: Richtlinie des Europäischen Parlamentes und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L Nr. 13 vom 19. Jänner 2000, S 12.

2. Abschnitt

Rechtserheblichkeit elektronischer Signaturen

Allgemeine Rechtswirkungen

§ 3. (1) Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.
(2) Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten ZDA ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18 erstellt wurde.

Besondere Rechtswirkungen

§ 4. (1) Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinne des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.
(2) Eine qualifizierte elektronische Signatur entfaltet nicht die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB bei
1. Rechtsgeschäften des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind,
2. anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind,

3. Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, und
4. einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird.
(2) Eine sichere elektronische Signatur entfaltet in folgenden Fällen nicht die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB:
1. Bei Rechtsgeschäften des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind, es sei denn, die über das Rechtsgeschäft errichtete Urkunde enthält die Erklärung eines Rechtsanwalts oder eines Notars, dass er den Signator über die Rechtsfolgen seiner Signatur aufgeklärt hat; letztwillige Anordnungen können in elektronischer Form jedoch nicht wirksam errichtet werden.
2. Bei anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind, soweit die öffentliche Beglaubigung, die gerichtliche oder notarielle Beurkundung oder der Notariatsakt in elektronischer Form nicht wirksam zustande kommt.
3. Bei Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, soweit die öffentliche Beglaubigung, die gerichtliche oder notarielle Beurkundung oder der Notariatsakt in elektronischer Form nicht wirksam zustande kommt.
4. Bei einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird, es sei denn, diese enthält die Erklärung eines Rechtsanwalts oder eines Notars, dass er den Bürgen über die Rechtsfolgen seiner Verpflichtungserklärung aufgeklärt hat.
(3) Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, anzuwenden.
(4) Die Rechtswirkungen der Abs. 1 und 3 treten nicht ein, wenn nachgewiesen wird, daß die Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.
Qualifizierte Zertifikate
§ 5. (1) Ein qualifiziertes Zertifikat hat zumindest folgende Angaben zu enthalten:
1. den Hinweis darauf, daß es sich um ein qualifiziertes Zertifikat handelt,
2. den unverwechselbaren Namen des ZDA und den Staat seiner Niederlassung,
3. den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muß,
4. gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft des Signators,
5. die dem Signator zugeordneten Signaturprüfdaten,
6. Beginn und Ende der Gültigkeit des Zertifikats,

7. die eindeutige Kennung des Zertifikats,
8. gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
9. gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist.

(2) Auf Verlangen des Zertifikatswerbers können weitere rechtlich erhebliche Angaben in das qualifizierte Zertifikat aufgenommen werden.

(3) Ein qualifiziertes Zertifikat muss mit einer fortgeschrittenen elektronischen Signatur des ZDA versehen sein.

3. Abschnitt

ZDA

Tätigkeit der ZDA

§ 6. (1) Die Aufnahme und die Ausübung der Tätigkeit eines ZDA bedürfen keiner gesonderten Genehmigung.

(2) Ein ZDA hat die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle (§ 13) anzuzeigen. Er hat dieser spätestens mit Aufnahme der Tätigkeit oder bei Änderung seiner Dienste ein Sicherheitskonzept sowie ein Zertifizierungskonzept der von ihm angebotenen Signatur- und Zertifizierungsdienste samt den verwendeten technischen Komponenten und Verfahren vorzulegen.

(3) Das Sicherheitskonzept hat die Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen darzulegen.

(4) Ein ZDA hat die im Sicherheits- und im Zertifizierungskonzept dargelegten Angaben sowohl bei der Aufnahme als auch während der Ausübung seiner Tätigkeit zu erfüllen.

(5) Ein ZDA hat alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich der Aufsichtsstelle anzuzeigen.

(6) (entfällt BGBl 8/2008)

(7) Ein Zertifikat für ZDA darf von diesen nur für die Erbringung von Zertifizierungsdiensten verwendet werden.

Anforderungen an ZDA

§ 7. (1) Ein ZDA hat

1. die erforderliche Zuverlässigkeit für die von ihm bereitgestellten Signatur- oder Zertifizierungsdienste aufzuweisen,
2. den Betrieb eines schnellen und sicheren Verzeichnisdienstes sowie eines unverzüglichen und sicheren Widerrufsdienstes sicherzustellen und im Sicherheitskonzept darzulegen, in welcher Form dies erfolgt,
3. in qualifizierten Zertifikaten sowie für Verzeichnis- und Widerrufsdienste qualitätsgesicherte Zeitangaben zu verwenden und jedenfalls sicherzustellen, daß der Zeitpunkt der Ausstellung und des Widerrufs eines qualifizierten Zertifikats bestimmt werden kann,
4. die Identität und gegebenenfalls besondere rechtlich erhebliche Eigenschaften der Person, für die ein qualifiziertes Zertifikat ausgestellt wird, zuverlässig zu überprüfen,
5. zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der

Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen und geeignete Verwaltungs- und Managementverfahren, die anerkannten Normen entsprechen, einzuhalten,

6. über ausreichende Finanzmittel zu verfügen, um den Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen zu entsprechen, sowie Vorsorge für die Befriedigung von Schadenersatzansprüchen, etwa durch Eingehen einer Haftpflichtversicherung, zu treffen,

7. alle maßgeblichen Umstände über ein qualifiziertes Zertifikat während eines für den Verwendungszweck angemessenen Zeitraums - gegebenenfalls auch elektronisch - aufzuzeichnen, sodaß insbesondere in gerichtlichen Verfahren die Zertifizierung nachgewiesen werden kann, sowie

8. Vorkehrungen dafür zu treffen, daß die Signaturerstellungsdaten der Signatoren weder vom ZDA noch von Dritten gespeichert oder kopiert werden können.

(2) Ein ZDA hat für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zertifikaten vertrauenswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen, zu verwenden. Er hat insbesondere geeignete Vorkehrungen dafür zu treffen, daß Signaturerstellungsdaten geheimgehalten werden, daß Daten für qualifizierte Zertifikate nicht unerkannt gefälscht oder verfälscht werden können und daß diese Zertifikate nur mit Zustimmung des Signators öffentlich abrufbar sind. Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten sind technische Komponenten und Verfahren, die den Anforderungen des § 18 entsprechen, zu verwenden.

(3) Signaturerstellungsdaten der ZDA sind vor unbefugtem Zugriff zu sichern.

(4) Für qualifizierte elektronische Signaturen kann das Vorliegen der Voraussetzungen der Abs. 1 bis 3 im Rahmen der freiwilligen Akkreditierung (§ 17) bescheinigt werden.

(5) Bei einer qualifizierten elektronischen Signatur muss aus dem Zertifikat, aus der elektronischen Signatur oder aus dem Sicherheits- und Zertifizierungskonzept, auf das im Zertifikat Bezug genommen wird, hervorgehen, dass es sich um eine qualifizierte elektronische Signatur handelt.

(6) Für die Prüfung von qualifiziert signierten Daten sind technische Komponenten und Verfahren geeignet, die sicherstellen, dass

1. die signierten Daten nicht verändert worden sind,

2. die Signatur zuverlässig geprüft und das Ergebnis korrekt angezeigt wird,

3. der Prüfer feststellen kann, auf welche Daten sich die elektronische Signatur bezieht,

4. der Prüfer feststellen kann, welchem Signator die elektronische Signatur zugeordnet ist, wobei die Verwendung eines Pseudonyms angezeigt werden muss, und

5. sicherheitsrelevante Veränderungen der signierten Daten erkannt werden können.

Auf Ersuchen von Gerichten oder anderen Behörden hat ein ZDA die Prüfung der auf seinen qualifizierten Zertifikaten beruhenden qualifizierten Signaturen vorzunehmen.

Ausstellung qualifizierter Zertifikate

§ 8. (1) Ein ZDA oder eine in seinem Auftrag tätige Stelle hat die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises oder durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis, festzustellen. Der ZDA hat die Zuordnung bestimmter Signaturprüfdaten zu dieser Person durch ein qualifiziertes Zertifikat zu bestätigen.

(2) (entfällt BGBl 8/2008)

(3) Ein ZDA hat nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers Angaben über seine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft in das qualifizierte Zertifikat aufzunehmen, sofern ihm oder einer anderen Stelle (Abs. 1) diese Umstände zuverlässig nachgewiesen werden.

(4) Ein ZDA kann nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers im Zertifikat anstatt des Namens des Signators ein Pseudonym angeben. Das Pseudonym darf weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein.

Widerruf von Zertifikaten

§ 9. (1) Ein ZDA hat ein Zertifikat unverzüglich zu widerrufen, wenn

1. der Signator oder ein im Zertifikat genannter Machtgeber dies verlangt,

2. der ZDA Kenntnis vom Ableben des Signators oder sonst von der Änderung im Zertifikat bescheinigter Umstände erlangt,

3. das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde,

4. der ZDA seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden,

5. die Aufsichtsstelle gemäß § 14 den Widerruf des Zertifikats anordnet oder

6. die Gefahr einer mißbräuchlichen Verwendung des Zertifikats besteht.

(2) Können die in Abs. 1 genannten Umstände nicht sofort zweifelsfrei festgestellt werden, so hat der ZDA das Zertifikat jedenfalls unverzüglich zu sperren.

(3) Die Veröffentlichung einer Sperre und eines Widerrufs muss den Zeitpunkt ihrer Wirksamkeit enthalten. Dieser Zeitpunkt darf nicht später als eine Stunde nach der Eintragung liegen. Eine rückwirkende Sperre oder ein rückwirkender Widerruf ist unzulässig. Der Signator bzw. sein Rechtsnachfolger ist von der Sperre oder dem Widerruf unverzüglich zu verständigen.

(4) Ein ZDA hat ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gesperrten und der widerrufenen qualifizierten Zertifikate zu führen.

(5) Die Aufsichtsstelle hat das Zertifikat eines ZDA unverzüglich zu widerrufen, wenn

1. dem ZDA die Ausübung seiner Tätigkeit untersagt wird und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen ZDA übernommen werden oder

2. der ZDA seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen ZDA übernommen werden.

(6) Unverzüglichkeit ist dann gegeben, wenn die entsprechende Maßnahme an Werktagen ausgenommen Samstag, von 9 bis 17 Uhr innerhalb von drei Stunden und außerhalb dieser Zeit innerhalb von sechs Stunden erfolgt. Bei postalischer Verständigung ist Unverzüglichkeit dann gegeben, wenn die entsprechende Maßnahme innerhalb von zwei Werktagen erfolgt.

Qualifizierte Zeitstempeldienste

§ 10. Stellt ein ZDA qualifizierte Zeitstempeldienste bereit, so hat er im Sicherheits- und im Zertifizierungskonzept nähere Angaben darzulegen. Es sind technische Komponenten und Verfahren zu verwenden, die die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellen und den Anforderungen des § 18 entsprechen. Er hat weiters für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zeitstempeln vertrauenswürdige Systeme, Produkte und Verfahren zu verwenden,

die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen. Er hat insbesondere geeignete Vorkehrungen dafür zu treffen, dass Signaturerstellungsdaten geheimgehalten werden und Daten für qualifizierte Zeitstempel nicht unerkannt gefälscht oder verfälscht werden können.

Dokumentation

§ 11. (1) Ein Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen, die er zur Einhaltung dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffen hat, sowie das Ausstellen und gegebenenfalls die Sperre und den Widerruf von Zertifikaten zu dokumentieren. Dabei müssen die Daten und ihre Unverfälschtheit sowie der Zeitpunkt ihrer Aufnahme in das Protokollierungssystem jederzeit nachprüfbar sein.

(2) Auf Ersuchen von Gerichten oder anderen Behörden hat ein ZDA die Dokumentation nach Abs. 1 auszufolgen. Im Fall der Einstellung seiner Tätigkeit hat ein ZDA die Dokumentation nach Abs. 1 dem mit der Weiterführung der Verzeichnis- und Widerrufsdienste betrauten ZDA oder der Aufsichtsstelle auszufolgen.

(3) Die Aufbewahrungsdauer der Dokumentation nach Abs. 1 ist im Sicherheits- und Zertifizierungskonzept anzugeben. Die Dokumentation des Ausstellens, der Sperre und des Widerrufs eines qualifizierten Zertifikats ist bis zum Ablauf der allgemeinen Verjährungszeit im Sinne des § 1478 ABGB, gerechnet ab dem im Zertifikat eingetragenen Ende der Gültigkeit, aufzubewahren.

Einstellung der Tätigkeit

§ 12. Ein ZDA hat die Einstellung seiner Tätigkeit unverzüglich der Aufsichtsstelle anzuzeigen. Weiters hat er die im Zeitpunkt der Einstellung seiner Tätigkeit gültigen Zertifikate zu widerrufen oder dafür Sorge zu tragen, daß zumindest seine Verzeichnis- und Widerrufsdienste von einem anderen ZDA übernommen werden. Die Signatoren sind von der Einstellung der Tätigkeit sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der ZDA sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des ZDA Sorge zu tragen.

4. Abschnitt

Aufsicht

Aufsichtsstelle

§ 13. (1) Aufsichtsstelle ist die Telekom-Control-Kommission (§ 116 TKG 2003). Ihr obliegt die laufende Aufsicht über die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen.

(2) (entfällt BGBl 8/2008)

(3) Die Aufsichtsstelle hat dafür Sorge zu tragen, dass ein elektronisch allgemein zugängliches Verzeichnis der gültigen, gesperrten und widerrufenen Zertifikate für ZDA, der im Inland niedergelassenen ZDA, der von ihr akkreditierten ZDA und der Drittstaaten-ZDA, für deren Zertifikate ein im Inland niedergelassener ZDA nach § 24 Abs. 2 Z 2 einsteht, geführt wird. Auf Antrag sind auch andere im Ausland niedergelassene ZDA in dieses Verzeichnis aufzunehmen. Zertifikate für ZDA können auch von der Aufsichtsstelle ausgestellt werden. Die Aufsichtsstelle hat die bei ihr geführten Verzeichnisse gesichert im Internet zu veröffentlichen.

(4) Die Aufsichtsstelle hat den ZDA für ihre Tätigkeit und für die Heranziehung der RTR-GmbH eine mit Verordnung festgelegte kostendeckende Gebühr vorzuschreiben. Die Einnahmen aus dieser Gebühr fließen der Aufsichtsstelle zu und sind nach Heranziehung der RTR-GmbH oder der Bestätigungsstelle nach deren Aufwand weiterzuleiten.

(5) Die Aufsichtsstelle kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle (§ 19) bedienen.

(6) Die Mitglieder der Aufsichtsstelle sind gemäß Art. 20 Abs. 2 B-VG bei Ausübung ihres Amtes an keine Weisungen gebunden. Sofern gesetzlich nicht anderes bestimmt ist, hat die Aufsichtsstelle das AVG 1991 anzuwenden. Sie entscheidet in oberster Instanz. Die Anrufung des Verwaltungsgerichtshofs ist zulässig.

(7) Die Tätigkeit der Aufsichtsstelle nach diesem Bundesgesetz ist von ihrer Tätigkeit nach anderen Bundesgesetzen organisatorisch und finanziell zu trennen.

Aufsichtsmaßnahmen

§ 14. (1) Die Aufsichtsstelle kann zur Sicherstellung der Erfüllung der Pflichten aus diesem Bundesgesetz und der auf seiner Grundlage ergangenen Verordnung Zertifikate für ZDA oder von Signatoren widerrufen oder den Widerruf der Zertifikate von Signatoren durch den ZDA anordnen.

(2) (entfällt BGBl 8/2008)

(3) Sofern nicht nach Abs. 6 gelindere Mittel in Betracht kommen, ist einem ZDA die Ausübung seiner Tätigkeit ganz oder teilweise zu untersagen, wenn die für die Ausübung einer solchen Tätigkeit erforderlichen Voraussetzungen nach diesem Bundesgesetz oder den auf seiner Grundlage ergangenen Verordnungen nicht erfüllt werden.

(4) (entfällt BGBl 8/2008)

(5) Wenn die Aufsichtsstelle einem ZDA die Ausübung seiner Tätigkeit untersagt, hat sie für den Widerruf der Zertifikate des ZDA und der Signatoren Sorge zu tragen oder die Übernahme der erbrachten Signatur- und Zertifizierungsdienste oder zumindest seiner Verzeichnis- und Widerrufsdienste durch einen anderen ZDA zu veranlassen, sofern die beteiligten ZDA der Übernahme zustimmen. Die Signatoren sind von der Untersagung sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der ZDA sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des ZDA Sorge zu tragen.

(6) Die Aufsichtsstelle hat von einer Untersagung der Tätigkeit eines ZDA abzusehen, soweit die Anordnung gelinderer Mittel ausreicht, um die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen sicherzustellen. Sie kann insbesondere Auflagen erteilen, unter Setzung einer angemessenen Frist zur Behebung von aufgezeigten Mängeln Maßnahmen androhen oder eine Akkreditierung widerrufen.

Heranziehung der RTR-GmbH

§ 15. (1) Die Aufsichtsstelle kann sich bei der Durchführung der Aufsicht der RTR-GmbH (§ 5 KOG) bedienen.

(2) Die RTR-GmbH hat insbesondere

1. die Aufsichtsstelle bei der laufenden Aufsicht der ZDA zu unterstützen und die technischen Produkte, Verfahren und sonstigen Mittel, die im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste eingesetzt werden, sowie die Qualifikation des Personals zu überprüfen,

2. (entfällt BGBl 8/2008)

3. Verzeichnisse der Zertifikate für ZDA und der ZDA (§ 13 Abs. 3) sowie ein Verzeichnis der akkreditierten ZDA (§ 17 Abs. 1) zu führen,

4. für den Fall der Einstellung oder Untersagung der Tätigkeit eines ZDA einen Widerrufsdienst zu führen, sofern keine Übernahme im Sinne der §§ 12 oder 14 Abs. 5 erfolgt,

5. auf Anordnung der Aufsichtsstelle die Erfüllung der Voraussetzungen einer freiwilligen Akkreditierung (§ 17) zu erheben,

6. bei der Feststellung der Gleichwertigkeit von Prüfberichten aus Drittstaaten im Sinne des § 24 Abs. 3 mitzuwirken und

7. im Fall des begründeten Verdachts, daß die Sicherheitsanforderungen dieses Bundesgesetzes oder der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten werden, oder auf Verlangen eines ZDA unmittelbar die vorläufige Untersagung der Tätigkeit des ZDA oder vorläufig Maßnahmen im Sinne des § 14 Abs. 1 anzuordnen.

(3) Die RTR-GmbH kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle (§ 19) bedienen. Die Wahrnehmung ihrer Aufgaben in technischen Belangen hat in Abstimmung mit einer Bestätigungsstelle (§ 19) zu erfolgen. Im Rahmen ihrer Tätigkeit für die Aufsichtsstelle ist das Personal der RTR-GmbH an die Weisungen des Vorsitzenden oder des in der Geschäftsordnung bezeichneten Mitgliedes gebunden.

(4) Unbeschadet der Zuständigkeit der ordentlichen Gerichte können Kunden oder Interessenvertretungen Streit- oder Beschwerdefälle, insbesondere über die Qualität eines Zertifizierungsdienstes, die mit dem ZDA nicht befriedigend gelöst worden sind, der RTR-GmbH vorlegen. Die RTR-GmbH hat sich zu bemühen, innerhalb angemessener Frist eine einvernehmliche Lösung herbeizuführen. Die ZDA sind verpflichtet, an einem solchen Verfahren mitzuwirken und alle zur Beurteilung der Sachlage erforderlichen Auskünfte zu erteilen. Die RTR-GmbH hat Richtlinien für die Durchführung dieses Verfahrens festzulegen, die in geeigneter Form zu veröffentlichen sind. Mit Zustimmung des Antragstellers kann das Verfahren auch auf elektronischem Weg durchgeführt werden.

(5) § 13 Abs. 7 über die organisatorische und finanzielle Trennung ist auf die Tätigkeit der RTR-GmbH anzuwenden.

Durchführung der Aufsicht

§ 16. (1) Die ZDA haben den im Auftrag der Aufsichtsstelle handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Bücher und sonstigen Aufzeichnungen oder Unterlagen einschließlich der Dokumentation nach § 11 vorzulegen oder zur Einsicht bereitzuhalten, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren. Bestehende gesetzliche Verschwiegenheits- und Aussageverweigerungsrechte bleiben unberührt.

(2) Die Organe des öffentlichen Sicherheitsdienstes haben der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen über deren Ersuchen zur Durchführung der Aufsicht im Rahmen ihres gesetzmäßigen Wirkungsbereichs Hilfe zu leisten.

(3) Die Durchführung der Aufsicht nach den Abs. 1 und 2 ist unter möglichster Schonung der Betroffenen und ohne unnötiges Aufsehen so durchzuführen, daß dadurch die Sicherheit der Signatur- und Zertifizierungsdienste nicht verletzt wird.

Freiwillige Akkreditierung

§ 17. (1) ZDA, die der Aufsichtsstelle vor der Aufnahme ihrer Tätigkeit als akkreditierte ZDA die Einhaltung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nachweisen, sind auf Antrag von der Aufsichtsstelle zu akkreditieren. Akkreditierte ZDA dürfen sich mit Zustimmung der Aufsichtsstelle im Geschäftsverkehr als solche bezeichnen. Im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten darf diese Bezeichnung nur verwendet werden, wenn die Sicherheitsanforderungen nach § 18 erfüllt werden. Die Aufsichtsstelle hat dafür Sorge zu tragen, daß die akkreditierten ZDA in ein elektronisch jederzeit allgemein zugängliches Verzeichnis aufgenommen werden.

(2) Die freiwillige Akkreditierung eines ZDA ist in das qualifizierte Zertifikat aufzunehmen oder sonst in geeigneter Weise zugänglich zu machen.

(3) Die Aufsichtsstelle hat für die laufende Aufsicht über die von ihr akkreditierten ZDA Sorge zu tragen. Sie hat die Akkreditierung eines ZDA zu widerrufen, wenn die Voraussetzungen einer Akkreditierung nach Abs. 1 nicht mehr erfüllt sind. § 14 Abs. 6 ist sinngemäß auch beim Widerruf einer Akkreditierung anzuwenden.

5. Abschnitt

Technische Sicherheitserfordernisse

Sicherheitsanforderungen für technische Komponenten und Verfahren

§ 18. (1) Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verläßlich verhindern.

(2) Die bei der Erstellung einer qualifizierten Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, daß die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, daß dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden und dass der Signator zu diesem Zeitpunkt über die Anzahl der Signaturen, die er im Signaturvorgang auslöst, Kenntnis erlangt. Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muß sichergestellt sein.

(3) Bei der Erstellung und Speicherung von qualifizierten Zertifikaten sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung von Zertifikaten verhindern.

(4) (entfällt BGBl 8/2008)

(5) Die technischen Komponenten und Verfahren für die Erstellung qualifizierter elektronischer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen an sichere Signaturerstellungseinheiten nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen muss von einer Bestätigungsstelle (§ 19) bescheinigt sein.

Bescheinigungen von Stellen, die von anderen Mitgliedstaaten der Europäischen Union oder von anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zur Beurteilung der Sicherheitsanforderungen für sichere Signaturerstellungseinheiten nach Art. 3 Abs. 4 der Signaturrichtlinie namhaft gemacht wurden, sind den Bescheinigungen einer Bestätigungsstelle gleich zu halten.

(6) Entsprechen technische Komponenten und Verfahren den allgemein anerkannten Normen, die von der Europäischen Kommission nach Art. 3 Abs. 5 der Signaturrichtlinie festgelegt werden, so gelten die entsprechenden Sicherheitsanforderungen nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen als erfüllt.

Bestätigungsstelle

§ 19. (1) Die nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle zugewiesenen Aufgaben können nur von einer dazu geeigneten Einrichtung wahrgenommen werden.

(2) Eine Einrichtung ist zur Wahrnehmung der einer Bestätigungsstelle zugewiesenen Aufgaben geeignet, wenn sie

1. die erforderliche Zuverlässigkeit aufweist,
2. zuverlässiges Personal mit den für diese Aufgaben erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Kenntnissen über elektronische Signaturen, angemessene Sicherheitsverfahren, Kryptographie, Kommunikations- und Chipkartentechnologien sowie die technische Begutachtung solcher Komponenten, beschäftigt,
3. über ausreichende technische Einrichtungen und Mittel sowie eine ausreichende wirtschaftliche Leistungsfähigkeit verfügt und
4. die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit sicherstellt.

(3) Darüber hinaus sind für die Eignung einer Bestätigungsstelle die von der Europäischen Kommission nach Art. 3 Abs. 4 der Signaturrichtlinie festgelegten Mindestkriterien für die Benennung von Bestätigungsstellen maßgeblich. Der Bundeskanzler hat diese Kriterien im Einvernehmen mit dem Bundesminister für Justiz mit Verordnung kundzumachen.

(4) Der Bundeskanzler hat im Einvernehmen mit dem Bundesminister für Justiz mit Verordnung festzustellen, daß eine Einrichtung als Bestätigungsstelle geeignet ist. Eine solche Verordnung kann nur auf Antrag der betreffenden Einrichtung erlassen werden. Die Eignung kann nur festgestellt werden, wenn die Einrichtung nach ihren Statuten oder Satzungen oder nach ihrem Gesellschaftsvertrag, nach ihrer Organisation und nach ihrem Sicherheits- und Finanzierungskonzept die in Abs. 2 genannten Anforderungen erfüllt.

(5) Eine Bestätigungsstelle kann zur Erfüllung der ihr nach diesem Bundesgesetz oder der auf seiner Grundlage ergangenen Verordnungen zugewiesenen Aufgaben von anderen Einrichtungen oder Stellen Prüfberichte zu technischen Komponenten und Verfahren einholen.

(6) Die organisatorische Aufsicht über die Bestätigungsstelle obliegt der Aufsichtsstelle (§ 13).

6. Abschnitt

Rechte und Pflichten der Anwender

Allgemeine Informationspflichten der ZDA

§ 20. (1) Ein ZDA hat den Zertifikatswerber vor Vertragsabschluss schriftlich oder unter Verwendung eines dauerhaften Datenträgers allgemein verständlich über den Inhalt des Sicherheits- und des Zertifizierungskonzepts, über die möglichen Rechtswirkungen des von ihm verwendeten Signaturverfahrens, über die Pflichten eines Signators sowie über die besondere Haftung des ZDA zu unterrichten. Zudem hat er die Bedingungen der Verwendung des Zertifikats, wie etwa Einschränkungen seines Anwendungsbereichs oder des Transaktionswerts, bekanntzugeben; weiters ist auf eine freiwillige Akkreditierung (§ 17) sowie auf besondere Streitbeilegungsverfahren hinzuweisen.

(2) Auf Verlangen sind die in Abs. 1 genannten Angaben auch Dritten, die ein rechtliches Interesse daran glaubhaft machen, zugänglich zu machen.

(3) (entfällt BGBl 8/2008)

Pflichten des Signators

§ 21. Der Signator hat die Signaturerstellungsdaten sorgfältig zu verwahren, soweit zumutbar Zugriffe auf Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen. Er hat den Widerruf des qualifizierten Zertifikats zu verlangen, wenn die Signaturerstellungsdaten abhanden kommen, wenn Anhaltspunkte für deren Kompromittierung bestehen oder wenn sich die im qualifizierten Zertifikat bescheinigten Umstände geändert haben.

Datenschutz

§ 22. (1) Ein ZDA darf nur jene personenbezogenen Daten verwenden, die er zur Durchführung der erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

(2) Bei Verwendung eines Pseudonyms hat der ZDA die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berechtigtes Interesse im Sinne des § 8 Abs. 1 Z 4 und Abs. 3 DSG glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

(3) Die Auskunfts- und Mitwirkungspflichten des ZDA gegenüber Gerichten und anderen Behörden bleiben unberührt.

Haftung der ZDA

§ 23. (1) Ein ZDA, der ein Zertifikat als qualifiziertes Zertifikat ausstellt oder für ein solches Zertifikat nach § 24 Abs. 2 Z 2 einsteht, haftet gegenüber jeder Person, die auf das Zertifikat vertraut, dafür, daß

1. alle Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Ausstellung richtig sind und das Zertifikat alle für ein qualifiziertes Zertifikat vorgeschriebenen Angaben enthält,

2. der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung des Zertifikats im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen,

3. die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei Verwendung der von ihm bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,

4. das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind sowie

5. die Anforderungen des § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten technische Komponenten und Verfahren nach § 18 verwendet werden.

(2) Ein ZDA haftet zudem dafür, daß für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstigen Mittel für die Erstellung elektronischer Signaturen sowie für die Darstellung zu signierender Daten nur technische Komponenten und Verfahren nach § 18 verwendet werden.

(3) Der ZDA haftet nicht, wenn er nachweist, daß ihn und seine Leute an der Verletzung der Verpflichtungen nach den Abs. 1 und 2 kein Verschulden trifft. Kann der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach den Abs. 1 und 2 verletzt oder die zur Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffenen Vorkehrungen kompromittiert wurden, so wird vermutet, daß der Schaden dadurch verursacht wurde. Diese Vermutung ist widerlegt, wenn der ZDA als wahrscheinlich dartut, daß der Schaden nicht durch eine Verletzung bzw. Kompromittierung der im zweiten Satz genannten Verpflichtungen und Vorkehrungen verursacht wurde.

(4) Enthält ein qualifiziertes Zertifikat eine Einschränkung des Anwendungsbereichs, so haftet der ZDA nicht für Schäden, die sich aus einer anderen Verwendung des Zertifikats ergeben. Enthält ein qualifiziertes Zertifikat einen bestimmten Transaktionswert, bis zu dem das Zertifikat verwendet werden darf, so haftet der ZDA nicht für Schäden, die sich aus der Überschreitung dieses Transaktionswerts ergeben.

(5) Die Haftung eines ZDA nach Abs. 1 bis 3 kann im vorhinein weder ausgeschlossen noch beschränkt werden.

(6) Bestimmungen des Allgemeinen Bürgerlichen Gesetzbuchs und anderer Rechtsvorschriften, nach denen Schäden in anderem Umfang oder von anderen Personen als nach diesem Bundesgesetz zu ersetzen sind, bleiben unberührt.

7. Abschnitt
Anerkennung ausländischer Zertifikate

Anerkennung

§ 24. (1) Zertifikate, die von einem in der Europäischen Gemeinschaft oder im Europäischen Wirtschaftsraum niedergelassenen ZDA ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, sind inländischen Zertifikaten gleichgestellt. Qualifizierte Zertifikate solcher ZDA entfalten dieselben Rechtswirkungen wie inländische qualifizierte Zertifikate.

(2) Zertifikate, die von einem in einem Drittstaat niedergelassenen ZDA ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, werden im Inland anerkannt. Qualifizierte Zertifikate werden inländischen qualifizierten Zertifikaten rechtlich gleichgestellt, wenn

1. der ZDA die Anforderungen nach § 7 erfüllt und unter einem freiwilligen Akkreditierungssystem eines Mitgliedstaates der Europäischen Union oder des Europäischen Wirtschaftraums akkreditiert ist,
2. ein in der Europäischen Gemeinschaft oder im Europäischen Wirtschaftraum niedergelassener ZDA, der die Anforderungen nach § 7 erfüllt, für das Zertifikat haftungsrechtlich einsteht oder
3. im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Gemeinschaft einerseits und Drittstaaten oder internationalen Organisationen andererseits das Zertifikat als qualifiziertes Zertifikat oder der ZDA als Aussteller qualifizierter Zertifikate anerkannt ist.

(3) Ist in einem Drittstaat zum Nachweis der Sicherheitsanforderungen für qualifizierte elektronische Signaturen eine staatlich anerkannte Stelle eingerichtet, so werden Bescheinigungen dieser Stelle über die Einhaltung der Sicherheitsanforderungen für die Erzeugung qualifizierter elektronischer Signaturen den Bescheinigungen einer Bestätigungsstelle (§ 19) gleichgehalten, soweit die Aufsichtsstelle feststellt, daß die den Beurteilungen dieser Stellen zugrunde liegenden technischen Anforderungen, Prüfungen und Prüfverfahren jenen der Bestätigungsstelle gleichwertig sind.

8. Abschnitt

Schlußbestimmungen

Signaturverordnung

§ 25. Der Bundeskanzler hat mit Verordnung im Einvernehmen mit dem Bundesminister für Justiz die nach dem jeweiligen Stand der Wissenschaft und Technik zur Durchführung dieses Bundesgesetzes erforderlichen Rechtsvorschriften zu erlassen über

1. die Festsetzung pauschaler kostendeckender Gebühren für die Leistungen der Aufsichtsstelle und der RTR-GmbH sowie die Vorschreibung dieser Gebühren,
2. die Festsetzung der zur Erfüllung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen ausreichenden Finanzmittel sowie der für die Abdeckung des Haftungsrisikos der ZDA ausreichenden Finanzmittel, insbesondere die Festsetzung einer Mindestversicherungssumme für eine Haftpflichtversicherung,
3. die Zuverlässigkeit des ZDA und seines Personals (§ 7 Abs. 1),
4. die näheren Anforderungen an die technischen Komponenten und Verfahren sowie die technischen Produkte und sonstigen Mittel zur Anwendung der §§ 7 Abs. 2, 10 und 18, die Durchführung der Prüfung der technischen Komponenten und Verfahren nach § 18 sowie die Ausstellung der Bestätigung, daß diese Anforderungen erfüllt sind,
5. die Dauer der Weiterführung der Widerrufsdienste durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5),
6. die Anwendungsbereiche, Anforderungen und Toleranzen von qualifizierten Zeitstempeldiensten,
7. (entfällt BGBl 8/2008)
8. die Form, Darstellung und Verfügbarkeit des Zertifizierungskonzepts (zB Klartext),
9. die Dauer der Aufbewahrung einer Dokumentation (§ 11) und
10. die Art und Form der Kennzeichnung akkreditierter ZDA.

Verwaltungsstrafbestimmungen

§ 26. (1) Eine Verwaltungsübertretung begeht und ist mit Geldstrafe bis zu 4 000 Euro zu bestrafen, wer fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators mißbräuchlich verwendet.

(2) Ein ZDA begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 8 000 Euro zu bestrafen, wenn er

1. entgegen § 9 Abs. 1 seine Widerrufspflicht verletzt,
2. entgegen § 11 seine Dokumentationspflicht verletzt,
3. entgegen § 16 Abs. 1 nicht Einsicht in die dort genannten Bücher, sonstige Aufzeichnungen oder Unterlagen gewährt oder nicht die notwendigen Auskünfte erteilt oder
4. entgegen § 20 Abs. 1 den Zertifikatswerber nicht unterrichtet.

(3) Ein ZDA begeht eine Verwaltungsübertretung und ist mit Geldstrafe bis zu 16 000 Euro zu bestrafen, wenn er

1. entgegen § 6 Abs. 2 die Aufnahme seiner Tätigkeit nicht anzeigt oder das Sicherheitskonzept oder das Zertifizierungskonzept nicht vorlegt,

2. entgegen § 6 Abs. 5 nicht alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, der Aufsichtsstelle anzeigt,

3. entgegen § 7 Abs. 1 Z 2 keinen geeigneten Widerrufsdienst oder keinen geeigneten Verzeichnisdienst führt,

4. entgegen § 7 Abs. 1 Z 8 keine geeigneten Vorkehrungen dafür trifft, daß die Signaturerstellungsdaten der Signatoren weder vom ZDA noch von Dritten gespeichert oder kopiert werden können,

5. entgegen § 18 keine geeigneten technischen Komponenten und Verfahren für qualifizierte elektronische Signaturen verwendet, bereitstellt oder bezeichnet oder

6. trotz Untersagung durch die Aufsichtsstelle (§ 14 Abs. 3) die ihm untersagte Tätigkeit weiterhin ausübt.

(4) Eine Verwaltungsübertretung gemäß den Abs. 1 bis 3 liegt nicht vor, wenn die Tat den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

(5) Im Straferkenntnis können die Gegenstände, mit denen die strafbare Handlung begangen wurde, für verfallen erklärt werden.

Inkrafttreten und Verweisungen

§ 27. (1) Dieses Bundesgesetz tritt mit 1. Jänner 2000 in Kraft.

(2) Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

(3) § 13 in der Fassung des Bundesgesetzes BGBl. I Nr. 137/2000 tritt mit 1. Oktober 2000 in Kraft.

(4) Die §§ 5, 7, 15, 18, 19, 23, 24, 26, 27 und 29 in der Fassung des Bundesgesetzes BGBl. I Nr. 137/2000 treten mit dem auf die Kundmachung dieses Bundesgesetzes folgenden Tag in Kraft.

(5) Die Bestimmungen der § 13 Abs. 4, § 15 Abs. 1 bis 5, § 25 Z 1 und § 27 Abs. 5 in der Fassung des Bundesgesetzes BGBl. I Nr. 32/2001 treten mit 1. April 2001 in Kraft.

(6) § 4 in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 tritt mit 1. Jänner 2002 in Kraft.

(7) § 4 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 164/2005 tritt mit 1. Jänner 2007 in Kraft.

(8) § 1 Abs. 3, § 2 Z 1 bis 3a, 5, 9, 10, 12, 13 und 14, § 3 Abs. 2, § 4 Abs. 1 bis 3, § 5 Abs. 1 Z 2 und Abs. 3, die Abschnittsüberschrift und Paragrafenüberschrift vor § 6, § 6 Abs. 1 bis 5 und 7, die Paragrafenüberschrift vor § 7, § 7 Abs. 1 und Abs. 1 Z 2 bis 4 sowie 8 und Abs. 2 bis 6, § 8 Abs. 1, 3 und 4, § 9 Abs. 1, Abs. 1 Z 2 und 4, Abs. 2 bis 5, Abs. 5 Z 1 und 2 und Abs. 6, § 10 samt Überschrift, § 11 Abs. 1 bis 3, § 12, § 13 Abs. 1, 3 und 4, § 14 Abs. 1, 3, 5 und 6, § 15 Abs. 1 und Abs. 2 Z 1, 3, 4 und 7, Abs. 3 und 4, § 16 Abs. 1, § 17 Abs. 1 bis 3, die Paragrafenüberschrift vor § 18, § 18 Abs. 1, 2, und 5, § 19 Abs. 6, die Paragrafenüberschrift vor § 20, § 20 Abs. 1, § 21, § 22 Abs. 2 und 3, die Paragrafenüberschrift vor § 23, § 23 Abs. 1 bis 5, § 24 Abs. 1 bis 3 und Abs. 2 Z 1 bis 3, § 25 Z 2, 3, 6 und 10, § 26 Abs. 2 und 3 und Abs. 3 Z 4 bis 6 und § 28 Z 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 8/2007 treten am 1. Jänner 2008 in Kraft; gleichzeitig treten § 6 Abs. 6, § 8 Abs. 2, § 13 Abs. 2, § 14 Abs. 2 und 4, § 15 Abs. 2 Z 2, § 18 Abs. 4, § 20 Abs. 3, und § 25 Z 7 außer Kraft.

Vollzug

§ 28. Mit der Vollziehung dieses Bundesgesetzes sind betraut:

1. hinsichtlich der §§ 3, 4 und 23 der Bundesminister für Justiz,

2. hinsichtlich der §§ 13 bis 17 der Bundesminister für Verkehr, Innovation und Technologie,

3. hinsichtlich der §§ 22 und 26 der Bundeskanzler,

4. hinsichtlich der §§ 7 Abs. 1 Z 6 und 13 Abs. 4 der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Finanzen und

5. hinsichtlich der übrigen Bestimmungen der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz.

Hinweis auf Umsetzung

§ 29. Mit diesem Bundesgesetz wird die Richtlinie 99/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L Nr. 13 vom 19. Jänner 2000, S 12, umgesetzt.

Lebenslauf

Persönliche Daten	
Name	Ayni Qais
geboren	am 18 Juli 1982 in Kabul
Familienstand	ledig
Kontakt	Qais@A1.net
Staatsbürgerschaft	Österreich
Schulausbildung	
1988 – 1989	Volkschule / Kabul in Afghanistan
1989 – 1991	Volkschule / Delhi in Indien
1991 – 1993	Hauptschule / Wien
1993 – 1999	Gymnasium (naturwissenschaftlicher Teil) /Wien
Bundesheer	08/99 – 04/00 Panzergrenadierkompanie in Großmittel
Hochschulstudium	
Oktober 2000	Beginn des Wirtschaftsinformatik –Studiums an der UNI und TU Wien
Jänner 2006	Beginn der Diplomarbeit
Februar 2006	Mitarbeit beim EC3 Projekt – Mobile Signaturen
November 008	Abschluss der Diplomarbeit
Studienbegleitende Tätigkeiten	Tätig bei diversen Firmen als EDV & Mathematiklehrer EDV – Administrator bei diversen Privatfirmen Teamleiter bei Fa. Mobidata (Promotion und Marketing) derzeitige Beschäftigung als Hotelmanager bei MR Hotels Seit Oktober 2006 selbständig im Consulting Bereich
Fremdsprachen	Englisch, Dari, Persisch, Paschto, Hindi und Urdu

Wien, 05. November 2008