Technische Hintergründe für das rechtlichte Handeln im Internet

Rene Mayrhofer
Johannes Kepler Universität Linz
rene@mayrhofer.eu.org
PGP Schlüssel Fingerabdruck:
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE

A. Einleitung

Internet-Recht bewegt sich grundsätzlich an der Schnittstelle zwischen Gesetzgebung und Technik. Wie an vielen Schnittstellen gibt es auch hier Schwierigkeiten zu überwinden, und zwar nicht nur in der Findung gemeinsamer Ziele, Arbeitsgruppen und schlussendlich Lösungen, sondern vor allem im gegenseitigen Verständnis der den jeweils anderen Bereich betreffenden Probleme. Dieser Beitrag soll die technischen Hintergründe einiger aktueller Themen an dieser Schnittstelle allgemein verständlich näher bringen. Die Auswahl an Themen, welche aus technischer Sicht einer Klärung durch die Gesetzgebung bedürfen bzw. derer, die durch neue Gesetze die Entwicklung neuer technischer Systeme erfordern, ist derzeit kaum mehr überschaubar und wächst weiter. Daher erfolgt in diesem Beitrag eine Konzentration auf die technischen Grundlagen für viele dieser Themen sowie auf eine kleine Auswahl von Themen, die von allgemeinem, auch öffentlichem bzw. gesellschaftlichem Interesse sind. Konkret werden die folgenden Themen angesprochen:

- **Grundlagen aus der Kryptographie:** Das wissenschaftliche Fachgebiet der *Kryptographie*, also die Lehre der Geheimschriften, liefert die notwendigen Methoden zur Umsetzung verschiedener Forderungen an sichere Systeme. Diese Forderungen sind üblicherweise *Vertraulichkeit*, *Integrität*, *Authentizität* und *Verbindlichkeit*, wobei in der entsprechenden Fachliteratur oft auch *Identifizierung*, *Authentifizierung*, *Autorisierung* und *Verfügbarkeit* genannt werden. Zur Behandlung dieser Forderungen stehen im Wesentlichen die Techniken der *Verschlüsselung* und der *digitalen Signatur* zur Verfügung.
- **Sichere Signatur:** Zur Erstellung von digitalen Signaturen, die ähnliche Beweiskraft wie die handschriftliche Signatur besitzen, sind zusätzlich zu technischen Erweiterungen auch organisatorische Strukturen nötig. Die nötigen technischen Änderungen betreffen hauptsächlich die sichere Speicherung des Schlüssels, der zur Erstellung von digitalen Signaturen immer nötig ist, während die organisatorischen Strukturen für eine eindeutige Bindung zwischen einer natürlichen oder juristischen Person (oder auch eines Computersystems) und eben diesen digitalen Schlüsseln sorgen.
- **Digitales Rechte Management (DRM):** Zur Absicherung elektronischer Dokumente gegen missbräuchliche Verwendung werden derzeit so genannte DRM-Systeme in verschiedenen Ausprägungen eingeführt. Das Grundprinzip dabei ist jeweils eine Bindung der Dateien, also zum Beispiel Musik- oder Filmdateien, an eine geographische Region oder an einzelne Computersysteme. Mittels DRM können Rechteinhaber die erlaubten Verwendungsarten detailliert festlegen und in der Datei selbst verankern.

- **Peer-to-Peer Systeme:** *Peer-to-Peer*, oft auch durch *P2P* abgekürzt, bedeutet, dass die miteinander kommunizierenden Systeme gleichberechtigte Teilnehmer (so genannte „*Peers*“) sind. Als Abkehr von der bekannten Trennung in Server und Client kann jeder Teilnehmer sowohl Dienste anbieten – in der Rolle eines klassischen Servers – als auch Dienste anderer Teilnehmer verwenden – in der Rolle eines Clients. Die auch durch Medienarbeit bekannteste Anwendung von Peer-to-Peer Systemen ist der Dateiaustausch, bei dem durch entsprechende Programme ein direkter Zugriff auf die Dateien anderer Computersysteme und entsprechende Suchmöglichkeiten geschaffen werden, doch das Konzept ist vielseitiger und wird unter anderem auch für Dienste wie Internet-Telefonie eingesetzt. Durch die Weiterentwicklung der Peer-to-Peer Konzepte entstanden bereits drei Generationen von Systemen, die jeweils unterschiedliche Daten zugänglich machen beziehungsweise verschieden resistent gegen Strafverfolgung oder staatliche Zensur sind. Aktuellste Generationen von Peer-to-Peer Systemen verbergen zunehmend Daten wie die eindeutigen Internet-Adressen der jeweiligen Teilnehmer, die zur Identifizierung der Nutzer dienen könnten.

Diese Themen stellen eine subjektive Auswahl dar, sollten jedoch die derzeit am stärksten – auch durch die Tagespresse – diskutierten Gebiete abdecken. Der Beitrag ist auf Leser ohne technisches Detailwissen ausgerichtet, Erfahrung im Umgang mit Computersystemen, also zum Beispiel mit Webbrowsern und Emailprogrammen, wird jedoch angenommen.

B. Grundlagen der Kryptographie

Die Kryptographie, also die Lehre der Geheimschriften, liefert einige Methoden zur gesicherten Kommunikation. In der Fachliteratur werden oft die folgenden acht Anforderungen an sichere Systeme erwähnt, wobei die ersten vier durch technische Mittel gelöst werden können.

I. Anforderungen

1. Vertraulichkeit (Geheimhaltung)

Die erste dieser Anforderungen, die *Vertraulichkeit*, auch als *Geheimhaltung* bezeichnet, bedeutet, dass Außenstehende die übertragenen Informationen nicht mitlesen können, also dass nur berechtigte Parteien Zugriff auf geschützte Information erhalten. Diese Forderung wird von der Kryptographie durch die Methode der *Verschlüsselung* erfüllt.

2. Integrität

Integrität fordert, dass eine Nachricht den Empfänger exakt so erreicht, wie der Sender sie versandt hat, also die Sicherheit, dass eine Nachricht während der Über-

tragung nicht verändert wurde. Diese Forderung wird durch die Methode der *digitalen Signatur* erfüllt.[1]

3. Authentizität

Die Forderung der *Authentizität* bedeutet, dass der Absender einer Nachricht nicht unbemerkt verändert werden kann, also die Sicherheit, dass eine Nachricht wirklich vom vorgegeben Absender stammt. Diese Forderung wird ebenfalls durch die Methode der *digitalen Signatur* erfüllt

4. Unleugbarkeit (Verbindlichkeit)

Unleugbarkeit bedeutet eine noch stärkere Forderung als Integrität und Authentizität gemeinsam, da Integrität und Authentizität sich lediglich auf den eigentlichen Empfänger einer Nachricht, aber nicht auf Dritte beziehen. Die Forderung nach Unleugbarkeit besagt hingegen, dass, wenn der eigentliche Empfänger einer Nachricht diese einem Dritten zugänglich macht, sich letzterer ebenfalls von der Integrität und Authentizität dieser Nachricht, also davon, dass sie vom vorgegeben Absender stammt und nicht verändert wurde, unabhängig und selbständig überzeugen kann. Diese Forderung kann ebenfalls durch die Methode der *digitalen Signatur* erfüllt werden, es sind jedoch, je nach verwendetem Verfahren, unter Umständen zusätzliche Maßnahmen zu treffen.
Obwohl Unleugbarkeit in manchen Beiträgen auch als *Verbindlichkeit* aufgefasst wird, kann eine Verbindlichkeit in rechtlichem Sinne alleine durch technische Maßnahmen nicht garantiert werden.

5. Identifizierung

Identifizierung bedeutet die Feststellung der Identität einer Person oder eines Computersystems. Als technisches Mittel steht dazu im Normalfall nur die Übermittlung eines Namens beziehungsweise Kennzeichners, wie zum Beispiel eines Benutzernamens oder einer Identifikationsnummer, zur Verfügung. Identifizierung kann in realen Anwendungen nur in Zusammenhang mit organisatorischen Maßnahmen erfolgen.

6. Authentifizierung

Authentifizierung stellt meist den zweiten Schritt nach einer Identifizierung dar, und bedeutet den Beweis der festgestellten Identität einer Person. Technische Mittel zur Authentifizierung sind zum Beispiel Passwörter, physikalische Objekte wie Magnet- oder Chipkarten oder biometrische Authentifizierung, die verwendeten Methoden sind jedoch meist stark von der jeweiligen Anwendung abhängig. Im Allgemeinen werden drei Möglichkeiten zur Authentifizierung angegeben:

- **Wissen:** zum Beispiel durch Eingabe von PINs oder Passwörtern zum Beweis des Wissens und der impliziten Annahme, dass dieses Wissen nur der zu au-

[1] Anmerkung: Es gibt auch andere Methoden zur Erfüllung dieser Forderung, jedoch werden diese hier nicht weiter betrachtet.

thentifizierenden Person beziehungsweise dem zu authentifizierenden System bekannt ist.

- **Besitz:** zum Beispiel durch Vorlage von Ausweisen oder elektronisch lesbaren Dokumenten wie Chipkarten und der impliziten Annahme, dass eine Vervielfältigung dieser Objekte nur der authentifizierenden/ausstellenden Partei möglich ist.
- **Eigenschaft:** zum Beispiel durch Feststellung bestimmter eindeutiger Merkmale wie Fingerabdrücke, Iris-Abbilder oder Stimmbilder und der impliziten Annahme, dass diese Merkmale eindeutig einer natürlichen Person zuzuordnen sind.

Die erste Möglichkeit kann auch zur Authentifizierung autonomer Systeme eingesetzt werden, die beiden letzteren beziehen sich meist auf die Authentifizierung natürlicher Personen. Für erhöhte Sicherheit können mehrere dieser Möglichkeiten für einen Authentifizierungsvorgang kombiniert werden.

7. Autorisierung

Nach der Feststellung und des Beweises der Identität einer Person oder eines Systems dient die *Autorisierung* zur Feststellung der Berechtigungen dieser Person oder des Systems. Da die Menge der möglichen Berechtigungen sowie deren Vergabe vollkommen anwendungsabhängig sind, bedarf die Lösung dieser Forderung hauptsächlich organisatorischer Maßnahmen.

8. Verfügbarkeit

Die Forderung nach *Verfügbarkeit* besagt, dass ein System legitimen Benutzern die definierten Funktionen innerhalb der geforderten Zeiträume unbedingt zur Verfügung stellen muss. Insbesondere darf es einem nicht legitimierten (korrekt identifizierten, authentifizierten und autorisierten) Benutzer nicht möglich sein, die Verfügbarkeit eines Systems für legitimierte Benutzer einzuschränken.
Zur Erfüllung dieser Forderung können zwar technische Maßnahmen auf allen Ebenen der Implementierung, also vom Kommunikationssystem über die Rechnersysteme bis zur Anwendungslogik, zur Verbesserung der Verfügbarkeit eingesetzt werden, zur Abgabe von Garantien beziehungsweise zur Erfüllung von definierten Verfügbarkeitsmaßen ist jedoch immer das entsprechende Gesamtsystem inklusive seiner Benutzer zu betrachten. Rein technische Maßnahmen können daher eine geforderte Verfügbarkeit nur selten sicherstellen.

II. Methoden

Um einige der oben genannten Forderungen an sichere Systeme zu erfüllen, stehen bekannte Methoden aus der Kryptographie zur Verfügung. Die für diesen Beitrag relevanten Methoden sind Verschlüsselung und digitale Signatur.

1. Verschlüsselung

Verschlüsselung, auch als *Chiffrierung* bezeichnet, wandelt eine Nachricht, den so genannten *Klartext*, in eine unleserliche Nachricht, das so genannte *Chiffrat*, um. Der umgekehrte Vorgang wird als *Entschlüsselung* oder *Dechiffrierung* bezeichnet. Die Umwandlung zwischen Klartext und Chiffrat wird durch einen Code, die so genannte *Chiffre* oder auch *Verschlüsselungsalgorithmus*, bestimmt.

Es ist wichtig, zwischen den historischen Chiffren, bei denen die Sicherheit des Verfahrens vom Geheimnis um den Algorithmus selbst abhing, und den modernen Chiffren, bei denen das Verfahren öffentlich bekannt ist, zu unterscheiden. Moderne Chiffren verwenden einen digitalen Schlüssel um zu chiffrieren beziehungsweise zu dechiffrieren.

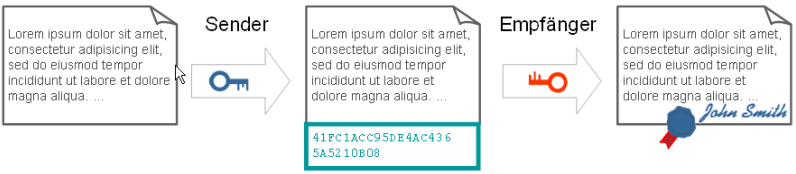
Ein Sender verschlüsselt üblicherweise die zu übertragende Information – bevor sie versandt wird – mit einem Teil eines digitalen Schlüssels. Wenn die Nachricht während der Übertragung von Dritten abgehört wird, ist es diesen unmöglich, ohne Kenntnis des passenden Schlüssels den Inhalt zu entziffern. Die Nachricht ist also geheim beziehungsweise vertraulich. Nur der rechtmäßige Empfänger kann die Entschlüsselung mit dem dazu passenden Schlüssel vornehmen und die Information entgegennehmen.

Das übertragene Chiffrat hat üblicherweise die gleiche Größe wie der Klartext. Es existieren sowohl Chiffren, die den gleichen Schlüssel zum Ver- wie zum Entschlüsseln verwenden (Verfahren mit *symmetrischen Schlüsseln*), als auch Chiffren, bei denen unterschiedliche Schlüssel verwendet werden (Verfahren mit *asymmetrischen Schlüsseln*). Letztere haben den Vorteil, dass jeder eine Verschlüsselung für einen bestimmten Empfänger vornehmen kann (der dazu nötige Schlüssel des Empfängers ist öffentlich bekannt), aber nur der legitime Empfänger die Entschlüsselung durchführen kann (mit dem nur ihm bekannten privaten Schlüssel). Bei der Erstellung von digitalen Schlüsseln für asymmetrische Verfahren wird daher ein *Schlüsselpaar* bestehend aus öffentlichem und privatem Schlüssel erstellt.

Beispiele für als sicher geltende symmetrische Chiffren sind *AES* (im Original *Rijndael*), *DES*, *Triple-DES*, *Twofish*, *RC6*, *RC4* oder *SEAL*, asymmetrische Chiffren sind *RSA* oder *ElGamal*.

2. Digitale Signatur

Die *digitale Signatur* ist ein Verfahren, mit dem der Sender einer Nachricht einen speziellen Block an die Nachricht anhängen kann, indem er wiederum einen Teil eines digitalen Schlüssels dazu verwendet. Der Empfänger kann dann diesen angehängten Block verwenden, um die Integrität und Authentizität zu prüfen. Wenn der empfangene Block zu der Nachricht passt, ist der Empfänger sicher, dass sie vom vorgegebenen Absender stammt und dass sie nicht verändert wurde. Auch für digitale Signaturen existieren sowohl symmetrische als auch asymmetrische Verfahren mit gleichen beziehungsweise verschiedenen Schlüsseln zur Signatur und zur Prüfung. Für die in diesem Beitrag besprochenen Themen sind asymmetrische Verfahren von größerer Bedeutung, weshalb die symmetrischen mit Verweis auf Standardliteratur[2] hier nicht weiter diskutiert werden.



Vergleichbar mit handschriftlichen Signaturen – aber im Gegensatz zur Verschlüsselung – ist der Signaturblock einer Nachricht beziehungsweise eines Dokumentes meist von konstanter Größe und deutlich kleiner als die signierte Nachricht. Diese Größenreduktion wird durch die Verwendung von so genannten *Hashes*, welche Fingerabdrücke von Nachrichten darstellen, erreicht. Anstelle der gesamten Nachrichten werden nur ihre entsprechenden Fingerabdrücke digital signiert.

Als Beispiele für Signaturalgorithmen werden hier die in der Änderung der Signaturverordnung[3] angegebenen verwendet: *RSA*, *DSA* und *ECDSA* sind asymmetrische Signaturalgorithmen, *SHA-1* und *RIPEMD-160* sind Fingerabdruckalgorithmen.

Allerdings lassen sich die weiteren Forderungen, nämlich die Verbindlichkeit bzw. Unleugbarkeit, die Identifikation, Authentifizierung, Autorisierung und die Verfügbarkeit nicht mit rein technischen Mitteln lösen. Dazu, und damit zum Aufbau von insgesamt sicheren Systemen, sind zusätzliche organisatorische Maßnahmen und damit ein Zusammenspiel mit der Gesetzgebung sowie den Rechtswissenschaften nötig.

---

2 B. Schneier: Applied Cryptography, John Wiley & Sons, ISBN 0-471-11709-9, 1996

3 527. Verordnung des Bundeskanzlers: Änderung der Signaturverordnung, Bundesgesetzblatt 30. Dezember 2004

C. Sichere Signatur

I. Ziel

Das Ziel der sicheren Signatur im österreichischen beziehungsweise der vergleichbaren qualifizierten Signatur im deutschen Signaturgesetz ist eine weitestgehende Gleichstellung mit der handschriftlichen.[4] Um eine hohe Sicherheit solcher rechtlich bindender Unterschriften mit entsprechender Beweiskraft zu gewährleisten, sind hier neben den technischen Maßnahmen wiederum organisatorische nötig.

II. Komponenten

1. Technische

Konkret wird zur Erstellung einer solchen sicheren Signatur eine Signaturkarte wie zum Beispiel die neuen Maestro-Karten, die zukünftig eingesetzten Gesundheitskarten, entsprechend ausgerüstete Mitgliedskarten wie die der Österreichischen Computergesellschaft oder auch die Kepler-Card der Universität Linz benötigt. Diese Chipkarten, auch Smartcards genannt, können den unbedingt geheim zu haltenden privaten Schlüssel sicher speichern und gewisse kryptographische Operationen selbständig ausführen. Zusätzlich wird ein Kartenleser mit integrierter Tastatur benötigt, um die Verbindung zwischen Computer und Signaturkarte herstellen zu können. Die Tastatur ist zur sicheren Eingabe der PIN, also des Codes zum Entsperren der Karte, nötig.

2. Organisatorische

Als organisatorische Maßnahme wird ein Zertifikat zur Bestätigung der Identität, also zur Authentifizierung gegenüber amtlichen Stellen, benötigt. Dieses Zertifikat kombiniert zwei der oben vorgestellten technischen Möglichkeiten zur Authentifizierung, nämlich Besitz (der Chipkarte) und Wissen (der zum Entsperren des privaten Schlüssels nötigen PIN), um eine angemessene Sicherheit bieten zu können. Als ergänzende organisatorische Maßnahme trägt die Verpflichtung von Karteninhabern, einen Verlust oder Diebstahl umgehend zu melden und dadurch eine Sperrung des Zertifikats zu veranlassen, zusätzliche Sicherheit bei.

III. Diskussion der Sicherheit

Der Unterschied zur gewöhnlichen digitalen Signatur besteht in eben diesen Punkten: Eine missbräuchliche Verwendung des Schlüssels zur Fälschung digitaler Signaturen ist ohne Besitz der Chipkarte und Kenntnis der PIN auch dann nicht möglich, wenn das verwendete Computersystem bereits kompromittiert ist, also nicht mehr vertrauenswürdig ist. Diese Resistenz gegen kompromittierte Computersysteme wird durch die Forderung einer in den Kartenleser integrierten Tastatur erreicht, da etwaig auf dem Computersystem laufende Programme so keinen Zugriff

[4] 30. Verordnung des Bundeskanzlers: Signaturverordnung – SigV, Bundesgesetzblatt 2. Februar 2000

auf die eingegebene PIN bekommen können. Der zweite Unterschied ist die starke Bindung des digitalen Schlüssels an eine (meist natürliche) Person durch entsprechende Zertifizierung durch vertrauenswürdige Dritte. Derzeit übernehmen zum Beispiel Banken den Identifizierungsteil dieser Zertifizierung, wobei die technische Infrastruktur von A-Trust betrieben wird. Die starke Bindung ermöglicht es, dass öffentliche Verzeichnisse geschaffen werden können, in denen die öffentlichen Schlüssel für die registrierten Personen gespeichert sind. So kann eine sichere Kommunikation mit einer Person stattfinden, ohne dass diese persönlich bekannt ist.

Die Chipkarte mit zugehöriger PIN wird in der praktischen Anwendung benötigt, um sichere Signaturen zu erstellen sowie Dokumente zu entschlüsseln, die gesichert empfangen wurde. Die jeweils gegensätzlichen Operationen, nämlich die Prüfung einer solchen sicheren Signatur und die Verschlüsselung von Dokumenten für bestimmte Personen erfordern keine Karte, sondern können von jedem unter Zuhilfenahme des bekannten öffentlichen Schlüssels durchgeführt werden (vergleiche Abschnitt B.II).

IV. Mögliche Probleme aus technischer Sicht

Der in Abschnitt C.II.2 angesprochene Widerruf von kompromittierten, also als nicht mehr sicher anzusehenden Zertifikaten, ist entscheidend für die Sicherheit des Gesamtkonzeptes. Denn eine gestohlene Chipkarte mit zusätzlich bekannt gewordener PIN[5] eröffnet durch die konzeptionell anvisierte Gleichstellung mit der handschriftlichen Unterschrift weitgehende Missbrauchsmöglichkeiten. In der Praxis zeigt sich aber, dass gerade der zeitnahe Zertifikatswiderruf problematisch ist und für große Umgebungen im Bereich mehrerer Millionen Zertifikate als nach wie vor ungelöst gilt.[6]

Bei der breiten Einführung von Bürgerkarten könnten signifikante Akzeptanzprobleme auftreten, da die Kostenträger, also die Endbenutzer, die Gruppe mit dem geringsten Nutzen darstellen. Für staatliche Stellen und große Institutionen sind die Einsparungen beträchtlich, für Endbenutzer ist die Zeitersparnis bei der Verwendung elektronischer Dokumente anstatt gedruckter derzeit allerdings kaum wahrnehmbar.

---

[5] Anmerkung: Da die PIN von den Benutzern festgelegt wird und geändert werden kann, ist die Verwendung einfach zu merkender und dadurch einfach zu erratender Zahlen wie des Geburtsdatums oder der eigenen Telefonnummer sehr wahrscheinlich. Die PIN wird daher in vielen Fällen von einem Angreifer erraten werden können, sodass lediglich der Diebstahl der entsprechenden Karte nötig ist. Eine erzwungene Verwendung zufälliger PINs wie bei Maestro-Karten würde diese Unsicherheit beseitigen, jedoch die üblichen Probleme von notierten Passwörtern erzeugen.

[6] P. Gutmann: PKI: It's Not Dead, Just Resting, veröffentlicht unter http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf, gekürzte Version in IEEE Computer Magazine, August 2002

Zusätzlich dazu steht derzeit noch keine Bürgerkarten-Software für Systeme außer Microsoft Windows zur Verfügung, und selbst diese ist nicht im Quelltext zugänglich. Dies macht es unmöglich, sichere Signaturen zu erstellen, zu prüfen oder die angebotene Verschlüsselung zu nutzen, wenn nicht Microsoft Windows eingesetzt wird. Eine unabhängige Prüfung dieser sehr sicherheitskritischen Programme wird leider ebenfalls verwehrt, da der dazu nötige Quelltext nicht offen beziehungsweise nur mit Vorbehalten zur Verfügung gestellt wird.

Ein weiteres aus Sicht des Autors noch unterbewertetes und somit zu wenig bedachtes Problem ist das der sicheren Zeitstempel. Derzeit steht noch keine entsprechende Infrastruktur zur Verfügung, um auch dem Zeitpunkt der digitalen Signatur eines Dokumentes oder einer Nachricht Beweiskraft geben zu können. Ohne Sicherstellung dieses Signaturzeitpunktes könnten digitale Signaturen für viele Anwendungen im Vertragsrecht weiterhin problematisch bleiben.

V. Amtssignatur

Die *Amtssignatur* ist eine Anwendung der sicheren Signatur und hat zum Ziel, dass die Authentizität amtlicher Bescheide in digitaler Form durch unabhängige Überprüfbarkeit gewährleistet ist. Zur Kennzeichnung solchermaßen gültiger amtlicher Schriftstücke wird eine digitale Bildmarke zur einfachen optischen Erkennbarkeit sowie eine entsprechende sichere Signatur des Dokumentes nach der Signaturverordnung verlangt.[7] Während die Bildmarke keinerlei Fälschungssicherheit bieten kann und nur optischen Zwecken dient, kann die sichere Signatur über das damit verbundene Zertifikat der unterzeichnenden Person und deren Rolle als Vertreter der jeweiligen Behörde zugeordnet werden.

Erste Versuche mit online veröffentlichten amtlichen Schriftstücken zeigen allerdings, dass die Umsetzung der Amtssignatur teilweise technisch mangelhaft erfolgt und damit die verlangten rechtlichen Auflagen nicht eingehalten werden. Ein Beispiel dafür ist die vom Bundeskanzler betriebene Plattform „RIS“, erreichbar unter *http://ris1.bka.gv.at/authentic/index.aspx* . Amtliche Dokumente, die Rechtsvorschriften (insbesondere Bundesgesetze und Verordnungen) enthalten, werden dort (scheinbar) mit Amtssignatur verlautbart, und die Auswahl eines solchermaßen (scheinbar) gegen Fälschung geschützten Dokumentes erzeugt die Ansicht einer Signaturprüfung inklusive der geforderten Bildmarke und Information über den Unterzeichner des jeweiligen Dokumentes.[8] Die Signaturprüfung erfolgt hier laut Anzeige auf dem Server und das positive Ergebnis dieser Prüfung wird zum jeweiligen Dokument vermerkt. Allerdings werden die zur unabhängigen Prüfung benötigten Felder der zu Folge § 8 Abs 1 BundesgesetzblattG verlangten sicheren Signatur nicht angegeben und eine Prüfung der Signatur zur Feststellung der Authentizität des jeweiligen Dokumentes auf Seiten der Bürger ist nicht möglich. Insbesondere die digitale Signatur selbst ist im Dokument nicht enthalten und kann auch nicht aus

[7] E-Government-Gesetz (E-GovG), BGBl. I Nr. 10/2004 §19

[8] Zum Beispiel https://ris1.bka.gv.at/authentic/findbgbl.aspx?name=entwurf&format=auth&docid=COO_2026_100_2_171105 für die weiter oben zitierte Novelle zur Signaturverordnung

den angezeigten Daten rekonstruiert werden. Durch diese Unmöglichkeit der Signaturprüfung scheint § 8 Abs 1 BundesgesetzblattG verletzt. Aus technischer Sicht erlaubt das Fehlen des eigentlichen Signaturwertes in den publizierten Dokumenten einfach durchführbare Fälschungen, die von den Empfängern der Schriftstücke nicht als solche erkennbar sind.[9]

D. Digitale Rechte Management (DRM) Systeme

Neben der sicheren Übertragung von Emails und Dokumenten ist auch der Schutz von digitalen Medien ein aktuelles Thema. *DRM* Systeme sind *Digitale Rechte Management* Systeme (von Kritikern auch als Systeme zum „Digitalen Restriktions Management“ bezeichnet). Sie sind eine weitere konkrete Anwendung der oben besprochenen Grundlagen der Kryptographie.

I. Ziele

Die Ziele von DRM sind sowohl die Bindung von Mediendaten an spezielle Endgeräte wie zum Beispiel PCs, Autoradios oder tragbare MP3-Player, als auch die Definition von Einschränkungen zur Verwendung dieser Medien. Dies erlaubt ein Abspielen der Medien nur auf den vom Rechteinhaber beziehungsweise -verwerter definierten Geräten. Mögliche Einschränkungen für die Verwendung von Medien sind zum Beispiel, dass eine Datei nur fünf Mal wiedergegeben werden darf oder dass sie nur ein einziges Mal auf CD gebrannt werden darf.

II. Ansatz

Die Methode zur Erreichung dieser Ziele ist im Wesentlichen die Verschlüsselung der Dateien speziell für jedes Endgerät mit einem jeweils eigenen Schlüssel. Dieser zum Entschlüsseln nötige Schlüssel wird an das Endgerät gebunden, und zwar entweder durch Maßnahmen in Software oder durch Zusatzhardware wie das standardisierte *Trusted Platform Module*, auch *TPM* genannt. Beim Wiedergeben einer auf diese Art geschützten Datei wird der Schlüssel des entsprechenden Gerätes verwendet, um die Dateien automatisch zu entschlüsseln. Dabei kontrolliert die Wiedergabe-Software auch die Einhaltung der Restriktionen, die zum Beispiel direkt in der Datei definiert sind oder auch bei jedem Abspielvorgang von einem entsprechend definierten Server abgerufen werden.

[9] Anmerkung: Die Veränderung eines solchermaßen publizierten oder die Erstellung eines neuen Schriftstückes ist trivial, wenn diese auf einem eigenen Web-Server publiziert werden. Durch so genannte (einfach durchführbare) DNS-Poisoning oder Phishing Angriffe kann den Empfängern des gefälschten Schriftstückes vorgetäuscht werden, diese Dokumente stammten von einem vertrauenswürdigen Server wie z.B. dem „RIS“ des BKA.

III. Probleme aus technischer Sicht

Das Hauptproblem aktueller DRM Systeme aus technischer Sicht ist deren Sicherheit. Einerseits muss der gerätespezifische Schlüssel so sicher abgelegt sein, dass er zwar ständig zur Verfügung steht, aber nicht aus dem Gerät entfernt und auf andere übertragen werden kann. Ein Schutz dieses Schlüssels in Software ist kaum zu garantieren, wie durch entsprechende Programme zur Extraktion der Medien aus dem eigentlich geschützten DRM-Format gezeigt wird. Zur entsprechenden Absicherung dieser Schlüssel wird Zusatzhardware benötigt, die noch nicht ausgereift ist und Probleme des Datenschutzes mit sich bringt. Andererseits verlangen Systeme, bei denen die Einschränkungen bei jedem Abspielvorgang von einem Server abgerufen werden, dass die Abspielgeräte ständig online mit dem Internet verbunden sind sowie eine entsprechende Verfügbarkeit der Lizenz-Server. Beide Anforderungen sind allerdings derzeit noch nicht zufriedenstellend erfüllbar.

Als weitere Probleme ergeben sich im Moment eine gewisse Unvereinbarkeit mit der Privatkopie und der daraus legitimierten Urheberrechtsabgabe sowie zum Teil massive Akzeptanzprobleme auf Seiten der Benutzer. Dies ist meist durch die oft unverhältnismäßigen Restriktionen sowie durch Eingriffe in die Privatsphäre bedingt. Die derzeit eingesetzte Zusatzhardware beschränkt sich nicht auf die eigentlich ausreichende Speicherung der digitalen Schlüssel, sondern kann auch zu umfassenden Kontrollmöglichkeiten genutzt werden. So könnte die Installation einer legal erworbenen Software auf dem Computersystem eines Kunden verhindert werden, da dieses von den Rechteinhabern oder -verwertern als „nicht sicher“ deklariert wird. Die damit entstehende zusätzliche Macht auf Seiten der Rechteverwerter führt zu einer beinahe kategorischen Ablehnung solcher Zusatzhardware bei den meisten technisch interessierten Benutzern.

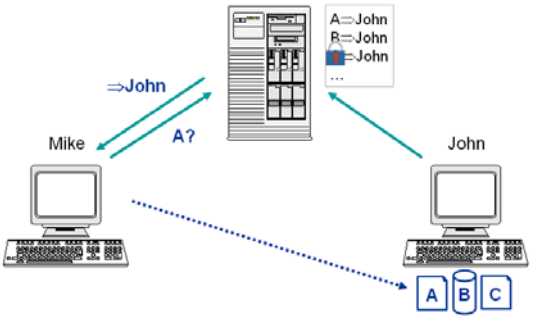
E. Peer-to-Peer

Ein weiteres Anwendungsgebiet kryptographische Methoden ist die Kommunikation über Computernetzwerke. Vor allem beim Verzicht auf zentrale Server und dem damit einhergehenden direkten Austausch von Daten zwischen vernetzten Computern ergeben sich neue Fragen der Sicherheit, des Datenschutzes und des Urheberrechtes. *Peer-to-Peer* bedeutet lediglich, dass die kommunizierenden Systeme gleichberechtigt sind – diese werden als *Peers* bezeichnet, um die strikte Unterteilung in *Server* und *Clients* zu vermeiden. Dieses Konzept ist nicht neu, denn das gesamte Internet ist grundsätzlich ein Peer-to-Peer System. Für Router im Internet ist es unbedeutend, ob eine Webcam Daten an ein Anzeigegerät sendet, ob Daten zwischen zwei PCs ausgetauscht werden oder ob ein Server Daten an Clients sendet. Es werden nur Datenpakete übertragen und jeder Teilnehmer ist gleichzeitig Sender und Empfänger.
Dies ist ein deutlicher Unterschied zum bekannten Rundfunk, also Radio und Fernsehen: Dort gibt es nur wenige Sender, aber viele Empfänger, die keine Antwortmöglichkeit haben. Im Internet kann jeder Teilnehmer automatisch auch senden.

I. Generation 0: Client/Server

Client/Server Systeme stellen die herkömmliche Kommunikationsform dar. Dabei kontaktieren alle Clients einen zentralen Server, auf dem auch die Dateien gespeichert sind. Ein Abrufen dieser Dateien erfolgt direkt vom Server, sodass dieser Zugriff auf alle Informationen hat, im Besonderen welcher Client welche Dateien anfordert, sowie umfangreiche Sperrmöglichkeiten bestehen. Ein Beispiel dafür ist ein Dateiserver in einem lokalen Netzwerk.

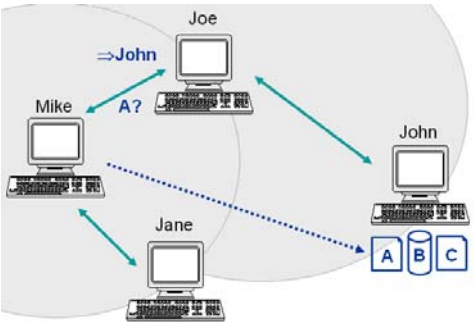
II. Generation 1: Zentrale Suche, dezentrale Daten



Die erste Generation von Peer-to-Peer Systemen verfolgt den Ansatz, dass die eigentlichen Dateien nicht mehr auf einem zentralen Server lagern, sondern auf die Peers verteilt sind, aber dass ein Server weiterhin Suchfunktionen bereitstellt. Dazu melden sich die Peers wiederum bei diesem Server an und übermitteln die Liste von Dateien, die sie anbieten. Der Server erstellt daraus eine Suchliste und kann auf Anfrage die Adresse des Peers zurückliefern, der die entsprechende Datei speichert. Wenn wie im obigen Beispiel Mike an der Datei A interessiert ist, wird der Server die Adresse von John zurückliefern, da dieser jene Datei speichert. Aus Effizienzgründen erfolgt die Übertragung direkt zwischen den Peers, also von John zu Mike.
Dadurch, dass der Server immer noch Zugriff auf alle Informationen hat, lassen sich auch hier zentrale Sperren einsetzen. Es wird zwar nicht die Verfügbarkeit der Datei

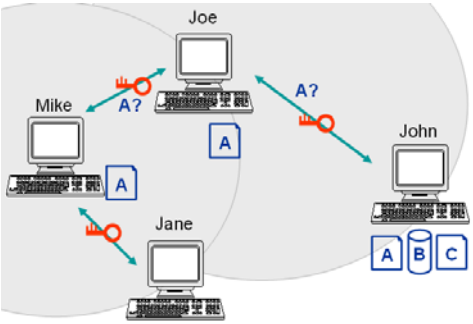
selbst gesperrt, aber indem sie im Index gesperrt wird, kann sie nicht mehr lokalisiert werden.
Ein bekanntes Beispiel für diese erste Generation ist *Napster* zum Austausch von Musikdateien, aber auch Instant Messenger wie *ICQ* oder *MSN* sowie Internet-Telefonie, Video-Telefonie oder *Bittorrent* beruhen auf diesem Prinzip.

III. Generation 2: Dezentrale Suche



Die zweite Generation verzichtet auf einen zentralen Server. Sowohl die Dateien als auch die Suchanfragen sind dezentral. Jeder Peer hat daher nur eine begrenzte Sicht auf das gesamte Netzwerk und ist üblicherweise nur mit wenigen ihm „nahe liegenden“ Peers verbunden. Wenn Mike in dieser Generation nach einer Datei A sucht, wird zum Beispiel Joe die Suche an ihm bekannte Peers weiterleiten und von John eine Antwort erhalten. Diese Antwort gibt er wiederum an Mike weiter, dem nun der Speicherort der Datei A bekannt ist. Die Übertragung erfolgt direkt.
Jeder Peer hat nur Zugriff auf eigene Kommunikationsdaten, also welche Suchanfragen an ihn gestellt werden, mit wem er in direktem Kontakt steht bzw. welche Dateien er wem übersendet und von wem er selbst Dateien bezieht. Zentrale Sperren sind hier nicht mehr möglich, eine Verfolgung anderer Peers, die Dateien vom eigenen Peer herunterladen, allerdings sehr wohl.
Beispiele für Dateitauschprogramme dieser Generation sind *Kazaa* und *Gnutella*.

IV. Generation 3: Anonymität



Die aktuellste Generation hat die selbe Struktur wie Generation 2. Allerdings wird ein hoher Grad an Anonymität dadurch erreicht, dass die Kommunikation verschlüsselt erfolgt. Die zwischen zwei Peers ausgetauschten Nachrichten sind nur diesen bekannt und können nicht von Dritten abgehört werden. Zusätzlich erfolgen sowohl Suche als auch Transfer indirekt über Ketten aus mehreren Peers. Wenn in dieser Generation Mike nach einer Datei A sucht, wird Joe diese Suche weiterleiten. John, der die Anfrage von Joe bekommt, weiß nicht ob Joe die Suche selbst gestartet hat oder nur weiterleitet. Wird die Datei gefunden, so wird sie über die Kette hinweg kopiert. John weiß wiederum nicht, ob Joe die Datei selbst bezieht oder dies nur als Stellvertreter für einen anderen tut. Umgekehrt weiß auch Mike, wenn er die Datei von Joe erhält, nicht, ob sie ursprünglich bei Joe gespeichert war oder ob dieser sie als Stellvertreter erst bezogen hat.
Bekannte Beispiele für solche aktuellen Systeme sind *Freenet* zum Dateiaustausch, *Mixmaster* zur anonymen Übermittlung von Emails und *Tor* für allgemeine Kommunikationsprotokolle.

Solche Anonymität erlaubt einerseits den Tausch von geschütztem oder rechtswidrigem Material, der nicht oder nur unter großem Aufwand verfolgt werden kann. Andererseits erlaubt sie unter totalitären Regierungsverhältnissen eine abhörsichere und leugbare Kommunikation zwischen Bürgern. So ist zum Beispiel das angesprochene *Freenet* in China weit verbreitet, und viele Informationen aus dem und in das Land gehen über diese Kanäle und entgehen dadurch der strengen Zensur der Regierung.

F. Zusammenfassung

Das Kernthema an der Schnittstelle zwischen Recht und Technik ist sicherlich die Kryptographie. Deren Methoden der *Verschlüsselung* und *digitalen Signatur* stellen die Basis für Anwendung wie die Bürgerkarte mit der dadurch ermöglichten sicheren Signatur oder Systeme des Digitalen Rechte Managements dar. Die Kryptographie selbst kann bereits als ausgereift angesehen werden, da ihre grundlegenden Methoden in den entsprechenden Fachkreisen gut verstanden werden und die Algorithmen gegeneinander austauschbare Bausteine darstellen. Werden in der Kryptoanalyse neue Angriffstechniken entwickelt, so können die betroffenen kryptographischen Algorithmen meist einfach durch neue, sicherere ausgetauscht werden.

Im Zeitalter der digitalen Informationsübermittlung haben die digitalen Medien, also üblicherweise Musik- und Filmdateien, bereits große Bedeutung erlangt. Zum Schutz dieser digitalen Medien vor Missbrauch sind beide Methoden nötig, also Verschlüsselung und digitale Signatur. Obwohl aktuelle DRM Systeme noch nicht ausgereift genug für weite Verbreitung sind, könnten zukünftige Systeme die Medienlandschaft deutlich prägen. Entscheidend dafür ist allerdings eine Zusammenarbeit aller beteiligten Parteien, also eine Involvierung der Künstler, Vertriebskanäle sowie der Konsumenten.
Nicht nur die Medien, sondern auch deren Übertragung – also die gesamte Kommunikation zwischen Computersystemen – bedarf heutzutage eines umfassenden Schutzes. Noch schwieriger, auch von der rechtlichen Seite betrachtet, sind Kommunikationsverfahren, die ohne zentralen Server auskommen. Bei diesen Peer-to-Peer Verfahren kommunizieren die Endgeräte direkt miteinander und werfen dadurch Probleme des Datenschutzes und des Urheberrechtes auf.

Die Verbindung von Informatik und Rechtswissenschaften ist noch sehr jung, doch ist sie eine wichtige. Denn viele der aktuellen Probleme in diesen Gebieten lassen sich nur durch eine enge Kooperation mit dem jeweils anderen Gebiet lösen. Derzeit befinden wir uns erst am Anfang, und noch zu lösende Probleme des Internet-Rechtes, oder allgemeiner des Informatik-Rechtes, werden in den nächsten Jahren vermutlich sprunghaft steigen. Der Physiker, Mathematiker und Philosoph Stephen Hawking äußerte sich dazu insofern, dass die Computerviren, also destruktive Programme, die bisher einzige Form von digitalem Leben seien, die wir bisher zu schaffen im Stande waren. Aktuelle Entwicklungen stellen Vorstufen zu digitalem Leben dar, wie zum Beispiel elektronische Buchungs- und Bietagenten, die im Auftrag ihres Besitzers handeln. Die Technik entwickelt sich rapide voran, und bestehende Rechtsunsicherheiten sollten daher besser jetzt als später ausgeräumt werden.