Jürgen Stuhldreier

Die digitale Signatur: Grundlagen, Konzepte, Einsatzmöglichkeiten

Diplomarbeit

Examicus

DIE DIGITALE SIGNATUR: GRUNDLAGEN, KONZEPTE, EINSATZMÖGLICHKEITEN

Diplomarbeit

eingereicht bei

Prof. Dr. Wolfgang König
Institut für Wirtschaftsinformatik
Fachbereich Wirtschaftswissenschaften
Johann Wolfgang Goethe-Universität
Frankfurt am Main

von

stud. rer. pol. Jürgen Stuhldreier

Studienrichtung: Betriebswirtschaftslehre, 13. Fachsemester

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

ASCII	American Standard Code of Information Interchange
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CCI	Competence Center Informatik
CCITT	Comité Consultatif International Télégraphique et Téléphonique
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DFN	Deutsches Forschungsnetz
DFN-PCA	Deutsches Forschungsnetz-Policy Certification Authority
DN	Distinguished Name
DuD	Datenschutz und Datensicherheit
EDI	Electronic Data Interchange
FTP	File Transfer Protocol
S-HTTP	Secure Hypertext Transfer Protocol
IDEA	International Data Encryption Algorithm
IPES	Improved Proposed Encryption Standard
ITSEC	Information Technology Security Evaluation Criteria
ITSG	Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH
ITU	International Telecommunication Union
IuKDG	Informations- und Kommunikationsdienste-Gesetz (des Bundes)
mod	Modula

MS	Microsoft
NBS	National Bureau of Standards
OSI	Open Systems Interconnection
PEM	Privacy Enhanced Mail
PES	Proposed Encryption Standard
PGP	Pretty Good Privacy
PIN	Personal Identification Number
Ra	Registration Authority
RSA	Ronald Rivest Adi Shamir Leonard Adleman
SigG	Signaturgesetz
SigV	Signaturverordnung
SSL	Secure Sockets Layer
TC	TrustCenter
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TSS	Transaction Security System
UN	United Nations
VerbrKrG	Verbraucherkredit-Gesetz
VU	Virtuelles Unternehmen
WWW	World Wide Web
ZPO	Zivilprozeßordnung

1. EINLEITUNG

1.1 Einführung in die Thematik

Elektronische Netze wie das Internet werden zunehmend für die tägliche Kommunikation und Kooperation genutzt. Offene Netze (keine Beschränkung auf bestimmte Nutzergruppen) erweisen sich für den Nutzer als attraktiv und wirtschaftlich bedeutsam: Sie sind für jeden leicht zugänglich und ermöglichen grundsätzlich Kontakt mit jedem weltweit. Im Internet entwickeln sich elektronische Märkte und elektronischer Verwaltungsverkehr. Aus transaktionstheoretischer Sicht reduzieren elektronische Märkte Transaktionskosten; die Vertragsanbahnung und -abwicklung zwischen örtlich über den Globus verteilten Kooperationspartnern vereinfacht sich wesentlich.
In einer Zeit des Arbeitsplatzabbaus bieten elektronische Netze zahlreiche Möglichkeiten für neue Märkte, neue Arbeitsplätze, ein umweltverträgliches Wirtschaftswachstum (Reduktion von papiergebundenen Dokumenten) und Kostenersparnis (Vermeidung von Medienbruch). Die Nutzung von Informations- und Kommunikationsnetzen weist aber auch neue Probleme auf: Daten können auf dem Weg der Übermittlung unmerklich verändert werden. Die Beweiskraft ist angesichts spurloser Manipulationsmöglichkeiten sehr gering.
Die Teilnehmer eines elektronischen Datenverkehrs möchten wissen, wie vertrauenswürdig der Inhalt einer Information ist, bevor sie eine Entscheidung treffen. Sie möchten wissen, von wem die Information stammt (Authentizität bzw. Identität) und ob die Information während der Übermittlung veränderte wurde (Integrität). Im informationstheoretischen Sinn soll Information zur Findung der bestmöglichen Lösung beitragen; Information, deren Inhalt aufgrund zahlreicher Manipulationsmöglichkeiten fragwürdig ist, kann diesem Anspruch nicht gerecht werden.
Kryptographische Verfahren erschweren durch Verschlüsselung den unbefugten Zugriff auf Daten in elektronischen Netzen. Mit Hilfe der digitalen Signatur können der Urheber und die nachträgliche Manipulation eines digitalen Dokuments nachgewiesen werden. Die Verwendung digitaler Signaturkonzepte verlangt das Vorhandensein einer organisatorischen Infrastruktur, einer ”Sicherungsinfrastruktur”[1], welche die erzeugten Chiffrier- und

[1] Hervorhebungen bestimmter Begriffe innerhalb des Textes erfolgen durch gerade gesetzte (englische) Anführungszeichen. Hervorhebungen zu Beginn einer Aufzählung

Dechiffrierschlüssel verwaltet, die Identität eines Schlüsselinhabers bezeugt und kompromittierte Schlüssel sperrt.

1.2 Zielsetzung der Arbeit

Der Gesetzgeber hat mit der Formulierung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) die Wichtigkeit der Vertrauenswürdigkeit des elektronischen Geschäftsverkehrs unterstrichen. Ziel dieser Arbeit ist es, die Signifikanz des Konzepts der digitalen Signatur im elektronischen Geschäftsverkehr zu verdeutlichen. Insbesondere soll aufgezeigt werden, daß die Verwendung der digitalen Signatur eines organisatorischen Rahmens bedarf, einer Sicherungsinfrastruktur (Vertrauensmodell), die die Nutzung der digitalen Signatur mit dem Ziel der Vertrauenswürdigkeit elektronischen Datenaustauschs gewährleistet. Es sollen sowohl die technischen Komponenten (Verschlüsselungsverfahren) als auch die organisatorischen Komponenten (z.B. Vertrauensinstanzen) eines möglichen Vertrauensmodells beschrieben werden. Einen Schwerpunkt bildet die Untersuchung möglicher Vertrauensmodelle; es sollen die wesentlichen Eigenschaften, mögliche Vor- und Nachteile der Vorgehensweise herausgearbeitet werden. Ziel dieser Arbeit ist es nicht, einen detaillierten technischen Einblick in Signaturverfahren zu geben; vielmehr möchte die Arbeit einen ersten fundierten Einblick in die Thematik der ”digitalen Signatur” zum jetzigen Zeitpunkt vermitteln und Ansatzpunkte für die derzeitige Diskussion unterschiedlicher Vertrauensmodelle liefern.

1.3 Aufbau der Arbeit

Die Ausführungen dieser Arbeit beginnen mit einer Einführung in die Aufgaben der traditionellen Unterschrift (Abschnitt 2.1). Anschließend erfolgt die Definition der digitalen Signatur (Abschnitt 2.2.1). Abschnitt 2.2.2 wägt die eigenhändige Unterschrift gegen die digitale Signatur ab. Es folgen die Anforderungen an digitale Signaturen (Abschnitt 2.2.3) und die Darstellung unterschiedlicher Signaturkonzepte (Abschnitt 2.2.4). Im Abschnitt 2.3 werden rechtliche Gesichtspunkte digital signierter Dokumente betrachtet. Zunächst erfolgt ein

---

erfolgen in Kursivschrift. Ebenso werden Formeln und Variablen kursiv gesetzt.

kurzer Überblick des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) des Bundes (Abschnitt 2.3.1), dann wird die rechtliche Anerkennung digital signierter Dokumente untersucht (Abschnitt 2.3.2).
Der Abschnitt 3 beschäftigt sich mit den kryptologischen Grundlagen: Zunächst werden symmetrische (Abschnitt 3.2), asymmetrische (Abschnitt 3.3) und hybride (Abschnitt 3.4) Verschlüsselungsverfahren exemplarisch dargestellt. Anschließend erfolgt die Verfahrensweise der digitalen Signierung (Abschnitt 3.5).
Abschnitt 4 beschreibt Vertrauensinstanzen als zentralen Bestandteil von Sicherungsinfrastrukturen. Zunächst beschreibt Abschnitt 4.1 die Unzulänglichkeit digitaler Signaturen und die notwendige Ergänzung durch Vertrauensinstanzen. Dann erfolgt die Definition (Abschnitt 4.2.1) und Aufgabenstellung (Abschnitt 4.2.3) dieser Institutionen. Wesen und Inhalt eines Schlüsselzertifikats beschreibt Abschnitt 4.2.2.
Abschnitt 5 untersucht die wesentlichen Merkmale unterschiedlicher Vertrauensmodelle (Sicherungsinfrastrukturen). Es erfolgt eine Unterscheidung in eine ”basisbestimmte Sicherungsinfrastruktur” (Abschnitt 5.1), eine ”marktbestimmte Sicherungsinfrastruktur” (Abschnitt 5.2) und schließlich eine ”staatlich verantwortete Sicherungsinfrastruktur” am Beispiel des deutschen Signaturgesetzes (SigG) (Abschnitt 5.3).
Im Schlußteil (Abschnitt 6) erfolgt zunächst die Zusammenfassung der wesentlichen Ergebnisse der Arbeit (Abschnitt 6.1) und abschließend im Abschnitt 6.2 ein kurzer Ausblick auf eine mögliche Kombination der in Abschnitt 5 untersuchten Ansätze (Abschnitt 6.2.1). Schließlich werden einige Anforderungen für eine Sicherungsinfrastruktur angeführt(Abschnitt 6.2.2).

Wörtliche Zitate werden in typographische (deutsche) Anführungszeichen gesetzt.