Elektronische Unterschriften

Konstantinos Georgopoulos, M.A.

FH Kaiserslautern, Standort FH Zweibrücken
Business-Value of IT – IT-Sicherheit
Prof. Knopper
20.12.2013

Konstantinos Georgopoulos, M.A.

Business-Value of IT – IT Sicherheit
Prof. Knopper
20.12.2013

Einleitung

„Der Bedarf an elektronischen Signaturen nimmt zu, das Halbwissen darüber leider ebenfalls“[1]

Elektronische Unterschriften gewinnen zunehmend an Bedeutung und sind sogar im heutigen Alltag gar nicht weg zu denken. Zwar können Dokumente, z.B. Verträge elektronisch erfasst werden, die rechtsverbindliche Unterzeichnung dieser erfolgt regelmäßig mit eigenhändiger Unterschrift der Unterzeichnenden. Dieser Umstand führt im Massengeschäft und vor allem bei räumlicher Trennung der Unterzeichnenden zwangsläufig zu Ineffizienzen. Es entsteht der Wunsch nach einer der eigenhändigen Unterschrift gleichgestellten Technik. Damit tangiert diese Anforderung sowohl rechtliche als auch (sicherheits)technische Aspekte, die in diesem Zusammenhang zu berücksichtigen sind.

Häufig werden die hierbei verwendeten Begriffe elektronische Signatur und digitale Signatur fälschlicherweise gleichgestellt. Bei der elektronischen Signatur handelt es sich um den rechtlichen Begriff, bei der digitalen um den technisch-mathematischen Begriff. Im Folgenden soll auf beide Aspekte näher eingegangen werden.

Rechtliche Aspekte

Bereits 1997 hat der deutsche Gesetzgeber ein Signaturgesetz (SigG) beschlossen, der die Voraussetzungen für die Gleichsetzung der elektronischen Signatur mit der handschriftlichen Unterschrift regelt.[2] Die damals geregelten Auflagen waren so streng, dass mit Verabschiedung der EG-Signaturrichtlinie 1999/93/EG das Gesetz grundlegend im neu erlassenen Signaturgesetz im Jahr 2001 überarbeitet worden ist.[3] Die Änderung betraf vor allem die genehmigungsfreie Zulassung von Zertifizierungsstellen, wobei diese als Ausgleich für auftretende Fehler streng haften sollen.[4]

[1] Schmoldt (2008), S. 6
[2] Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung (2003), S. 1
[3] http://de.wikipedia.org/wiki/Signaturgesetz_(Deutschland), letzter Zugriff: 17.12.2013
[4] http://de.wikipedia.org/wiki/Signaturgesetz_(Deutschland), letzter Zugriff: 17.12.2013

Neben dem Signaturgesetz ist auch die Signaturverordnung einschlägig, die ergänzend Einzelregelungen beinhaltet bezüglich der Anforderungen an die Zertifizierungsdiensteanbieter, der technischen Produkte und Verfahren die in diesem Zusammenhang eingesetzt werden, sowie der Kostenregelung. [5] Der Gesetzgeber unterscheidet im Signaturgesetz drei Kategorien die in der folgenden Tabelle näher erläutert werden:[6]

Form	Definition	Beispiel
(Einfache) elektronische Signatur (EES)	Nach §2 Nr. 1 SigG: Daten in elektronischer Form, die anderen Daten beigefügt sind und zur Authentifizierung dienen.	Ein Angebot wird in MS Word geschrieben und die eingescannte handschriftliche Unterschrift des Verfassers wird als Grafik in den Text eingefügt. Anschließend wird die Datei als PDF-Datei im Anhang zu einer Email an den Empfänger versandt.
Fortgeschrittene elektronische Signatur (FES)	Nach §2 Nr. 2 SigG: Zusätzliche Anforderungen gegenüber EES: Signaturen, die • ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind und • seine Identifizierung ermöglichen, • mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seine alleinigen Kontrolle halten kann, und • mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann	Das in MS Word erstellte Angebot wird als Datei gespeichert. Diese von einem weiteren Programm mit dem Private Key der mit einem Passwort aktiviert wird signiert. Die Weise der Verknüpfung des Dokumentes mit der Signatur macht das spätere Ändern am Text unmöglich. Auf Grund der Zuordnung wird die Urheberschaft dokumentiert.
Qualifizierte elektronische Signatur (QES)	Nach §2 Nr. 3 SigG: Zusätzliche Anforderungen gegenüber FES: Signaturen, die • auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und • mit einer sicheren Signaturerstellungseinheit erzeugt werden.	Ablauf im Wesentlichen wie bei der FES, allerdings wird hier zum Erstellen der digitalen Signatur spezielle Soft- und Hardware z.B. ein Lesegerät (USB-Stick) mit Chipkarte, eingesetzt. Diese Chipkarte wird durch die Eingabe einer geheimen PIN aktiviert. Die Echtheit des Signatur ist zudem zertifiziert.

Darüber hinaus regelt der Gesetzgeber die Qualifizierte elektronische Signatur mit Anbieter-Akkreditierung, die auch als akkreditierte elektronische Signatur bezeichnet wird. Hierbei unterzieht sich der Zertifizierungsdiensteanbieter der freiwilligen Akkreditierung gemäß § 15

[5] http://de.wikipedia.org/wiki/Signaturverordnung_(Deutschland), letzter Zugriff: 17.12.2013

[6] Eigene Darstellung, Inhalt entnommen aus: Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung (2003), S. 14 f.

SigG.[7] Diesem wird ein Gütezeichen erteilt der die umfassend geprüfte technische und administrative Sicherheit der Signatur zum Ausdruck bringt.[8]

Da für Rechtsgeschäfte, z.B. Kaufverträge die Formfreiheit gilt bedarf es grundsätzlich keiner Signatur[9] so dass meist eine EES oder FES ausreicht. Allerdings gibt es Rechtsgeschäfte die gemäß § 126 BGB explizit die Schriftform verlangen. Dazu zählen die Kündigung eines Arbeitsvertrages gemäß § 623 BGB, die Erteilung eines Arbeitszeugnisses gemäß § 630 BGB, das Schuldanerkenntnis und –versprechen gemäß §§ 780, 781 sowie der Abschluss eines Verbraucherdarlehensvertrages.

Nur die QES ist laut SigG der eigenhändigen Unterschrift gleichgestellt.[10] Beispielsweise erfolgt die Anmeldung zum Handelsregister durch Notare ausschließlich mit einer qualifizierten elektronischen Unterschrift.[11] Auch Steuerberater bedienen sich dieses Verfahrens in dem sie die Umsatzsteuervoranmeldungen an das zuständige Finanzamt übermitteln. Auch der deutsche Personalausweis ist seit November 2010 mit einer Chipkarte versehen und für die QES gegen Zahlung einer Gebühr aktivierbar, wobei dieser ohne Zertifikat ausgestellt wird, so dass man ein solchen käuflich erwerben muss.[12]

Technische Aspekte

Sowohl bei einer handschriftlichen Unterschrift als auch bei der elektronischen Signatur sind die zwei wesentlichen Anforderungen Authentizität und Integrität zu berücksichtigen. Authentizität bedeutet die Gewährleistung der Echtheit der Herkunft des Signierenden und Integrität die Unverfälschtheit des Inhalts des signierten Dokumentes.[13]

Auch für digitale Signaturen kommen asymmetrische kryptografische Verfahren in Anwendung, die eine öffentlichen (public key) und einen privaten Schlüssel (private key) vorsehen. „Die Bundesnetzagentur veröffentlicht im Bundesanzeiger eine Übersicht über die

[7] Eine aktuelle Auflistung der Zertifizierungsdiensteanbieter findet sich online auf der Seite der Bundesnetzagentur: http://www.bundesnetzagentur.de/cln_1912/DE/Service-Funktionen/QualifizierteelektronischeSigantur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/ZertifizierungsDiensteAnbietr_node.html

[8] Die Bundesnetzagentur kann so ein Gütezeichen nach §15 SigG erteilen.

[9] Wenn nicht explizit im Gesetz ausdrücklich die Schriftform oder die QES verlangt wird.

[10] Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung (2003), S. 19

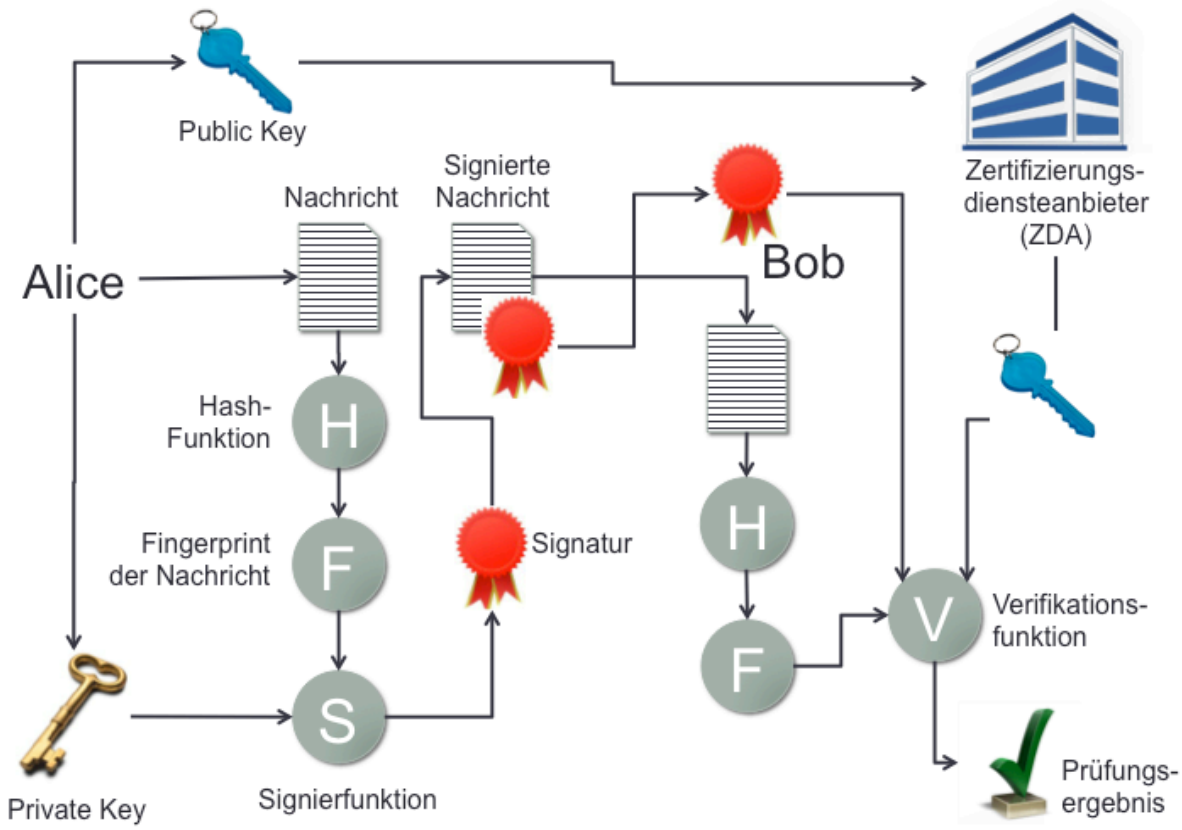
[11] http://de.wikipedia.org/wiki/Qualifizierte_elektronische_Signatur, letzter Zugriff: 17.12.2013

[12] Wobei dies den Vorteil hat, dass man sich den Zertifizierungsdiensteanbieter selbst aussuchen kann. http://de.wikipedia.org/wiki/Personalausweis_(Deutschland)#Qualifizierte_elektronische_Signatur_.28QES.29, letzter Zugriff: 18.12.2013

[13] Crantz (2010), S. 168; Groß/Matheis (2011), S. VII

Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen."[14]

„Ein Zertifikat des Zertifizierungsdiensteanbieters (ZDA) ist die elektronische Bescheinigung, dass der Signaturprüfschlüssel und damit auch der korrespondierende Signaturschlüssel einer Person zugeordnet wurde und die Identität dieser Person bestätigt werden kann (vgl. § 2 Nr. 6 Signaturgesetz). Bei der elektronischen Signatur enthält das Zertifikat den öffentlichen Schlüssel, mit dem der während der Signaturerstellung verschlüsselte Hashwert (Prüfsumme) des elektronischen Dokuments entschlüsselt und gegen einen neu erstellten Hashwert verglichen und damit die Authentizität des elektronischen Dokuments überprüft werden kann."[15]



Eigene Darstellung, in Anlehnung an Wolf (1999)

[14] http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2013Algorithmenkatalog.pdf?__blob=publicationFile&v=2

[15] http://de.wikipedia.org/wiki/Qualifizierte_elektronische_Signatur, letzter Zugriff: 18.12.2013

RSA-Berechnungsbeispiel

Im Folgenden soll ein einfaches Beispiel für die Verschlüsselung mittels RSA dargestellt werden.[16] Will man einen Text verschlüsseln, müssen zunächst die Buchstaben in Zahlen umgewandelt werden, so z.B. mit Hilfe des ASCII-Codes. Wir wählen hier die Zuordnung A = 01, B = 02, C = 03, etc. sowie 00 = Leerzeichen.

Darüber hinaus sei angenommen, dass jeweils drei Zeichen zu einer Zahl zusammengefasst werden. Die Buchstabenfolge AXT wird also zu 012420. Die kleinste zu verschlüsselnde Zahl ist dann 000000 (drei Leerzeichen), die größte 262626 (ZZZ). Der Modulus N = p * q muss also größer als 262626 sein.

Klartext: W I K I P E D I A

Kodierung: 23 09 11 09 16 05 04 09 01

Schlüsselerzeugung

Zunächst werden geheim zwei Primzahlen gewählt, z.B. p=307 und q=859.
Damit ergibt sich:
N = p * q = 263713 → RSA-Modul
phi(N) = (p-1) * (q-1) = 262548 → Eulersche Phi-Funktion
e = 1721 (zufällig, teilerfremd zu phi(N))
d = 1373 (das multiplikative Inverse zu e mod phi(N) mit Hilfe des erweiterten euklidischen Algorithmus)
Öffentlicher Schlüssel: e = 1721 und N = 263713 → Schlüsselpaar (e, N) = (1721, 263713)
Privater Schlüssel: d = 1373 und N = 263713 → Schlüsselpaar (d, N) = (1373, 263713)

Verschlüsselung

$C_n = K_n^e \bmod N$ für n=1,2,3(,...)
$C_1 = 230911^{1721} \bmod 263713 = 001715$
$C_2 = 091605^{1721} \bmod 263713 = 184304$
$C_3 = 040901^{1721} \bmod 263713 = 219983$

Entschlüsselung

$K_n = C_n^d \bmod N$ für n=1,2,3(,...)
$K_1 = 001715^{1373} \bmod 263713 = 230911$ → WIK
$K_2 = 184304^{1373} \bmod 263713 = 091605$ → IPE
$K_3 = 219983^{1373} \bmod 263713 = 040901$ → DIA

Signatur

$C_n = K_n^d \bmod N$
$C_1 = 230911^{1373} \bmod 263713 = 219611$
$C_2 = 091605^{1373} \bmod 263713 = 121243$
$C_3 = 040901^{1373} \bmod 263713 = 138570$

Verifikation

$K_n = C_n^e \bmod N$
$K_1 = 219611^{1721} \bmod 263713 = 230911$ → WIK
$K_2 = 121243^{1721} \bmod 263713 = 091605$ → IPE
$K_3 = 138570^{1721} \bmod 263713 = 040901$ → DIA

[16] Entnommen aus: http://de.wikipedia.org/wiki/RSA-Kryptosystem, letzter Zugriff: 18.12.2013

Literaturverzeichnis

Bundesnetzagentur: www.bundesnetzagentur.de

Crantz (2010): Elektronischer Rechnungsversand: Was ist bei Signaturen und EDI-Verfahren in der Praxis zu beachten?, in BC 2010, S. 168 – 172.

Groß/Matheis (2011): Im Blickpunkt: Electronic Invoicing, in Betriebs-Berater 34.2011 v. 28.08.2011, S. VI- VII.

Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung (2003): Digitale Signatur, Leitfaden zum Einsatz digitaler Signaturen, letzter Zugriff: 18.12.2013, online abrufbar unter: www.hessen-it.de/mm/DigitaleSignatur.pdf

Schmoldt (2008): Leitfaden Elektronische Signatur, Version 5, Release Datum 4. Dezember 2008, letzter Zugriff: 17.12.2013, online abrufbar unter: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CFEQFjAA&url=http%3A%2F%2Fwww.signature-perfect.de%2Fdocs%2FLeitfaden_Elektronische_Signatur.pdf&ei=n2CwUv6tD8PXtAazvIGYDQ&usg=AFQjCNGh7Jn2IdQOKFwEpCJ5SAthtRtUJA&sig2=b4HHLS10MKgsYQpkAxyVBg

Wikipedia: www.wikipedia.org

Wolf (1999): Verifikation digitaler Signaturen, letzter Zugriff: 18.12.2013, online abrufbar unter: http://www.informatik.tu-darmstadt.de/BS/Lehre/Sem98_99/T11/index.html#tth_sEc3