Signatur und Zeitstempel zur Wahrung von Authentizität und Integrität

Niels Fromm | fromm@cms.hu-berlin.de

Der folgende Artikel beschreibt die Eigenschaften von Signaturen als Grundlage für die rechtssichere Nutzung elektronischer Kommunikation und deren Einsatz auf dem Dokumentenserver der Humboldt-Universität zu Berlin.

Unter den Begriffen Signatur oder elektronische Signatur und Zeitstempel versteht man Verfahren, die dazu dienen, Authentizität und Integrität von Daten in elektronischer bzw. digitaler Form zu sichern. Es können beliebige Arten von elektronischen Daten mit einer Signatur oder einem Zeitstempel versehen werden, z. B. auch Bild- oder Videodateien. Im Bereich des elektronischen Publizierens bestehen die elektronischen Daten aber meist aus Dokumenten wie MS Word- oder Adobe PDF-Dateien. Die wohl bekannteste Anwendung ist die Signatur von Rechnungen in elektronischer Form.

Authentizität bedeutet dabei, dass einem signierten Dokument eindeutig die Person zugeordnet werden kann, die die Signatur erstellt hat. Dies kann der Autor oder der Absender eines elektronischen Dokumentes sein. Unter Integrität wird in diesem Zusammenhang die Unversehrtheit z. B. eines elektronischen Dokumentes verstanden. Dies bedeutet, dass ein elektronisches Dokument vor Veränderungen oder Manipulationen geschützt ist. Die Fragen „Wer hat eine Nachricht gesendet?“ und „Wurde die Nachricht nach dem Absenden unbefugt verändert?“ sind schon bei den bisherigen Kommunikationsformen wie Telefon, Fax und Brief von großem Interesse. Sie gewinnen hinsichtlich von Dokumenten in elektronischer Form, die über das Internet über-mittelt werden, zusätzlich an Bedeutung, da diese ohne besondere Sicherungen spurlos verändert und damit verfälscht werden können. Da elektronischen Dokumenten eine nachprüfbare Beziehung zu ihrem Urheber fehlt, sind im Internet Manipulationen oder das Abstreiten von Handlungen möglich, ohne dass dies erkannt und verhindert werden könnte.

Eine rechtssichere Nutzung der elektronischen Kommunikation, wie der Kommunikation über E-Mail, ist allerdings nur denkbar, wenn solcher Missbrauch der technischen Möglichkeiten wirksam ausgeschlossen werden kann. Das Konzept der elektronischen Signaturen stellt eine Möglichkeit dar, eine im Sinne der Authentizität und Integrität von elektronischen Dokumenten sichere Kommunikation zu ermöglichen.

Nach der europäischen Signaturrichtlinie [1], die im Jahr 2001 durch das Signaturgesetz in deutsches Recht umgesetzt wurde, ist eine rechtssichere Kommunikation nur mit Hilfe von qualifizierten elektronischen Signaturen möglich. Zeitstempel sind eine besondere Form dieser Signaturen, die vorrangig der Feststellung eines bestimmten Zeitpunktes und nicht der Authentifizierung dienen. So kann mit einem Zeitstempel rechtssicher die Existenz von Daten zu einem bestimmten Zeitpunkt bewiesen werden, nicht aber, von wem diese Daten stammen.

Abb. 1: Signaturherstellungsgerät

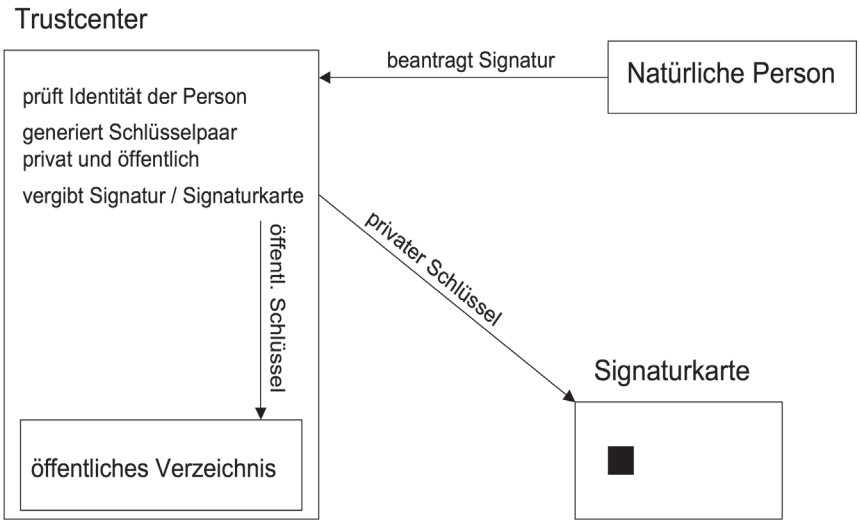

Abb. 1: Ablauf Ausgabe Signaturkarte

Technisch basiert eine qualifizierte elektronische Signatur auf zwei Verfahren: einem asymmetrischen Kryptografieverfahren und einer Hashfunktion. Bei asymmetrischen Kryptografieverfahren kommen zwei Schlüssel zum Einsatz. Es gibt einen öffentlichen und einen vom Nutzer geheim zu haltenden privaten Schlüssel, weshalb dieses Verfahren oft auch als „Public-Key"-Verfahren bezeichnet wird. Der öffentliche Schlüssel darf und soll veröffentlicht werden und kann dann von jedem anderen Anwender benutzt werden, um an den Eigentümer eine verschlüsselte Nachricht zu senden. Mit dem privaten Schlüssel des Eigentümers kann dieser dann die Nachricht wieder entschlüsseln. Bekannt ist die Anwendung eines solchen Public-Key-Verfahrens zum Beispiel bei der SSL-Verschlüsselung von Webseiten beim Online-Banking zur sicheren Eingabe von Daten. Beim Dokumentenserver wird diese Art der Verschlüsselung genutzt, um die Eingabe von persönlichen Daten bei der Abgabe von elektronischen Publikationen abzusichern.

Eine Hashfunktion ist im mathematischen Sinne eine Einwegfunktion, deren Ziel die Abbildung unterschiedlich großer Eingabemengen in eine kleine Ausgabemenge ist. Das Resultat einer solchen Hashfunktion bildet der sogenannte Hashwert. Somit können beliebig große Dateien durch einen kleinen Hashwert mit fester Größe eindeutig identifiziert werden. Kleinste Änderungen an der Datei resultieren in einem anderen Hashwert.

Zu einer qualifizierten elektronischen Signatur gehört auch ein sogenannter „vertrauenswürdiger Dritter" oder Trustcenter, in Deutschland sind dies unter anderem die Trustcenter der Deutschen Telekom oder der Deutschen Post (siehe [2]). Für den Betrieb eines solchen Trustcenters gibt es strenge Regeln, deren Einhaltung das Bundesamt für Sicherheit und Informationstechnik (BSI) [3] überwacht. In der folgenden Abbildung wird der Ablauf der Ausstellung einer Signaturkarte für die Signaturerstellung und die handelnden Personen dargestellt.

Das Zertifikat in Form des öffentlichen Schlüssels ermöglicht die Identifizierung des Unterzeichners, da einer Signatur eine Person zugeordnet werden kann. Um eine Datei mit einer qualifizierten elektronischen Signatur zu versehen, benötigt man eine von einem beim BSI zertifizierten und akkreditierten Trustcenter ausgestellte Signaturkarte. Auch die für den gesamten Ablauf notwendige Software, sowie auch das benutzte Kartenlesegerät müssen vom BSI zertifiziert werden.

Beim Vorgang der Signaturerstellung wird zunächst von der zu signierenden Datei ein Hashwert erzeugt. Dieser Hashwert identifiziert die zu signierende Datei im Sinne des Signaturgesetzes eindeutig, wenn ein vom BSI zur Signaturerstellung erlaubtes Hashverfahren eingesetzt wird. Für den eigentlichen Vorgang der Signierung wird dieser Hashwert an die Signaturkarte übertragen, die den privaten Schlüssel des Karteneigentümers enthält.

Der private Schlüssel verlässt niemals die Signaturkarte, um einer möglichen Kompromittierung der Sicherungseigenschaft vorzubeugen. Die eigentliche Unterschrift wird durch die mathematische Verknüpfung von Hashwert und privatem Schlüssel in der Signaturkarte erstellt und dann ausgegeben. Dieser Vorgang wird von der Signaturkarte aber nur nach erfolgreicher Authentifizierung des Inhabers durch Eingabe einer Persönlichen Identifikationsnummer (PIN) durchgeführt.

Diese Kombination von Hashwert und Unterschrift wird als qualifizierte elektronische Signatur bezeichnet, wenn sie mit einer von einem akkreditiertem Trustcenter herausgegebenen Signaturkarte erzeugt wurde. Eine durch eine qualifizierte elektronische Signatur geschützte Datei besteht meist aus der sig-

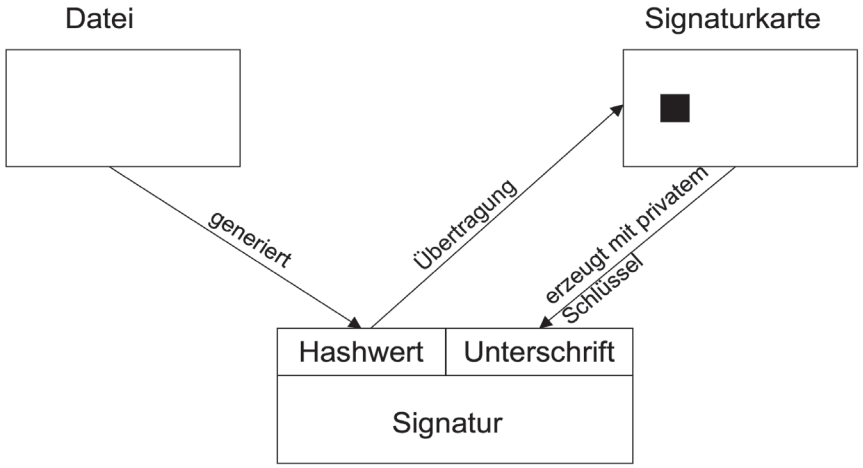

Abb. 2: Signieren einer Datei

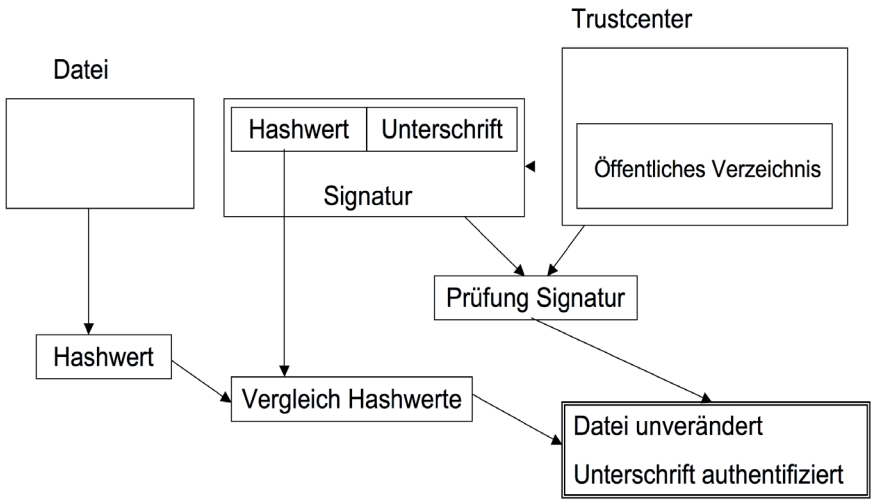

Abb. 3: Prüfen einer Signatur

nierten Datei selbst und einer weiteren Datei, die den Hashwert und die Unterschrift enthält.

Mit der Signatursoftware kann man auch ohne eine Signaturkarte die Signatur prüfen. Diese Prüfung erfolgt in zwei Stufen: Zunächst wird von der zu prüfenden Datei ein Hashwert mit dem gleichen Verfahren erzeugt, das für die Signatur verwendet wurde. Dieser Wert wird nun mit dem in der Signatur enthaltenen Wert verglichen. Stimmen beide überein, hat man den Nachweis, dass die zu prüfende Datei identisch mit der signierten ist und somit unverändert vorliegt.

Der zweite Teil der Prüfung besteht in der Prüfung der Unterschrift gegen das vorhandene Zertifikat, also dem öffentlichen Teil des Schlüsselpaares. Hier wird geprüft, von welchem Schlüsselpaar die Unterschrift erzeugt wurde bzw. welche Person diese Unterschrift geleistet hat. In dieser Kombination und unter Einbeziehung des Trustcenters lassen sich Integrität und Authentizität der Datei und qualifizierter Signatur rechtssicher beweisen. Für eine weitere Auseinandersetzung mit dem Thema sei das Buch „Grundlagen der elektronischen Signatur“ [4] empfohlen.

Anwendung auf dem Dokumentenserver

Der Bestand des Dokumenten- und Publikationsservers der Humboldt-Universität zu Berlin soll archiviert und dabei die Integrität der abgelegten Dokumente durch den Einsatz von Hashverfahren gesichert werden. Dazu wird für jede Datei auf dem Dokumentenserver ein Hashwert ermittelt, der mit dem auf dem Archiv- und Signaturserver gespeicherten Hashwert der entsprechenden Datei abgeglichen wird. Bei Übereinstimmung beider Hashwerte ist die Identität mit der archivierten Datei und somit deren Integrität gegeben. Durch einen automatisierten Vergleich der Hashwerte für alle auf dem Dokumentenserver vorhandenen Dateien kann die Integrität des gesamten Bestandes überprüft werden.

Die an den Dokumenten vorgenommenen Änderungen sollen erfasst und dokumentiert werden. Dies bedeutet, dass festgehalten wird, welcher Mitarbeiter aus welchem Grund eine Änderung durchgeführt hat. Zusätzlich wird ein Teil der Dokumente, die universitären Qualifikationsarbeiten wie Dissertationen und Habilitationsschriften, durch elektronische Signaturen und Zeitstempel rechtssicher abgelegt werden. Damit wird die Möglichkeit geschaffen, den Zeitpunkt der elektronischen Veröffentlichung einer Qualifikationsarbeit und deren Unversehrtheit auch nach vielen Jahren vor Gericht beweisen zu können.

Voraussetzung für eine elektronische Veröffentlichung einer Qualifikationsarbeit an der Humboldt-Universität zu Berlin ist die Annahme dieser Arbeit durch die Arbeitsgruppe Elektronisches Publizieren. Dazu wird geprüft, ob die abgegebene Arbeit die von der Arbeitsgruppe aufgestellten Bedingungen zur Veröffentlichung von Dokumenten auf dem Dokumentenserver erfüllt. Nach der erfolgreichen Prüfung der Publikation wird sie an die Universitätsbibliothek weitergeleitet, die daraufhin die Publikationsbescheinigung ausstellen kann. Gleichzeitig wird die Publikation in dem Publikationsformat PDF dem Bestand des Dokumentenservers der Humboldt-Universität zu Berlin hinzugefügt. Damit ist die Publikation über die Webseiten des Dokumentenservers im Internet frei zugänglich und gilt somit als veröffentlicht.

Dies ist daher der Zeitpunkt der elektronischen Veröffentlichung einer Publikation, der rechtssicher dokumentiert werden soll. Dazu wird zu diesem Zeitpunkt über die gesamte Publikation ein Zeitstempel erzeugt.

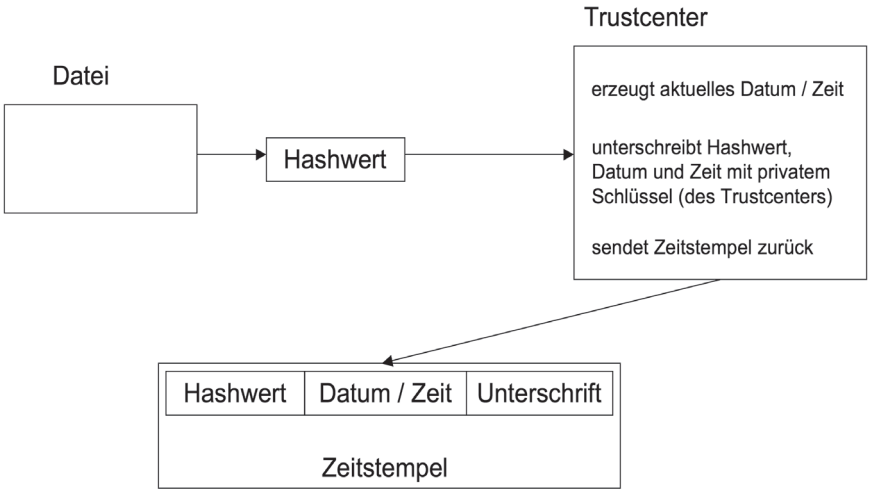

Abb. 4: Erzeugung eines Zeitstempels

Wie bei der Signierung von Dateien wird zunächst wieder ein Hashwert der Datei erzeugt, die einen Zeitstempel erhalten soll. Im Anschluss daran wird dieser Hashwert an ein Trustcenter geschickt. Das Trustcenter ermittelt die Zeit und das Datum bei Erhalt dieses Hashwertes. Dann unterschreibt das Trustcenter den Hashwert und die ermittelte Zeit und Datum, analog zur Erstellung einer Signatur, jedoch mit Signaturkarten des Trustcenters. Die drei Elemente Hashwert, Zeit bei Erhalt des Hashwertes und die Unterschrift des Trustcenters bilden zusammen den sogenannten Zeitstempel. Das Trustcenter bezeugt, dass der vorgelegte Hashwert zu der Zeit der Annahme existiert hat. Da der Hashwert eine bestimmte Datei identifiziert, beglaubigt das Trustcenter also indirekt, das eine bestimmte Datei zu einem bestimmten Zeitpunkt vorgelegen hat. Mit diesem Zeitstempel lässt sich dann rechtssicher beweisen, dass diese Publikation zu dem im Zeitstempel festgehaltenen Zeitpunkt in genau dieser Form existiert hat.

Weiter wird diese Art von Publikation bei jeder Änderung mit einer qualifizierten elektronischen Signatur versehen und somit festgehalten, welcher Mitarbeiter diese Änderungen vorgenommen hat. Alle Publikationen und zugehörigen Hashwerte, Zeitstempel und Signaturen werden auf einem gesonderten Archiv- und Signaturserver getrennt vom eigentlichen Dokumentenserver archiviert.

Dieser Server wird besonders gesichert und ist nicht über das Internet öffentlich zugänglich. Zugriff haben nur Mitarbeiter der Arbeitsgruppe von bestimmten Arbeitsplätzen aus. Der Archiv- und Signaturserver muss derart gesichert werden, denn die darauf gespeicherten Hashwerte, Zeitstempel und Signaturen bilden den Beweis für die Integrität und Authentizität aller auf dem Dokumentenserver der Humboldt-Universität zu Berlin angebotenen Publikationen.

Rechtssichere Archivierung

Bei der rechtssicheren Archivierung sollen Dokumente in elektronischer Form für einen längeren Zeitraum, in der Regel mindestens zehn Jahre, aufbewahrt und dabei die Gültigkeit ihrer elektronischen Signaturen erhalten werden.

Eine qualifizierte elektronische Signatur ist unbegrenzt gültig, wenn sie nach den rechtlichen Vorgaben erstellt wurde und das für die Signatur genutzte Zertifikat zum Zeitpunkt der Signaturerzeugung nicht gesperrt war. Nach längerer Zeit der Archivierung entstehen jedoch Probleme beim Versuch zu beweisen, dass ein Zertifikat bei der Erzeugung nicht gesperrt war und die damit erzeugte Signatur somit ungültig ist. Noch wichtiger ist der Beweis, dass die signierten Dokumente wirklich noch genau den ursprünglich signierten entsprechen oder ob sie verfälscht wurden.

In der Signaturverordnung ist daher ein Verfahren zur langfristigen Sicherung von signierten Dokumenten festgelegt. Dabei sind die mit einer qualifizierten elektronischen Signatur versehenen Dokumente „(...) vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.“[5] Dieses Verfahren wird als Neu- oder Übersignatur bezeichnet.

Das Konzept der Übersignatur ist somit die Grundlage für Projekte im Bereich der rechtssicheren Archivierung. Das Pilotprojekt in Deutschland für den Einsatz von elektronischen Signaturen in der Archivierung von Dokumenten ist das Projekt Archisafe [6] der Physikalisch-Technischen Bundesanstalt (PTB) [7]. Der Fokus des Projektes lag vor allem darauf, die Übersignatur für eine große Anzahl von Dokumenten effizient durchführen zu können.

Für die Archivierung der Dokumente und Signaturen wurde jedoch ein kommerzielles Produkt eingesetzt, daher ist eine Nachnutzung der Ergebnisse dieses Projektes nur bedingt möglich. Auch sind die Dokumente dabei ausschließlich PDF/A-Dokumente mit integrierter Signatur. Dabei soll die langfristige Lesbarkeit der Dokumente allein durch Verwendung des PDF/A-Dokumentformats erreicht werden.

Im Gegensatz dazu soll an der Humboldt-Universität zu Berlin die langfristige Lesbarkeit durch die kontinuierliche Migration der Dokumente sichergestellt werden. Für die rechtssichere Archivierung von Qualifikationsarbeiten der Humboldt-Universität zu Berlin wurde daher ein eigenes Konzept entwickelt [8].

Das ursprüngliche Konzept für die rechtssichere Archivierung wurde vom Autor weiterentwickelt und für eine genaue Beschreibung wird auf „Einsatz elektronischer Signaturen auf dem Dokumentenserver der Humboldt-Universität zu Berlin“ [9] verwiesen.

Literatur

[1] *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*. 2001

[2] *T7 e.V.– Arbeitsgemeinschaft der Trustcenterbetreiber.* URL: http://www.t7ev.org/

[3] *Bundesamt für Sicherheit in der Informationstechnik*. URL: http://www.bsi.de/

[4] Hühnlein & Korte: *Grundlagen der elektronischen Signatur.* 2006

[5] Bundesministerium für Justiz: *Verordnung zur elektronischen Signatur.* 2001 d, S. 3079 §17.

[6] *Archisafe*. URL: http://www.archisafe.de

[7] *Physikalisch-Technische Bundesanstalt*. URL: http:// www.ptb.de (letzter Zugriff am 04.12.2008)

[8] Ohst: *Einsatz elektronischer Signaturen und Zeitstempel für die Sicherung digitaler Dokumente*. 2004

[9] Fromm: *Einsatz elektronischer Signaturen auf dem Dokumentenserver der Humboldt-Universität zu Berlin*. 2008