Elektronische Geschäftsprozesse mit fortgeschrittener Signatur

Dr. Ulrich Pordesch

Einleitung

Die hochdynamische Entwicklung der Informationstechnik wirft viele Rechtsfragen auf, deren Klärung die interdisziplinäre Zusammenarbeit[1] zwischen Technikern und Juristen erfordert. Der von Dr. Dirk-Meints Polter betreute Vorstandsbereich Personal und Recht der Fraunhofer-Gesellschaft und seine Mitarbeiter stellen sich dieser Entwicklung. Ein Beispiel hierfür ist die Zusammenarbeit mit dem Kompetenzzentrum PKI und dem IT-Sicherheitskoordinator bei elektronischen Geschäftsprozessen und Signaturen, die der folgende Beitrag behandelt. Hierbei geht esbeispielsweise um die Frage, inwieweit die zeit- und arbeitsaufwändigen internen papiergebundenen Geschäftsvorgänge durch den Einsatz fortgeschrittener elektronischer Signaturen vereinfacht werden können und welche rechtlichen Vorgaben dabei zu beachten sind.

Interne Geschäftsprozesse

Leistungen von Unternehmen und Verwaltungen werden in unserer fortgeschrittenen Industrie- und Informationsgesellschaft stark arbeitsteilig erbracht. Viele Stellen sind daran beteiligt, beauftragen Tätigkeiten, planen sie, führen sie durch, nehmen sie ab und überwachen sie. Dabei geht die Tendenz stets in Richtung stärkerer Formalisierung der damit verbundenen Vorgänge, was sich in einer „Flut von Formularen“ auswirkt, die von mehreren Beteiligten auszufüllen und zu unterschrieben sind. Dies gilt besonders für Organisationen wie die Fraunhofer-Gesellschaft, die als mit öffentlichen Mitteln gemäß Art. 91b GG geförderte Forschungseinrichtung zahlreichen Nachweispflichten unterliegt und aufgrund ihrer Größe und räumlichen Verteilung stark arbeitteilig organisiert ist. Beispiele für formularorientierte interne Geschäftsvorgänge aus der Fraunhofer-Gesellschaft sind:

- Reiseanträge, Urlaubsanträge, Beschaffungsanträge
- Zeitaufschreibung
- Interne Leistungsverrechnung
- Kenntnisnahmeerklärungen
- Sitzungsprotokolle

1 Der Verfasser dankt Herrn Dr. Markus Zirkel, Abteilung Recht der Fraunhofer-Gesellschaft, für die wertvollen Hinweise.

Dokumentation und Dokumentenaustausch erfolgen heute häufig noch per Papier. Zwar werden Formulare zunehmend elektronisch bereitgestellt und Dokumente am Rechner bearbeitet. Am Ende werden sie meist jedoch ausgedruckt, händisch unterschrieben, per Post oder Hauspost versendet, teilweise in administrative Datenbanksysteme neu eingegeben und schließlich als Papieroriginalbeleg archiviert oder eingescannt. Wegen der Medienbrüche sind diese Verfahren mit langen Wegezeiten behaftet, arbeitsaufwändig und fehleranfällig. Eine papierlose vollelektronische Realisierung wäre daher erstrebenswert. Dieser stand jedoch bisher entgegen, dass Daten spurenlos verfälschbar und die darauf basierenden Verfahren daher nicht hinreichend sicher sind. Außerdem wurde das Fehlen einer (Hand-)Unterschrift oder deren Kurzform als Paraphe als rechtlich bedenklich angesehen.

Die elektronische Signatur

Für beide Probleme, nämlich die Erfüllung des Unterschriftserfordernisses und die Sicherung vor spurenlosen Veränderungen bietet die elektronische Signatur eine Lösung. Als elektronische Signatur werden Daten bezeichnet, die den Nachweis der Integrität (Unversehrtheit) eines elektronischen Dokumentes ermöglichen und zudem zeigen, wer sie erzeugt hat. Elektronische Signaturen werden programmmgesteuert aus den Dokumentdaten und einem persönlichen kryptographischen Schlüssel erzeugt. Ihre Überprüfung ist mit einem zum jeweiligen Signaturschlüssel gehörenden öffentlichen Signaturprüfschlüssel möglich. Anhand der durch ein Zertifikat bestätigten Zuordnung des Signaturprüfschlüssels zu einer bestimmten Person, lässt sich die Urheberschaft der Signatur erkennen und nachweisen.

Werden Dokumentdaten elektronisch signiert, lässt sich prinzipiell deren unbemerkte Verfälschung erkennen bzw. die Unverfälschtheit nachweisen und zugleich ein Äquivalent zur herkömmlichen Unterschrift oder Paraphe erhalten. Inwieweit diese Ziele tatsächlich erreicht werden, hängt allerdings insbesondere von der Sicherheit der zur Signaturerzeugung verwendeten Algorithmen, der Geheimhaltung der persönlichen Schlüssel und der ordnungsgemäßen Zuordnung des Signaturprüfschlüssels zu seinem Inhaber. Um hier Rechtssicherheit zu schaffen hat der Gesetzgeber im Signaturgesetz Rahmenbedingungen für Signaturen geschaffen und dabei vier Sicherheitsniveaus für Signaturen definiert:

– Einfache Signaturen: Für sie gelten keine besondere Sicherheitsanforderungen.
– Fortgeschrittene Signaturen: Bei ihnen muss der Signaturschlüssel „unter alleiniger Kontrolle des Signaturschlüsselinhabers" stehen und damit besonders geschützt werden.
– Qualifizierte Signaturen: Für diese müssen Schlüssel verwendet werden, die von Zertifizierungsdiensteanbietern erzeugt und verwaltet werden, die hohe Sicherheitsanforderungen erfüllen müssen. Außerdem sollen die Anwender sicherheitszertifizierte Komponenten für die Signaturschlüsselanwendung einsetzen.
– „Akkreditierte" Signaturen: Dies ist ein in der Literatur (nicht im Gesetz) verwendeter Begriff für qualifizierte Signaturen auf der Basis von Zertifikaten akkreditierter Zertifizierungsdiensteanbieter, die ihren Betrieb vorab und regelmäßig streng prüfen lassen müssen.

Rechtsfolgen sind bisher nur für mindestens qualifizierte Signaturen gesetzlich festgelegt worden. Gemäß § 126a BGB gilt, dass Dokumente mit qualifizierter Signatur als „Elektronische Form" Papier und Unterschrift, d.h. die herkömmliche Schriftform, ersetzen können, sofern das Gesetz nicht ausdrücklich etwas anderes regelt. Zudem legt § 371a ZPO fest, dass aus dem nachgewiesenen Vorliegen einer gültigen qualifizierten Signatur auf die Echtheit einer Erklärung geschlossen werden darf.

Probleme der qualifizierten Signatur

Auf den ersten Blick legt die Gesetzeslage es nahe, auch im innerbetrieblichen Formularwesen durchgängig qualifizierte Signaturen einzusetzen. Dem stehen jedoch eine Reihe von Gründen entgegen:

– Kosten: Die nötigen zertifizierten technischen Komponenten (Signaturkarten, Leser, Anwendungskomponenten) und Zertifizierungsdienste externer Diensteanbieteranbieter sind teuer. So ist es in der Fraunhofer-Gesellschaft kaum zu rechtfertigen, jeden auch nur kurzfristig

– Verfügbarkeit: Für viele Anwendungsformate und Systemplattformen gibt es noch keine zertifizierten Anwendungskomponenten. In der Fraunhofer-Gesellschaft kommen jedoch viele Formate und nahezu jede Systemplattform in jeder Version vor, die man nicht generell vereinheitlichen kann.

– Sicherheit: Das für qualifizierte Signaturen nötige Sicherheitsniveau der Umgebung, in der Anwendungskomponenten betrieben werden, ist in einem relativ offenen Forschungsumfeld flächendeckend kaum sicherzustellen.

Neben diesen technischen und ökonomischen Gründen gibt es auch rechtliche Bedenken:

– Fraglicher Anschein: Der durch § 371a Abs. 1 S. 2 ZPO eingeführte Anschein der Echtheit eines in elektronischer Form vorliegenden Dokuments, das in ihrer Beweiskraft einer Urkunde gleich steht[2], ist sachlich nicht gerechtfertigt. Hier hat der Gesetzgeber übersehen, dass auch die qualifizierte Signatur zunächst nur die Unverfälschheit einer Folge von Bits beweist, nicht aber, wie diese Bitfolge korrekt darzustellen ist. Es ist unklar, wie Gerichte urteilen werden, wenn ihnen die ersten Dokumente präsentiert werden, die etwa aufgrund aktiver Inhalte abhängig von Umgebungsparametern wie der Browsereinstellung unterschiedliche Erklärungsinhalte aufweisen.

– Fehlende Kontrolle: Gerade im innerbetrieblichen Umfeld kommt als Problem hinzu, dass der Rechner nicht vom signierenden Arbeitnehmer, sondern von Administratoren gewartet werden. Für die Sicherheit ist professionelle Wartung zwar von Vorteil, der Mitarbeiter - und damit der auf elektronischem Weg sich Erklärende - hat aber keine Kontrolle darüber. Der hypothetische Fall, dass ein Mitarbeiter auf seinem vom Arbeitgeber manipulierten System die eigene Kündigung signiert und dann beweisen soll, dass sein System manipuliert war, um einen Anschein zu erschüttern, bringt dieses Dilemma zugespitzt zum Ausdruck.

– Akzeptanz: Die Befürchtung vor einer Umkehr der Beweislast zu Lasten von Arbeitnehmern, sowie die bei qualifizierten Signaturen von Arbeitnehmern einzuhaltenden strengen Sicherheitsvorkehrungen sind auch hinderlich für deren Akzeptanz im betrieblichen Mitbestimmungsprozess.

2 Thomas/Putzo, Zivilprozessordung, 27. Aufl., § 371a ZPO Rn. 1

– Verfügungsgewalt: Im innerbetrieblichen Umfeld stellt sich die Frage, wer Eigentümer der Karte ist (gesetzlich ist dies der Schlüsselinhaber) und wer über deren Verwendung und Sperrung entscheiden darf.

Diese und weitere Probleme und Rechtsfragen sind nicht unlösbar. So ist es möglich, dass in den nächsten Jahren Karten für die Erzeugung qualifizierter Signaturen über Ausweiskarten wie Personalausweise, Gesundheits- oder Bankkarten verbreitet werden, die man nach der Klärung damit verbundener Rechtsfragen auch betrieblich einsetzen könnte. Zertifizierte Signaturanwendungsprodukte werden allmählich auch für immer mehr Plattformen und Anwendungen bereitgestellt und die Plattformen, auf denen sie betrieben werden, werden sicherer. Schließlich wird, wenn schon nicht der Gesetzgeber, so doch die Rechtsprechung für eine allmähliche Klärung der rechtlichen und beweisrechtlichen Fragen sorgen.

Dies alles wird jedoch voraussichtlich noch etliche Jahre dauern. Bis dahin fehlt dem breiten Einsatz qualifizierter Signaturen innerbetrieblich die Grundlage. Man setzt sie zunächst schrittweise an bestimmten Stellen im Unternehmen (etwa Einkauf, Poststelle) ein, in denen Schriftform bzw. elektronische Form vorgeschrieben ist - an einzelnen Arbeitsplätzen, die man gut absichern kann und für die man gesonderte Regelungen entwickeln kann.

Zwischenschritt: Fortgeschrittene Signatur

Auf den ersten Blick ist nicht ersichtlich, wieso die fortgeschrittene Signatur diese Probleme lösen soll, weist sie definitionsgemäß ein etwas niedrigeres Sicherheitsniveau auf. Faktisch haben fortgeschrittene Signaturen jedoch derzeit durchaus noch Vorteile:

– Für fortgeschrittene Signaturen sind Sicherheitsanforderungen nur recht allgemein beschrieben, so dass bei der Auswahl von technischen Komponenten große Freiräume verbleiben. Die erforderlichen Zertifizierungsdienste können prinzipiell auch innerbetrieblich erbracht und mit anderen ohnedies erforderlichen Sicherheitsdiensten (etwa zur Erzeugung von Verschlüsselungsschlüsseln oder Mitarbeiterausweisen) kombiniert werden.

– Das Sicherheitsniveau kann trotzdem sehr hoch und deutlich höher sein, als bei Handunterschriften und Paraphen.

– Für fortgeschrittene Signaturen gibt es keine Anscheinsbeweisregel, die Gerichte binden und faktisch die Beweislast umkehren. Sie unterliegen wie unsignierte Dokumente und die meisten andere Beweismittel der freien richterlichen Beweiswürdigung. Ihr Beweiswert ist deutlich höher als der unsignierter Dokumente und in vielerlei Hinsicht auch der von Handunterschriften. Im Rechtsstreit kann jedoch jede Seite ihre Argumente vorbringen und diese sind dann ohne Einschränkungen abzuwägen.

– Die Kosten sind niedriger und die Akzeptanz unter den Mitarbeitern ist mutmaßlich höher.

Die fortgeschrittene Signatur ist also so gesehen geeignet, einen bedeutenden Schritt zur effektiveren und transparenteren Realisierung vollelektronischer interner Geschäftsprozesse zu ermöglichen. Doch ist ihr Einsatz rechtlich auch zulässig?

Zulässigkeit und Akzeptanz

Grundsätzlich gilt in Verwaltungsverfahren das Prinzip der Nichtförmlichkeit. Solange die elektronische Form oder die Schriftform mit Unterschrift nicht vorgeschrieben sind, sind fortgeschrittene Signaturen gesetzlich nicht ausgeschlossen - es könnte theoretisch sogar ganz auf Signaturen verzichtet werden. Voraussetzung ist, dass die allgemeinen Sicherungsanforderungen erfüllt werden können, wie sie sich aus der Aktenführungspflicht der Verwaltung, sowie (bei buchungsrelevanten Unterlagen) aus den Grundsätzen ordnungsgemäßer DV-gestützter Buchbührungssysteme (GoBS) ergeben.[3]

Für viele interne Formularvorgänge wie die Leistungsverrechnung gibt es keine Vorgaben einer bestimmten Form. Allgemeine Pflichten nachvollziehbaren Verwaltungshandelns, die sich für die Fraunhofer-Gesellschaft unter anderem aus der Pflicht zur wirtschaftlichen Mittelverwendung in Zuwendungsbescheiden ergeben, sprechen jedoch ebenso wie Eigeninteressen für ein sichere und revisionsgeeignete Ausgestaltung des Verfahrens. Die fortgeschrittene Signatur ist ein geeignetes Mittel hierfür.

3 Siehe Bundesministerium der Finanzen, Schreiben vom 7.11.1995, Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), BStBl 1995-1-0738.

Etwas anders sieht es beispielsweise für die Zeiterfassung aus, d.h. die Erfassung der tatsächlichen Arbeitszeit der einzelnen Mitarbeiter. Hier hat insbesondere auch der Zuwendungsgeber das Recht, das Medium für den Nachweis der abrechnungsfähigen Mitarbeiterstunden vorzugeben. Bisher enthalten etwa die Nebenbestimmungen des Bundesministeriums für Bildung und Forschung (kurz: BMBF) zwar bestimmte Vordrucke, die ausgedruckt und ausgefüllt werden können. Zuwendungsgeber können jedoch auch andere Verfahren akzeptieren. Sie tun dies auch bereits, um die Zeiterfassung für viele Einzelprojekte zu vereinfachen und dadurch den bürokratischen Aufwand zu begrenzen und eine wirtschaftliche Mittelverwenung zu ermöglichen. Vollelektronische Verfahren haben auch für Revisoren klare Vorteile, da sie wesentlich schnellere und umfassendere Prüfungen ermöglichen - inhaltlich durch Übernahme von Inhalten aus den Dokumenten (per Cut and Paste) und formal, weil die Prüfung von Signaturen im Gegensatz zu der von Paraphen und Unterschriften ohne Sachverständigengutachten möglich ist. Voraussetzung der Akzeptanz vollelektronischer Verfahren ist hier auch wieder die revisionseignete und sichere Ausgestaltung des Verfahrens, die gegebenenfalls durch eine entsprechende Testierung von einem Dritten nachgewiesen werden kann.

Sicherheit und Revisionseignung

Wie gezeigt kommt es auf die Sicherheit und Revisionsfähigkeit und eine eventuelle diesbezügliche Testierung der Verfahren an. Dies betrifft nicht nur die eingesetzten Signaturverfahren, sondern auch deren Integration in Anwendungsprogrammme und die Anwendungssicherheit insgesamt.

Hinsichtlich der Signaturen reicht der Verweis darauf, dass diese fortgeschritten seien, sicher nicht aus. Die Verfahren der Schlüsselerzeugung, der verwendeten Algorithmen, der Zuordnung von Schlüsseln zu Personen in Zertifikaten, der Sperrung von Schlüsseln bzw. Zertifikaten, der Identifikation von Nutzern bei der Schlüsselausgabe usw. sind überzeugend sicher auszugestalten und durch eine Dokumentation für Dritte nachprüfbar zu machen. Die Erzeugung von Schlüsseln durch geschulte Mitarbeiter auf einem PC mit selbst installierter freier Software und deren Versendung als Datei genügt solchen Anforderungen sicher nicht. Ein gut dokumentierter rechenzentrumsähnlicher Betrieb mit zugangsgesicherten Bereichen, Sicherheitskonzepten und Dokumentation, der der regelmäßigen Auditierung unterliegt, ist vielmehr erforderlich. Schlüssel sollten zudem auf Hardwaretokens (spe-

ziellen USB-Sticks oder Smartcards) sicher gespeichert werden, weil sie als Dateien über Benutzerprofile in betrieblichen Netzwerken zirkulieren und kaum unter „alleiniger Kontrolle des Schlüsselinhabers" zu halten sind.

Neben der Sicherheit der Signaturen kommt es auch auf die Sicherheit der Anwendungsumgebung an. So ist durch eventuell wiederum auf Kryptoverfahren basierende Benutzerauthentisierung und gezielte Einschränkungen bei der Vergabe von Zugriffsrechten sicherzustellen, dass Fehler- und Manipulationsmöglichkeiten - etwa unbefugtes oder falsches Ausfüllen von Formularfeldern - eingeschränkt werden. Gelegentliche Querprüfungen verschiedener Datenquellen, etwa der von Formularen und von Datenbanken können Inkonsistenzen aufzeigen und zur Sicherheit der Verfahren beitragen. Zu nennen ist auch die zeitnahe Ablage in sicheren Dokumentenmanagementsystemen, wo sie nicht mehr verändert und gelöscht werden können.

Fazit und Ausblick

Vollelektronische interne Geschäftsprozesse haben gegenüber herkömmlichen papiergebundenen Verfahren zahlreiche Vorteile für alle Beteiligten. Sie sparen Kosten, sind deutlich weniger fehleranfällig, sicherer, transparenter für die Mitarbeiter und wesentlich besser kontrollierbar. Verfahren auf der Basis fortgeschrittener Signaturen können ausreichend sicher und revisionsgeeignet ausgestaltet werden, um die Anforderungen erfüllen zu können und auf Akzeptanz zu stoßen. Sie sind ein notwendiger und sinnvoller Zwischenschritt, bis die qualifizierte Signatur in einigen Jahren reif auch für den breiten unternehmensinternen Einsatz sein wird.