

Beweiseignung fortgeschrittener elektronischer Signaturen

(BefeS)

Das von der Deutschen Forschungsgemeinschaft (DFG) geförderte Projekt verfolgte das Ziel, die technische und die organisatorische Sicherheit der in der Praxis verwendeten Verfahren zur Erzeugung fortgeschrittener elektronischer Signaturen auf der Grundlage der abstrakten gesetzlichen Vorgaben zu bewerten.

Fortgeschrittene Signaturverfahren sind im Vergleich zu qualifizierten Signaturverfahren, die sich in der Praxis bisher nur in einzelnen Anwendungsbereichen durchgesetzt haben, weit verbreitet. In der Forschung wurden die fortgeschrittenen Signaturverfahren, insbesondere deren Beweiseignung im Rechtsverkehr und vor Gericht bisher gegenüber den qualifizierten Signaturverfahren vernachlässigt.

Anhand einer umfassenden Risikoanalyse wurde im Rahmen des Forschungsprojektes „BefeS“ untersucht, durch welche Komponenten genau sich qualifizierte und fortgeschrittene elektronische Signaturen unterscheiden. Darüber hinaus wurde die Beweissicherheit fortgeschrittener elektronischer Signaturen umfassend und für die unterschiedlichen Prozessordnungen beurteilt. Ferner wurden Prüfkriterien für die Bestimmung des Beweiswerts fortgeschrittener elektronischer Signaturen entwickelt, die den

Richtern ihre Bewertung in der freien Beweiswürdigung erleichtern sollen. Anschließend wurde die Feststellung getroffen, ob – gegebenenfalls einzelne – Verfahren zur Erzeugung fortgeschrittener elektronischer eine ausreichende Sicherheit bieten, um Rechtsfolgen an ihre Verwendung zu knüpfen, die gegebenenfalls eine entsprechende Ergänzung der Beweisvorschriften ermöglichen.

Die wichtigsten Ergebnisse des Forschungsprojekts sind:

Fortgeschrittene elektronische Signaturen gewährleisten zwar ein höheres Sicherheitsniveau als einfache elektronische Signaturen, erfüllen jedoch nicht die Anforderungen, die an qualifizierte elektronische Signaturen gestellt werden. Mit fortgeschrittenen elektronischen Signaturen wird lediglich ein mittleres, d.h. ein Sicherheitsniveau zwischen einfachen und qualifizierten elektronischen Signaturen, angestrebt. Sie sollen eine kostengünstige Möglichkeit der elektronischen Kommunikation – vor allem beim Abschluss von Onlinegeschäften – bieten.

Die Anwendungsbereiche der untersuchten Signaturverfahren, die nicht als qualifizierte elektronische Signaturen bei der Bundesnetzagentur angezeigt sind, erstrecken sich vom privaten E-Mail-

Verkehr, über elektronische Steuerklärungen und Online-Banking bis hin zu Verwaltungsverfahren und die Ausstellung elektronischer Rechnungen.

Die Analyse der Signaturverfahren unter dem Niveau einer qualifizierten elektronischen Signatur hat ergeben, dass der Gestaltungsspielraum und somit das Sicherheitsniveau sehr unterschiedlich sind. Dieses reicht von niedrig bis relativ hoch. Eine pauschale Aussage über die Sicherheit von Signaturverfahren unterhalb des Niveaus qualifizierter elektronischer Signaturen konnte demzufolge nicht getroffen werden. Jedes einzelne Signaturverfahren muss für sich allein betrachtet und bewertet werden.

Die Analyse der Manipulationsrisiken bei den untersuchten Signaturverfahren hat ergeben, dass diese Unterschiede sowohl bei der mathematischen als auch technischen und organisatorische Sicherheit aufweisen können.

Der Einsatz unsicherer Hash- und Signaturalgorithmen führt dazu, dass eine untrennbare Verknüpfung vom Dokument und Signatur nicht vorliegt. Im Nachhinein kann nicht mit Sicherheit bewiesen werden, auf welches (unveränderte) Dokument sich die elektronische Signatur bezieht.

Die Identifizierung der Manipulationsrisiken bei der technischen Sicherheit hat ergeben, dass diese zum einen aus der Verwendung unsicherer Trägermedien und aus der Verwendung unsicherer Sig-

naturanwendungskomponenten resultieren können.

Die Untersuchung der organisatorischen Sicherheit hat gezeigt, dass Manipulationsrisiken einerseits durch eine mangelhafte Identifizierung entstehen können, indem eine falsche Person im Zertifikat genannt oder das Zertifikat ohne das Wissen der angegebenen Person beantragt wird. Andererseits kann auch das Fehlen eines Verzeichnis- und/oder Sperrdienstes das Entstehen von Manipulationsrisiken begünstigen.

Die Analyse der beweisrechtlichen Bewertung in freier Beweiswürdigung hat ergeben, dass die Beweisnot des Signaturempfängers im Zivilprozess am größten ist. Hinsichtlich der Durchsetzung der Vorlagepflicht durch den Signaturschlüssel-Inhaber oder den Zertifizierungsdiensteanbieter ist der Empfänger des fortgeschritten signierten Dokuments im Zivilprozess am schlechtesten gestellt und genießt weniger Sicherheit bei der Beweisführung im Vergleich zu anderen untersuchten Gerichtsprozessordnungen (Verwaltungs-, Arbeits-, Sozial- und Finanzgerichtsprozess).

Darüber hinaus konnte festgestellt werden, dass einem Sachverständiger eine entscheidende Bedeutung bei der Beurteilung der mathematischen, technischen und organisatorischen Sicherheit des eingesetzten fortgeschrittenen Signaturverfahrens zu kommen wird. Seine Tätigkeit wird auch in aller Regel nicht auf die Mitteilung von Erfahrungssätzen be-

schränkt sein. Vielmehr wird er diese auf den konkreten Fall anwenden, Tatsachen feststellen und Schlüsse ziehen müssen.

Basierend auf den Ergebnissen zu den Manipulationsrisiken wurden Beweissituationen durchgeprüft, in denen die Echtheit einer fortgeschrittenen elektronischen Signatur bestritten wurde (Beweiseinreden). Dabei wurde eine Einteilung der Beweiseinreden auf drei Sicherheitsebenen (niedrige, mittlere und hohe) vorgenommen. Die Bewertung hat gezeigt, dass Dokumente, die mittels Signaturverfahren auf niedrigster Sicherheitsebene (lediglich Erfüllung der Mindestanforderungen nach § 2 Nr. 2 SigG) signiert wurden, die am wenigsten verlässliche Beweissicherheit bieten. Je weniger der Signaturempfänger über objektiv geeignete Beweismittel verfügen und je weniger er sie erkennen und benennen kann, desto geringer sind seine Handlungsmöglichkeiten bei der Beweisführung im Gerichtsprozess und desto größer ist sein Risiko, den Anspruch nicht durchsetzen zu können.

Aus den Erkenntnissen zu den Beweiseinreden wurde als Ergebnis dieses Arbeitspakets eine systematische Übersicht für Sachverständige und Richter in Form einer Matrix und eines erläuternden Textes erarbeitet. Darüber hinaus wurden Beweisdefizite und Empfehlungen, sie zu vermindern oder zu verhindern, ausgearbeitet. Vorschläge zur Verminderung oder sogar Vermeidung von Defiziten in

Beweisverfahren wie z.B. die Führung der Dokumentation oder die Verwendung von Chipkarten als Trägermedium konnten zwar formuliert werden. Jedoch musste auch festgestellt werden, dass die Beweismöglichkeiten, wie qualifizierte elektronische Signaturen sie bieten, für fortgeschrittene elektronische Signaturen nicht vollständig erreicht werden können.

Im Hinblick auf mögliche rechtspolitische Fortentwicklungen des geltenden Rechts wurde unter anderem die Möglichkeit der Einführung eines gesetzlichen Anscheinsbeweises für fortgeschrittene elektronische Signaturen wie in § 371 a und § 371 b ZPO für fortgeschrittene elektronische Signaturen skeptisch gesehen. Auch nach Ende des Forschungsprojekts gibt es keine einschlägige Rechtsprechung zum Thema „Beweiswert fortgeschritten signierter Dokumente“. Auf eine ausreichende Erfahrung mit fortgeschrittenen elektronischen Signaturen kann sich der gesetzliche Anschein daher nicht stützen.

Auch bestehen keine rechtlichen Anforderungen, die eine ausreichend hohe Manipulationssicherheit einfordern, und keine Verwaltungsverfahren, um deren Erfüllung sicherzustellen. Für den Gesetzgeber gibt es daher keinen sachlichen Grund, an den er die Anordnung einer Beweisregel knüpfen könnte. Als möglicher Grund bliebe allein die Förderung einer bestimmten Technik durch den Umweg über eine Beweisregel, von

der erhofft wird, dass sie zur Verbreitung dieser Technik beiträgt, wobei von einer solchen Lösung ist aus grundsätzlichen Überlegungen der gesetzlichen Techniksteuerung abzuraten.

Die Empfehlung an den Gesetzgeber lautet daher, die Maßnahmen zur Stärkung des faktischen Beweiswerts fortgeschrittener elektronischer Signaturen abzuwarten und die Erfahrungen mit diesen auszuwerten. Sollten sie zu befriedigenden Ergebnissen führen, sind rechtspolitische Änderungen nicht erforderlich.

Nachwuchsförderung:

Abschlussstipendium zur Fertigstellung von Promotionen an der Universität Kassel im Anschluss an das Forschungsprojekt

Stipendiatin: Olga Grigorjew / Förderzeitraum: April bis September 2013

Im Zusammenhang mit dem Forschungsprojekt entstanden folgende Veröffentlichungen, die durch die Befassung mit fortgeschrittenen elektronischen Signaturen in dem Projekt mehr oder weniger stark beeinflusst wurden:

Grigorjew, O.: Dissertation: „Die Beweiseignung fortgeschrittener elektronischer Signaturen“. Die erste Fassung liegt bereits vor; im Erscheinen.

Roßnagel, A.: Kommentierung des SigG und der SigV, des § 3a und 37 VwVfG und des § 371a ZPO in: Roßnagel, A. (Hrsg.): Beck'scher Kommentar zum

Recht der Telemediendienste, Kommentar zum TMG, SigG, SigV, JMStV, BGB (Auszüge), VwVfG (Auszüge), ZPO (Auszüge), München 2013.

Roßnagel, A., Auf dem Weg zur elektronischen Verwaltung – das E-Government-Gesetz, NJW 2013, S. 2710-2716.

Grigorjew, O. / Johannes, P.C. / Roßnagel, A.: Der fortgeschritten signierte Verwaltungsakt; im Erscheinen.