Focke Höhne, Henrich C. Pöhls, Kai Samelin

Rechtsfolgen editierbarer Signaturen

Editierbare Signaturen erlauben – in begrenzten Bereichen – nachträgliche Modifikationen an einem signierten Dokument ohne Kenntnis des geheimen Signaturschlüssels des Ausstellers.[1] Der Beitrag beleuchtet die Rechtsfolgen editierbarer Signaturen und beschreibt ihren Einsatz am Beispiel von Lebensmittelwarenketten. Im Unterschied zu konventionellen Signaturen werden befugte Änderungen rechtlich dem Aussteller zugerechnet. Anwendungsbeispiele sind Schwärzungen[2] zum Schutz von Geschäftsgeheimnissen oder personenbezogenen Daten, sowie Inhaltsänderungen zu Korrekturzwecken.

1 Einleitung

In der Praxis werden konventionelle digitale Signaturen eingesetzt, um die Integrität und Authentizität von Daten zu schützen. Ein Beispiel für ein Signaturverfahren im technischen Sinne ist der RSA-Algorithmus [1]. In ihrem einführenden Beitrag „Redigierbare Signaturen", beschreiben Slamanig und Rass die technischen Grundlagen editierbarer Signaturen. Offengelassen wurde die Frage, welche Rechtsfolgen die Benutzung editierbarer Signaturen haben [2]. Dieser Beitrag geht der Frage nach, ob auch editierbare Signaturen als qualifizierte elektronische Signaturen gewertet werden können oder ob, aus anderen Gründen, ihr Beweiswert ähnlich hoch ist. Im Folgenden werden die rechtlichen Anforderungen an die technische Umsetzung erstmals untersucht. Insbesondere wird geklärt welcher Beweiswert editierbaren Signaturen zukommt.[3]

Zur sprachlichen Abgrenzung bezeichnen wir die technischen Umsetzungen als digitale Signaturen. Im Recht werden technische und *organisatorische* Anforderungen beschrieben, welche eine digitale Signatur besitzen muss, um als qualifizierte elektronische Signatur zu gelten.[4] Technisch ist es gängige Praxis, mit Hilfe asymmetrischer Kryptographie eine digitale Signatur eines digitalen Dokuments zu erzeugen, welche nur mit einem privaten Signaturschlüssel erzeugt und mittels des dazugehörigen öffentlichen Schlüssels geprüft werden kann [1]. Die Signatur wird nur dann als valide eingestuft, wenn das digitale Dokument nicht verändert wurde.[5] Nur in diesem Fall wird die Signatur akzeptiert. Damit ist das Prüfergebnis der Signaturvalidierung positiv.

2 Fragestellungen

2.1 Was sind die rechtlichen Anforderungen und der Beweiswert von qualifizierten Signaturen?

Das Signaturrecht beschreibt die Anforderungen an die technische Ausgestaltung einer qualifizierten elektronischen Signatur. Insbesondere fordert das Recht, dass fortgeschrittene und qualifizierte elektronische Signaturen Daten vor unbemerkten und unbefugten nachträglichen Änderungen zu schützen sind. Eine gül-

1 „Aussteller" ist der in § 126a BGB genutzte Begriff. Dieser korreliert mit „Signaturschlüssel-Inhaber" in § 17 SigG; technisch im Englischen „Signer" genannt.

2 In § 7 Abs. 2 Satz 2 IFG „Unkenntlichmachung" genannt.

3 Zu digitalen bzw. elektronischen Signaturen in der Praxis und den Rechtsfolgen siehe insbesondere die Schwerpunkthefte DuD 9/1999, 2/2000, 2/2001, 2/2002, 2/2003 und 11/2009.

4 Während das deutsche Signaturrecht qualifiziert elektronische Signaturen definiert, wird dieses Konzept in der EU-Signaturrichtlinie als fortgeschrittene Signatur basierend auf einem qualifizierten Zertifikat bezeichnet.

5 Siehe auch Bourseau/Fox/Thiel, Vorzüge und Grenzen des RSA-Verfahrens, DuD 2/2002, S. 84-89.

Focke Höhne

Ass. jur. ist Akad. Rat auf Zeit am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht der Universität Passau.

E-Mail: focke.hoehne@uni-passau.de

Henrich C. Pöhls

Dipl.-Inf., M.Sc. Information Security ist wissenschaftlicher Mitarbeiter am Lehrstuhl für IT-Sicherheit der Universität Passau.

E-Mail: hp@sec.uni-passau.de

Kai Samelin

Dipl.-Inf. (FH), M.Sc. ist wissenschaftlicher Mitarbeiter am Lehrstuhl Rechnernetze und Rechnerkommunikation der Universität Passau.

E-Mail: ks@sec.uni-passau.de

tige qualifiziert elektronische Signatur ist rechtlich einer Unterschrift gleichgestellt.[6] Sofern die rechtliche Vermutung, dass die signierte Erklärung vom Unterzeichner abgegeben wurde nicht entkräftet werden kann, hat das qualifiziert elektronische Dokument die Beweiskraft von Privaturkunden.[7]
Papiergebundene Informationen genießen vor Gericht einen hohen Beweiswert. Bei elektronischen Daten ist eine nachträgliche Änderung im Allgemeinen leicht durchzuführen und nur schwer nachzuweisen. Deshalb wurden Rechtsnormen zur qualifizierten elektronischen Signatur geschaffen. Bei Verwendung von solchen Signaturen werden nachträgliche Änderungen erkennbar. Maßgebend sind die europäische Signaturrichtlinie (EU-SigRL)[8] und die jeweiligen Umsetzungen in nationales Recht. In Deutschland enthalten das Signaturgesetz (SigG), sowie die Signaturverordnung (SigVO), das Bürgerliche Gesetzbuch (BGB) und die Prozessordnungen (ZPO, StPO und VwGO) relevante Vorschriften. Wenn die Vorgaben eingehalten werden, kommt den elektronischen Dokumenten nach § 371a Abs. 1 Satz 1 ZPO eine entsprechende Beweiskraft zu wie privaten (papiergebundenen) Urkunden.[9]

Das Signaturgesetz unterscheidet zwischen elektronischen Signaturen, fortgeschrittenen elektronischen und qualifizierten elektronischen Signaturen.[10] Für Letztere besteht eine wesentliche Vorgabe darin, Verfälschungen signierter Daten zuverlässig erkennbar zu machen und gegen unberechtigte Nutzung der Signaturschlüssel zu schützen.[11]

Technisch können qualifizierte elektronische Signaturen aufbauend auf kryptographisch sicheren digitalen Signaturverfahren, sicheren Signaturerstellungs-Einheiten flankiert durch organisatorische Maßnahmen realisiert werden. Ein Beispiel für eine sichere Signaturerstellungseinheit ist der Neue Personalausweis.[12] Als ausreichender Signaturalgorithmus wird dabei das RSA-Verfahren angesehen[13]. Dieses ist ein konventionelles digitales Signaturverfahren.

2.2 Worin unterscheiden sich editierbare Signaturen von konventionellen?

Im Gegensatz zu konventionellen digitalen Signaturen erlauben editierbare Signaturen nachträgliche Modifikation an den signierten Daten während das Prüfergebnis positiv bleibt. Der Unterzeichner[14] der Signatur legt Art und Umfang der Änderungsmöglichkeiten bereits *zum Zeitpunkt der Signaturerstellung* fest. Der Unterzeichner der Signatur muss für *spätere* Änderungen nicht mehr involviert werden.

Zusammenfassend weisen editierbare Signaturen folgende Charakteristika auf:

- Der Unterzeichner legt Modifikationsbefugnisse bei Signaturerstellung fest.
- Befugte Modifikationen ändern das Prüfergebnis nicht.
- Unbefugte Modifikationen führen zu einem negativen Prüfergebnis.
- Außer Unterzeichner und Verifizierer gibt es einen dritten Beteiligten, den sog. „Sanitizer“[15], der vom Unterzeichner die Befugnis zur Modifikation erhalten hat.
- Zur Modifikation bedarf es nicht der Kenntnis des geheimen Signaturschlüssels des Unterzeichners.

Editierbare Signaturen erfassen Befugnisse zur Modifikation, indem sie diese innerhalb der Signatur festhalten. Die Signatur gewährleistet Integritätsschutz durch die Erkennung von *unbefugten*, nachträglichen Änderungen. Dem Verständnis von Integrität und Erkennbarkeit aus [3] folgend, unterscheiden wir zwischen:

- Der Erkennbarkeit der Beteiligung mindestens eines Sanitizers.
- Der Erkennbarkeit zukünftiger Modifikationsmöglichkeiten.

2.3 Sind editierbare Signaturen qualifiziert?

Qualifiziert elektronische Signaturen bewirken die Erkennbarkeit von Änderungen bzw. Verfälschungen des Inhalts einer Erklärung. Als *Verfälschung* ist im strafrechtlichen Sinn „jede nachträgliche Veränderung des gedanklichen Inhalts einer echten Urkunde anzusehen, durch die der Anschein erweckt wird, als habe der Aussteller die Erklärung in der Form abgegeben, die sie durch die Verfälschung erlangt hat“.[16] Wird allerdings der Urkundeninhalt mit Einverständnis des Ausstellers abgeändert, „so liegt keine Verfälschung vor, da der geänderte Inhalt geistig vom Aussteller herrührt“.[17] Die qualifizierte Signatur muss „vor *unbefugter* Veränderung“ schützen [Hervorhebung durch die Verfasser].[18] Eine befugte Veränderung ist daher nicht aus diesem Grund durch das SigG ausgeschlossen. Ebenso wenig verbietet die SigVO ausdrücklich befugte Änderungen.[19] Außerdem müssen nach EU-SigRL „sichere Signaturerstellungseinheiten“ gewährleisten, dass „die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten von dem rechtmäßigen Unterzeichner vor der Verwendung durch andere verlässlich geschützt werden können.“[20] Unter Signaturerstellungsdaten fallen einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden.[21] Wie bereits oben erwähnt, wird bei editierbaren Signaturen dem Sanitizer der geheime Signaturschlüssel nicht offenbart. Damit sind die Signaturerstellungsdaten hinreichend verlässlich geschützt.

Jedoch wird in der EU-SigRL (umgesetzt durch § 17 Abs. 2 Satz 1 SigG) die Anforderung gestellt, dass die zu unterzeichnenden Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden.[22] Bei Benutzung einer editierbaren Signatur sind Modifikationen zwar gewollt, aber dem Unterzeichner nicht zum Zeit-

6 Art. 5 Abs. 1 lit. A EU-SigRL, § 126a Abs. 1 BGB, § 3a Abs. 2 VwVfG, § 36a Abs. 2 SGB I, § 87a Abs. 3 AO.

7 § 371a Abs. 1 ZPO.

8 Richtlinie 1999/93/EG vom 13.12.1999; ABl. EG Nr. L 13/12 vom 19.01.2000.

9 Siehe dazu auch Balfanz/Laue, DuD 2010, 815 (816 f.). Die Vorgabe dafür findet sich in Art. 5 Abs. 1 lit. a der EU-SigRL.

10 Vgl. § 2 Nr. 1 SigG („elektronische Signatur“), Nr. 2 („fortgeschrittene elektronische Signatur“) und Nr. 3 („qualifizierte elektronische Signatur“).

11 § 17 Abs. 1 Satz 1 SigG.

12 § 22 Satz 1 PAuswG.

13 Abschnitt 3.1 der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 30.12.2011, Bundesanzeiger Nr. 10, S. 243.

14 Legaldefinition in Art. 2 Nr. 3 EU-SigRL, in § 2 Nr. 9 SigG als „Signaturschlüssel-Inhaber“ und technisch im Englischen als „Signer“ bezeichnet.

15 Wir benutzen im Folgenden den Fachbegriff Sanitizer der englischen Literatur, da sich dieser nicht treffend übersetzen lässt.

16 Schönke/Schröder: StGB, 28. Aufl. 2010, § 267, Rdnr. 64.

17 Schönke/Schröder: StGB, 28. Aufl. 2010, § 267, Rdnr. 67.

18 § 17 Abs. 3 Nr. 2 SigG.

19 Vgl. § 15 SigVO.

20 Nr. 1 lit. c des Anhangs III EU-SigRL.

21 Legaldefinition nach Art. 2 Nr. 4 EU-SigRL.

22 Absatz 2 des Anhangs III EU-SigRL.

punkt der Signaturerstellung bekannt und daher nicht darstellbar. Diese Anforderung wird bei tatsächlich *editierten* signierten Dokumenten nicht erfüllt; bei unveränderten *editierbaren* signierten Dokumenten hingegen schon.

Nur wegen der fehlenden Anzeigemöglichkeit stellen editierte Signaturen keine qualifizierten Signaturen im Rechtssinne dar. Sie gelten aber als elektronische Signaturen.[23]

3 Beweiswert von Daten

Die Anforderungen des Rechts an die technische Ausgestaltung qualifizierter Signaturen dienen der Erzeugung beweisgeeigneter Daten. Beweisbedürftig sind Tatsachen, die im Prozess behauptet und zulässig bestritten werden. Daher erläutern wir nun die Beweiseignung und den Beweiswert signierter Daten.

3.1 Beweisgeeignetheit und Beweiswert signierter Daten

Qualifizierte elektronische Signaturen im Rechtssinne müssen stets als Beweismittel in Gerichtsverfahren zugelassen werden.[24] Elektronische Signaturen, die nicht qualifiziert im Sinne des Gesetzes sind, können nur unter eingeschränkten Gründen als Beweismittel zurückgewiesen werden.[25] Die Editierbarkeit unterfällt keinem der Zurückweisungsgründe. Grundsätzlich müssen deshalb auch editierbare Signaturen als Beweismittel zugelassen werden, da sie als elektronische Signatur gelten. Im Allgemeinen richtet sich der Beweiswert eines Beweismittels nach den jeweils anwendbaren Prozessordnungen. Im Zivilverfahren gilt grundsätzlich die freie Beweiswürdigung.[26] Als Beweismittel kommen Sachverständige, Augenschein, Parteivernehmung, Urkunden und Zeugen in Betracht. Auf Daten sind grundsätzlich die Regeln zum Augenscheinsbeweis anwendbar.[27] Der Beweisantritt erfolgt durch Vorlegung oder Übermittlung der Datei an das Gericht.[28] Die leichte Fälschbarkeit und dessen schwieriger Nachweis bei elektronischen Dokumenten bewirken indes einen sehr geringen Beweiswert.[29] Höher ist der Beweiswert bei qualifiziert signierten „öffentlichen elektronischen Dokumenten". Für diese besteht eine gesetzliche Beweisvermutung (der Echtheit).[30] Für private elektronische Dokumente, die qualifiziert elektronisch signiert wurden, existiert eine gesetzliche Beweiserleichterung.[31] Der Vollbeweis über die in dem Dokument enthaltene Erklärung des Unterzeichners ist geführt, wenn die Anforderungen des Signaturgesetzes (und der Signaturverordnung) erfüllt werden und die Vermutung, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist, weder erschüttert noch widerlegt wurde. Diese gesetzliche Beweisvermutung wird daher generell auf editierbare Signaturen mangels Erfüllung der Anforderungen des Signaturgesetzes keine Anwendung finden.

3.2 Anforderungen an eine editierbare Signatur zur Erhaltung des Beweiswertes

Hinsichtlich editierbarer Signaturen bleibt es damit bei dem oben genannten Grundsatz der freien Beweiswürdigung. Allerdings ist „freie Beweiswürdigung" nicht gleichbedeutend mit beliebiger Beweiswürdigung. Eine hundertprozentige Sicherheit, dass die Erklärung nicht verfälscht wurde, lässt sich praktisch nicht erreichen. Vielmehr ist entscheidend, ob mit einem für das praktische Leben brauchbaren Grad an Gewissheit festgestellt werden kann, dass die Information unverfälscht ist.[32] Maßgebend dafür sind die Wahrscheinlichkeit eines manipulierenden Eingriffs und deren Entdeckungsmöglichkeit. Der technische Aufwand, eine editierbare Signatur anders als vom Unterzeichner zugelassen und trotzdem nicht nachweisbar zu verfälschen, ist genauso hoch wie der Aufwand einer unentdeckbaren Verfälschung einer konventionellen digitalen Signatur. Dadurch kann mit vergleichbarer Sicherheit die Unverfälschtheit der signierten Information nachgewiesen werden.

Eine editierbare Urkunde entspricht einem Blankett, also einer bewusst unvollständigen Erklärung, die unterschrieben wurde, und bei dem sich der Unterzeichner der Ausfüllung durch einen Dritten bewusst ist. Solche Blanketterklärungen sind in entsprechender Anwendung des § 172 Abs. 2 BGB wirksam.[33] Das zivilrechtliche[34] Risiko einer abredewidrigen Ausfüllung trägt der Aussteller.[35] Urkundenaussteller dürfen ein höheres Risiko einer Erklärung bewusst eingehen. Sie müssen sich selbst bei qualifizierten elektronischen Signaturen nicht den Inhalt vor der Anbringung der Signatur anzeigen lassen. Die zu unterzeichnenden Daten müssen allerdings dem Unterzeichner vor dem Signaturvorgang dargestellt werden *können,* um als qualifizierte elektronische Signatur geschützt zu sein. Damit spricht das Merkmal der bewussten (eingeschränkten) Veränderbarkeit des Inhalts der Erklärung nicht gegen einen ähnlich hohen Beweiswert wie für qualifizierte elektronische Signaturen gesetzlich vermutet wird. Zumindest wird aber ein für das praktische Leben hinreichend sicherer Grad an Gewissheit erreicht, dass der Unterzeichner die Erklärung so abgeben wollte, weil er bewusst einem Dritten bestimmte Inhalte seiner Erklärung zur Ausfüllung überlassen hat. Unter Berücksichtigung der Umstände des Einzelfalls ist den editierbaren Signaturen somit grundsätzlich ein hoher Beweiswert zuzuerkennen.

4 Editierbare Signaturen

Wie bereits in der Einleitung beschrieben, kann ein Sanitizer, welcher nicht im Besitz des Signaturschlüssels ist, erlaubte Änderungen an einem bereits signierten Dokument durchführen. Hierbei wird das positive Prüfergebnis erhalten. Dies widerspricht dem Konzept konventioneller digitaler Signaturen, die *jegliche* nachträgliche Änderungen an einem signierten Dokument durch ein negatives Prüfergebnis erkennbar machen. Für editierbare Signaturen muss daher sichergestellt werden, dass die Änderungen

23 Vgl. Art. 2 Nr. 1 EU-SigRL.
24 Art. 5 Abs. 1 lit. b EU-SigRL.
25 Vgl. Art. 5 Abs. 2 EU-SigRL.
26 § 268 Abs. 1 Satz 1 ZPO.
27 Dies folgt aus § 371 Abs. 1 Satz 2 ZPO, wonach sich die Regeln des Augenscheinsbeweises auch auf elektronische Dokumente erstrecken.
28 Vgl. § 371 Abs. 1 Satz 2 ZPO.
29 Roßnagel/Pfitzmann, NJW 2003, 1209.
30 § 371a Abs. 2 Satz 2 i.V.m. § 437 Abs. 1 ZPO.
31 § 371a Abs. 1 ZPO.
32 BGH, Urteil vom 26.10.1993 – VI ZR 155/92.
33 BGH, Urteil vom 11.7.1963 – VII ZR 120/62; Schramm in: Münchener Kommentar zum BGB, 6. Aufl. 2012, § 172 BGB, Rn. 17.
34 Strafrechtlich wäre eine Urkundenfälschung gegeben, vgl. BGH, Urteil vom 04.02.1954 – 4 StR 445/53.
35 BGH, Urteil vom 11.07.1963 – VII ZR 120/62.

durch den Unterzeichner begrenzt werden können, da ansonsten die Benutzung solcher Signaturen wenig vorteilhaft erscheint. Editierbare Signaturen erlauben es daher, den Integritätsschutz konventioneller Signaturen gezielt abzuschwächen. Der Unterzeichner muss allerdings den Rahmen, wie das signierte Dokument editiert werden kann, während der Signaturerstellung festlegen. Um den Sanitizer gezielt einschränken zu können, gehen wir im Folgenden davon aus, dass das Dokument m in disjunkte, also nicht überlappende, Teildokumente m_i aufgeteilt wird. Damit gilt: $m=m_1||...||m_n$. Überlappende Teildokumente wurden bisher nur von Klonowski et al. [4] und Pöhls et al. [5] behandelt. Der Einfachheit halber werden überlappende Teildokumente nicht berücksichtigt. Darüber hinaus werden Datenstrukturen, welche über die Komplexität von Listen hinausgehen, nicht in dieser rechtlichen Betrachtung behandelt.[36] Die grundsätzlichen Ideen und Sicherheitsziele sind jedoch ohne Weiteres übertragbar.

Editierbare Signaturen kommen in zwei unterschiedlichen Ausprägungen vor:

- „Sanitizable Signatures“ und
- „Redactable Signatures“.

Technisch handelt es sich hingegen um unterschiedliche Konzepte.[37] Im Folgenden werden wir beide erläutern.

4.1 Sanitizable Signatures

Eine Ausprägung editierbarer Signaturen wird in der englischen Literatur als “Sanitizable Signatures“ bezeichnet [7]. Diese erlaubt es einer vom Unterzeichner festgelegten dritten Partei, dem “Sanitizer“, vom Unterzeichner designierte Blöcke $m_i \subseteq m$ des Dokumentes beliebig zu ändern. Konkret erlauben es Sanitizable Signatures, dass ein Dokument $m=m_1||...||m_n$ durch den Sanitizer in $m'=m_1'||...||m_n'$ abgewandelt werden kann. Zu beachten ist hier, dass Blöcke nur geändert, allerdings nicht entfernt werden können. Die Blöcke, die vom Sanitizer geändert werden können, werden als „admissible blocks“ (ADM) bezeichnet. ADM kann beispielsweise als Menge aufgefasst werden, welche die Indizes der vom Sanitizer änderbaren Teildokumente von m beschreibt. Darüber hinaus existieren Möglichkeiten, die die Auswahl zulässiger Inhalte für änderbare Blöcke einschränken [4].

Brzuska et al. [8] haben ein algorithmisches Modell für Sanitizable Signatures entwickelt. In diesem Modell gibt es nur einen Sanitizer. Im Weiteren benutzen wir dieses Modell zur Beschreibung. Die Algorithmen ihres Modells sind:

- $\mathtt{KeyGen}_{Sig}$: Der Unterzeichner muss ein Schlüsselpaar (pk_{Sig}, sk_{Sig}) generieren, welches zur Ausstellung und Verifikation der erstellten Signaturen genutzt wird.
- $\mathtt{KeyGen}_{San}$: Der designierte Sanitizer muss ein Schlüsselpaar (pk_{San}, sk_{San}) für die Schwärzung generieren. Der Algorithmus darf nicht vom Unterzeichner ausgeführt werden, um die Verantwortlichkeit nachvollziehbar zu machen.
- Sign: Erstellt die Signatur. Dieser Algorithmus benötigt den privaten Schlüssel des Unterzeichners, jedoch nur den öffentlichen Schlüssel des Sanitizers. Darüber hinaus muss der Unterzeichner festlegen, welche Teile des Dokumentes (ADM) schwärzbar sind.
- Verify: Verifiziert die Signatur mit Hilfe des öffentlichen Schlüssels des Unterzeichners.
- Sanitize: Jeder, der im Besitz von sk_{San} ist, kann die designierten Blöcke, gelistet in ADM, beliebig abändern.
- Proof: Mit Hilfe von sk_{Sig} generiert dieser Algorithmus einen Beweis π, welcher vom
- Judge: genutzt wird, um die Herkunft des Signatur-Dokument-Paares zu bestimmen.[38]

In der obigen Beschreibung wird ersichtlich, dass der Unterzeichner nicht in der Lage ist, nachträgliche Änderungen durchzuführen. Dies ist ausnahmslos dem Sanitizer möglich. Dieser Umstand erlaubt es, im Nachhinein eindeutig festzustellen, welche Partei zuletzt Änderungen durchgeführt hat. Zu beachten ist, dass ein Sanitizer die Möglichkeit hat, die signierte Nachricht nicht zu editieren, aber dennoch die schützende Signatur mit seinem Schlüssel zu ändern. Dies führt nach Definition dazu, dass der Algorithmus Judge den Sanitizer als den technisch Verantwortlichen des Signatur-Dokument-Paares ausgibt. In diesem Fall muss der Unterzeichner dazu veranlasst werden, das Originaldokument herauszugeben, um tatsächliche Änderungen am Dokument feststellen zu können.

4.2 Redactable Signatures

Die zweite Ausprägung, im Englischen „Redactable Signatures“ genannt, wurden als „Content Extraction Signatures“ eingeführt [9] bzw. als „Homomorphic Signatures“ [10]. Im Gegensatz zu Sanitizable Signatures erlauben es Redactable Signatures nicht, Teildokumente beliebig zu ändern, sondern nur, dass Teildokumente durch das spezielle Symbol $\perp$, $\perp \notin \{0,1\}^*$, zu ersetzen. Bei diesen editierbaren Signaturen ist es jeder Partei, also auch dem Unterzeichner selbst, möglich, Teildokumente m_i des Dokumentes m zu entfernen, also ein Dokument zu schwärzen.[39]

Redactable Signatures können wiederum in zwei weitere Kategorien eingeteilt werden:

- **Quoteable Signatures:** Erlauben es nur *zusammenhängende Teile* einer Liste zu *zitieren*.
- **General Redactable Signatures:** Erlauben es *beliebige Elemente* einer Liste zu *entfernen*.

Im Folgenden wird keine Unterscheidung getroffen, da sich die Sicherheitsmodelle und die algorithmische Beschreibung nur unwesentlich voneinander unterscheiden. Die algorithmische Beschreibung:

- $\mathtt{KeyGen}_{Sig}$**:** Wie für Sanitizable Signatures.
- Sign**:** Führt die Aktion der Signaturerstellung durch. Dieser Algorithmus benötigt den privaten Schlüssel des Unterzeichners.
- Verify**:** Verifiziert die Signatur.
- Redact**:** Entfernt eine Menge von Blöcken. Dieser Algorithmus benötigt *keine* privaten Schlüssel.
- Close**:** Verbietet es einem weiteren Sanitizer, Blöcke zu entfernen. Dieser Algorithmus benötigt ebenfalls keine privaten Schlüssel und erlaubt die Umsetzung des „Consecutive Sanitization Control“.

36 Dies sind unter Anderem Bäume oder Graphen, wie von Kundu et al. [6] beschrieben.

37 Von Slamanig und Raas [2] wurden diese Ausprägungen als Eigenschaft eingestuft.

38 Judge benötigt den Beweis π. Diesen kann nur der Unterzeichner generieren.

39 Es existieren Schemata, die Mischformen aus Redactable und Sanitizable Signatures darstellen [11].

4.3 Sicherheitsmodell

Jede konkrete Umsetzung verfügt über eigene Sicherheitsmodelle, die denen der qualifizierten elektronischen Signaturen gleichwertig sein müssen. Über die Modellgrenzen hinweg lassen sich die grundlegenden Sicherheitseigenschaften editierbarer Signaturen wie folgt beschreiben. Es werden die englischsprachigen Begriffe verwendet, um Irritation zu vermeiden. Zunächst gibt es eine Eigenschaft, die sich von denen konventioneller Signaturen kaum unterscheidet:

- **Unforgeability**: Niemand, außer dem Unterzeichner, darf in der Lage sein, Signaturen zu erzeugen, die sich nicht aus Bestehenden ableiten lassen.

Da editierbare Signaturen spätere Änderungen zulassen, muss es weitere Sicherheitseinschränkungen geben. Diese werden nun erläutert.

- **Immutability/Disclosure-Secure:** Ein Sanitizer darf nicht in der Lage sein, Blöcke des signierten Dokumentes zu ändern oder zu entfernen, welche nicht dafür vorgesehen wurden.
- **Privacy/Transparency/Detectability:** *Privacy* bedeutet, dass ein Verifizierer keine Rückschlüsse auf die Originalnachricht treffen kann, wenn ihm eine signierte Nachricht vorliegt. Dieses ist vergleichbar mit der durch Verschlüsselung erreichten Vertraulichkeit. Transparency ist eine stärkere Eigenschaft als Privacy. *Transparency* bedeutet, dass ein Verifizierer nicht entscheiden kann, welcher private Schlüssel (Unterzeichner oder Sanitizer) als Letztes eingesetzt wurde. *Detectability* ist das Gegenteil von Transparency: Wenn ein Sanitizer die Signatur geändert hat, dann soll dies ein Verifizierer sehen können.
- **(In-)Visibility:** *Visibility* bedeutet, dass der Verifizierer sehen kann, welche Blöcke modifizierbar sind; dies bedeutet, dass `ADM` von Jedem rekonstruiert werden kann. Konsequenterweise bedeutet daher *Invisibility*, dass ein Verifizierer nicht sehen kann, welche Blöcke schwärzbar sind. Beide Eigenschaften gibt es nur für Sanitizable Signatures, da Redactable Signatures einem Jeden Veränderungen erlauben.
- **Accountability:** *Accountability* bedeutet, dass derjenige festgestellt werden kann, der als Letztes seinen privaten Schlüssel eingesetzt hat. Dies bedeutet, dass die Algorithmen `Judge` und `Proof` korrekt arbeiten.
- **Restrict-to-Values:** Diese Eigenschaft verbietet einem Sanitizer einen modifizierbaren Block beliebig zu ändern. Vielmehr kann der Sanitizer nur einen Wert aus einer Wertemenge einfügen, welche vorher vom Unterzeichner festgelegt wurde.

4.4 Erkennbarkeit

Angenommen, man kann die Änderungen an der signierten Nachricht technisch erkennen, so lassen sich die folgenden Fälle unterscheiden:

- Fall 1: Unverändert
- Fall 2: Befugte Änderung
- Fall 3: Unbefugte Änderung.

Der Einfachheit halber betrachten wir nur das gesamte Dokument und halten unbefugte Änderungen für schwerwiegender. Damit wird bei gleichzeitiger Anwesenheit von befugten und unbefugten Änderungen das Dokument insgesamt als unbefugt klassifiziert. Bei der technischen Umsetzung muss Privacy gewahrt bleiben. Eine Implementierung darf trotz der Erkennbarkeit zwischen „Unverändert" und „Befugte Änderung" keine Rückschlüsse auf die Ursprungsnachricht zulassen. Daher kommt es in der technischen Umsetzung zu folgender Besonderheit: Trotz unveränderter Nachricht ($\mathtt{m} = \mathtt{m}'$) gilt der Status „befugte Änderung", sofern der Sanitizer dies wünscht. Es ist also nicht möglich aus dem Status „Befugte Änderung" alleine zu folgern, dass sich die Nachricht geändert hat. Detectability und Accountability ermöglichen technisch eine Unterscheidbarkeit von Fall 1 und 2, mit der Einschränkung, dass die Nachricht nicht geändert worden sein muss. Der Unterschied zwischen Detectability und Accountability besteht darin, dass Accountability den privaten Schlüssel des Unterzeichners und damit seine aktive Teilnahme benötigt. Bei Detectability hingegen werden nur die involvierten öffentlichen Schlüssel benötigt. Weitergehend kann der Grad der Änderungserkennung verfeinert werden:

- Mindestens eine Änderung
- Genaue Anzahl der Änderungen
- Genaue Position der Änderung.

5 Praxisbeispiele

Nach einer kurzen Einführung in lebensmittelrechtliche Vorgaben, beleuchten wir anhand des Praxisbeispiels einer *stillen Rücknahme* Schwärzungen von Dokumentinhalten und anschließend im Praxisbeispiel *Ablieferbeleg* zugelassene Änderungen von Dokumentinhalten.

5.1 Einführung in das Lebensmittelrecht

Das Lebensmittelrecht verfolgt unter Anderem zwei wichtige Ziele: Herstellung von Sicherheit und Vertrauen für die Beteiligten.[40] Dennoch sind „Lebensmittelskandale" keine Seltenheit. Teilweise mehrmals im Jahr werden unsichere[41] oder gar lebensgefährliche Nahrungsmittel zurückgerufen. Häufig kommt es zu einer stillen internen Rücknahme[42]. Einen öffentlichen Rückruf[43] muss ein Unternehmen nur starten, wenn Produkte bereits an Endverbraucher verkauft und wahrscheinlich noch nicht verbraucht wurden (z.B. wegen relativ langer Haltbarkeit der Ware). Um einen Produktrückruf zu ermöglichen, ist eine Identifizierung betroffener Produkte erforderlich. Diese Identifizierung erfolgt in der Praxis zumeist anhand der Chargennummer (rechtlich: Los-Kennzeichnung[44]) in Verbindung mit dem Mindesthaltbarkeits-

40 Erwägungsgründe 9, 18, 22, 23, 35 und 40 der VO (EG) 178/2002. „Sicherheit und Vertrauen der Verbraucher in der Gemeinschaft und in Drittländern sind von größter Bedeutung." (Erwägungsgrund 23).

41 Unsicher ist der in Art. 14 Basisverordnung 178/2002 benutzte Oberbegriff für gesundheitsschädliche und verzehrungeeignete Lebensmittel, worunter auch verdorbene, ekelerregende und in täuschender Weise falschetikettierte Nahrungsmittel fallen.

42 Rücknahme wird in Art. 2 lit. h der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit definiert als: „jede Maßnahme, mit der verhindert werden soll, dass ein gefährliches Produkt vertrieben, ausgestellt oder dem Verbraucher angeboten wird."

43 Rückruf ist in Art. 2 lit. g der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit definiert als: „jede Maßnahme, die auf Erwirkung der Rückgabe eines dem Verbraucher vom Hersteller oder Händler bereits gelieferten oder zur Verfügung gestellten gefährlichen Produkts abzielt."

44 Geregelt in der Los-Kennzeichnungs-Verordnung vom 23.06.1993; BGBl. I S. 1022.

datum[45]. Rückverfolgungssysteme sind nach Art. 18 Abs. 2 und 3 der Lebensmittelbasisverordnung[46] europaweit verpflichtend vorgeschrieben. Danach sind Lebensmittelunternehmen verpflichtet, Systeme und Verfahren einzurichten, mittels derer sie jede Person feststellen können, von denen sie Lebensmittel oder Lebensmittelzutaten bezogen oder ausgeliefert haben. Die Ausgabe an den Endverbraucher ist nicht betroffen. Der Zweck dieser Vorgabe liegt darin, unsichere Lebensmittel schnell und effektiv aus dem Verkehr ziehen zu können. Das wird dadurch erreicht, dass die beteiligten Händler unverzüglich informiert werden. Im Folgenden wird exemplarisch erläutert, wie durch editierbare Signaturen der Prozess des Produktrückrufes medienbruchfrei, elektronisch verifizierbar wird.

5.2 Praxisbeispiel: Stille Rücknahme (Redactable)

Rechtlich besteht keine chargengenaue Dokumentationspflicht sondern nur eine Obliegenheit.[47] Das bedeutet, dass es dem Unternehmer freigestellt ist, wie präzise er die Lebensmittelprodukte verfolgt. Allerdings muss der Unternehmer im Rückruffall Nachteile in Kauf nehmen, wenn betroffene Produkte nicht genau identifiziert werden können (etwa durch eine Chargenverfolgung), weil dann nicht nur eine Charge zurückgerufen werden muss, sondern alle derartigen Produkte. Derzeit erfolgt die Dokumentation zumeist auf unterschiedlichen Medien, was Fälschungen erleichtert und eine zügige Rückverfolgung erschwert. Beim Dioxinskandal 2010/2011 dauerte die vollständige Auswertung aller beschlagnahmten Dokumente mehrere Wochen. Für eine effektivere Information aller Betroffenen, müsste die Auswertung der Dokumente viel schneller erfolgen. Das Problem ist die weitreichende Verflechtung der Warenströme. Beim Dioxinskandal wurden aus ca. 180t dioxinbelasteter Mischfettsäure über 2.000t Futtermischfette produziert und an über 20 Futtermittelhersteller geliefert. Daraus wiederum wurden 25.000 bis 125.000t[48] belastete Futtermittel hergestellt, die an Tiere verfüttert wurden. Eine schnellere Identifikation des Verursachers kann durch Auswertung der Dokumente erfolgen die zwischen den Beteiligten ausgetauscht wurden. Dazu ist es aber nicht nur notwendig, dass die Dokumente elektronisch erfasst werden, sondern auch, dass die Dokumente nicht verfälscht werden können, um so die Vertuschung von Problemen zu erschweren. Signiert man nun alle Dokumente konventionell digital, so kann man sie nur in Gänze verifizieren. Die dazu notwendige Weitergabe aller Informationen widerspricht den schutzwürdigen Interessen der beteiligten Unternehmen, da mehr Informationen preisgegeben werden müssten als zur Aufklärung oder Rekonstruktion von Lieferverflechtungen nötig sind. Beispielsweise sind Einkaufspreise hierfür in der Regel nicht relevant und werden im Normalfall als Geschäftsgeheimnisse betrachtet[49]. Hier bietet sich der Einsatz von Redactable Signatures an.

Angenommen bei einer routinemäßigen Eigenkontrolle eines Eierproduzenten werden gesundheitsgefährdende Dioxinbelastungen festgestellt. Um einem Imageschaden und Umsatzeinbußen vorzubeugen, wird eine stille Rücknahme in Betracht gezogen. Diese ist nur dann möglich, wenn die belastete Charge noch nicht den Endverbraucher erreicht hat. Um dies festzustellen, tauschen die an der Lebensmittelwarenkette Beteiligten schnellstmöglich Dokumente untereinander aus. Um Geschäftsgeheimnisse zu wahren, werden vor Weitergabe der Dokumente nicht relevante Geschäftsgeheimnisse geschwärzt. Trotzdem müssen alle Dokumente verlässlich sein und einen dementsprechend hohen Beweiswert besitzen. Dies bezweckt eine Absicherung für einen potenziell eintretenden Haftungsfall und Schutz vor unzulässig manipulierten Dokumenten. Insbesondere muss sich aus den Dokumenten ergeben, dass die belastete Charge den Endverbraucher beweisbar nicht erreicht hat, da ansonsten ein öffentlicher Warenrückruf über die Massenmedien erfolgen muss.[50] Editierbare Signaturen ermöglichen dies. Dafür müssen sie die folgenden technischen Eigenschaften aufweisen:

- Privacy, um die geheimnisbewahrende Schwärzung zu ermöglichen,
- Unforgeability und Disclosure Security gewährleisten Fälschungssicherheit,
- Accountability, ermöglicht im Nachgang die Klärung der Verantwortlichkeit.

Hat man zusätzlich zu Accountability noch Detectability, so erreicht man das Schutzniveau konventioneller Signaturen, solange keine Schwärzung vorliegt. Detectability führt damit die editierbare Signatur einer weiteren Nutzung zu, so dass man sie auch im regulären Geschäftsverkehr anstelle konventioneller Signaturen einsetzen kann.

5.3 Praxisbeispiel: Änderungen des Ablieferbelegs (Sanitizable)

Angenommen ein Abfüller (Lebensmittelunternehmer) verkauft eine Lieferung Obstbrand an einen gewerblichen Empfänger. Ein Frachtführer erhält nun den Transportauftrag. Der Abfüller erstellt einen Frachtbrief[51] mitsamt einer vorgefertigten änderbaren Ablieferquittung[52]. Der Frachtbrief beschreibt Art und Menge der Ware. Der Abfüller signiert den Frachtbrief mit einer Sanitizable Signature und legt als Sanitizer den Empfänger fest. Der Frachtführer signiert nach Prüfung der Ware ebenfalls den Frachtbrief. Dadurch wird (widerleglich) nachgewiesen, dass der Obstbrand vom Frachtführer unversehrt übernommen wurde. Bei der Signatur des Frachtführers handelt es sich ebenso um eine nur durch den späteren Empfänger änderbare Sanitizable Signature. Beide Signaturen erlauben ausschließlich eine Änderung der vorgefertigten Ablieferquittung durch den Empfänger. Bei Ablieferung

45 Die Angabe des Mindesthaltbarkeitsdatums bzw. des Verbrauchsdatums oder des Datums des ersten Einfrierens ist vorgeschrieben in Art. 9 Abs. 1 lit. f und Art. 24 der EU-Kennzeichnungsverordnung VO (EG) Nr. 1169/2011 vom 25.10.2011; ABl. EU Nr. L 304/18 vom 22.11.2011.

46 VO (EG) Nr. 178/2002 vom 28.01.2002; ABl. EG Nr. L 31/1 vom 01.02.2002.

47 Etwas anderes gilt für Lebensmittel tierischen Ursprungs nach Art. 3 Abs. 1 lit. g der Durchführungsverordnung (EU) Nr. 931/2011 vom 19.09.2011, der (besonders deutlich in der deutschen Fassung) eine chargengenaue Rückverfolgbarkeit vorschreibt.

48 Zahlen sind Schätzungen des BfR, Stellungnahme Nr. 002/2011 vom 26.01.2011 und BMELV, Pressemitteilung Nr. 229 vom 07.01.2011.

49 Quedenfeld in: Münchener Kommentar zum HGB, 2. Aufl. 2008, § 333 HGB, Rn. 15.

50 Vgl. Art. 19 Abs. 1 und 3 VO (EG) 178/2002; die Behörde kann einen öffentlichen Rückruf anordnen nach § 39 Abs. 2 Satz 2 Nr. 7, 8 LFGB.

51 § 408 Abs. 2 HGB bestimmt: „Der Frachtbrief wird in drei Originalausfertigungen ausgestellt, die vom Absender unterzeichnet werden. Der Absender kann verlangen, dass auch der Frachtführer den Frachtbrief unterzeichnet." § 409 HGB enthält Vorgaben zur Beweisvermutung des Frachtbriefs, insbesondere der unversehrten Übernahme durch den Frachtführer.

52 Die Ablieferquittung bestimmt sich nach § 368 BGB.

quittiert der Empfänger (Abnehmer) die Menge des erhaltenen Gutes und seines äußerlichen Zustandes auf erkennbare Schäden, indem der Empfänger die Rolle des Sanitizers der Ablieferquittung annimmt. Technisch bedarf es zur Ausübung der Sanitizerrolle der Kenntnis des privaten Schlüssels des Sanitizers. Damit wird nachgewiesen, dass die bestätigte Menge unversehrt übernommen wurde. Diese Anwendung einer Sanitizable Signature ermöglicht dem Abfüller und dem Frachtführer eine integritätssichernde und beweiskräftige elektronische Dokumentation des gesamten Vorganges in nur einem Dokument mit jeweils nur einer Signatur. Diese kann den Lebensmittelbehörden einfach und schnell übermittelt und von ihnen schneller elektronisch ausgewertet werden.

Dafür müssen sie die folgenden technischen Eigenschaften aufweisen:

- Immutability, welche dem Unterzeichner erlaubt, Teile des Frachtbriefes gegen jegliche Änderungen zu schützen.
- Privacy, um vor einem Externen die gemachten Änderungen (beispielsweise bei beschädigter Ladung) geheimnisbewahrend zu verstecken.
- Unforgeability gewährleistet die Beweiskraft.
- Accountability ermöglicht den späteren Nachweis, dass der Empfänger als Sanitizer Änderungen vorgenommen hat. Damit wird die Quittungsfunktion umgesetzt.

Zusätzliche Einschränkungen sind durch die Nutzung der Eigenschaft Restrict-to-Values möglich. Wie im vorherigen Beispiel, ist auch hier die Eigenschaft Detectability hilfreich, Accountability aber hinreichend.

6 Fazit

Während die Technik die Möglichkeit zur Erzeugung editierbarer Signaturen bietet – zum Beispiel zur nachträglichen „Schwärzung" von Inhalten oder der Korrektur von Angaben durch den Empfänger –, hat das Signaturrecht diese Entwicklungen bislang noch nicht inkorporiert. Dennoch kann eine Nutzung in der Praxis bereits die Vorteile erzielen, auch ohne den Status der qualifiziert elektronischen Signatur zu erlangen.

Die Einsatzfelder editierbarer Signaturen sind dabei nicht auf das Lebensmittelrecht beschränkt. Die Fälschungssicherheit entspricht technisch der konventioneller Signaturen. Sie muss aber nach geltendem Recht im jeweiligen Gerichtsprozess erst mittels Sachverständigengutachten erwiesen werden. Deshalb bleiben die Möglichkeiten in der Praxis noch ungenutzt. Daher ist es als Rechtsfortbildungsvorschlag sinnvoll, editierbare Signaturen wie qualifizierte elektronische Signaturen einzustufen. Dies gilt unter der Prämisse, dass das Sicherheitsniveau der editierbaren Signaturen dem der konventionellen Signaturen entspricht. Dazu gehört die Vergleichbarkeit von Schlüssellängen, Verfahren sowie von organisatorischen Maßnahmen. Wie wir gezeigt haben, sind editierbare Signaturen bisher nur als qualifizierte elektronische Signaturen, mit entsprechend hohem Beweiswert einzustufen, wenn das signierte Dokument nachweisbar nicht geändert wurde. Editierbare Signaturen werden durch die vielfältigen Anwendungsmöglichkeiten den Einzug in die Praxis schaffen.[53]

Literatur

[1] R. Rivest, A. Shamir und L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", in: *Commun. ACM*, 1983.

[2] D. Slamanig und S. Rass, „Redigierbare Digitale Signaturen: Theorie und Praxis" in: *Datenschutz und Datensicherheit,* Bd. 35, Nr. 11, S. 757-762, 2011.

[3] H. C. Pöhls und F. Höhne, „The Role of Data Integrity in EU Digital Signature Legislation - Achieving Statutory Trust for Sanitizable Signature Schemes" in: *7th International Workshop on Security and Trust Management*, 2011.

[4] M. Klonowski und A. Lauks, „Extended Sanitizable Signatures" in: *ICISC*, 2006.

[5] H. C. Pöhls, K. Samelin und J. Posegga, „Sanitizable Signatures in XML Signature - Performance, Mixing Properties, and Revisiting the Property of Transparency" in: *Applied Cryptography and Network Security*, 2011.

[6] A. Kundu, M. Atallah und E. Bertino, „Data in the Cloud: Authentication of Trees, Graphs, and Forests Without Leaking" Computer Science CERIAS, 2010.

[7] G. Ateniese, D. H. Chou, B. de Medeiros und G. Tsudik, „Sanitizable Signatures" in: *European Symposium on Research in Computer Security*, 2005.

[8] C. Brzuska, M. Fischlin, T. Freudenreich, A. Lehmann, M. Page, J. Schelbert, D. Schröder und F. Volk, „Security of Sanitizable Signatures Revisited" in: *Public Key Cryptography*, 2009.

[9] R. Steinfeld und L. Bull, „Content Extraction Signatures" in: *Information Security and Cryptology*, 2002.

[10] R. Johnson, M. David, D. X. Song und D. Wagner, „Homomorphic Signature Schemes" in: *CT-RSA*, 2002.

[11] T. Izu, N. Kunihiro, K. Ohta, M. Sano und M. Takenaka, „Sanitizable and Deletable Signature" in: *WISA*, 2008.

[12] K. Miyazaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, S. Tezuka und H. Imai, „Digitally Signed Document Sanitizing Scheme with Disclosure" in: *IEICE Transactions*, 2005.

53 Beispielhaft dargestellt im Projekt MedVault: Ensuring Security & Privacy for Medical Data. http://medvault.gtisc.gatech.edu/ (Stand: Mai 2012); Das Einsatzgebiet editierbarer Signaturen kann insbesondere auch auf XML-Dokumente Anwendung finden, vgl. hierzu beispielhaft: Geuer-Pollmann, XML Signature – Einführung und Empfehlungen für den sicheren Einsatz, DuD 7/2003, S. 734; Giessmann, X.509-konforme Gültigkeitsprüfungen von XML-Signaturen, DuD 4/2005, S. 201; Grimm, XML-Sicherheits-mechanismen erobern die Anwendungen, DuD 11/2007, S. 798.