

Gültigkeit elektronischer Signaturen

Immer wieder wird – auch von so genannten Spezialisten – behauptet, dass elektronische Signaturen nur begrenzt gültig wären. Z. T. ergänzt mit der Konkretisierung einer Gültigkeit von 5 Jahren laut Signaturgesetz. Somit müssten Signaturen kontinuierlich erneuert, d.h. nachsigniert werden.

Diese Aussage ist gleich in mehrfacher Hinsicht falsch!

1. Die „qualifizierte elektronische Signatur“ (nur die ist hier relevant) ist laut §126a BGB der traditionellen Unterschrift gleich gestellt und genau wie diese unbegrenzt gültig.
2. Nicht die Signatur, sondern das Zertifikat (der elektronische Personalausweis) ist - meist auf zwei oder drei Jahre – begrenzt, wie die meisten anderen Identifikationskarten auch.
3. Die im Signaturgesetz genannten 5 Jahre beziehen sich auf die Verpflichtung der Trust Center die Zertifikatdaten zur eventuellen Prüfung vorzuhalten. In Deutschland gibt es aber fast nur „akkreditierte“ Trust Center, die die Daten 30 Jahre vorhalten müssen. Beide Fristen beginnen mit Ablauf des Zertifikats, so dass die Prüfung bis zu 8 bzw. 33 Jahre möglich ist.
4. Nachsignieren verlängert nicht die Signatur, z. B. die Willenserklärung, sondern „friert“ – typischerweise mit einem Zeitstempel - das Gesamtkonstrukt ein.

Warum ist das Zertifikat nun begrenzt gültig? Dies ist durch die Verbindung zu den mathematischen Verschlüsselungsverfahren begründet, mit denen die Signatur erstellt wird. Durch die Fortschritte der Informationstechnologie wird befürchtet, dass die Algorithmen gebrochen werden und damit unentdeckte Manipulationen der Originaldaten möglich werden könnten. In der Praxis wäre die Vertuschung einer gezielten Manipulation auch mit einem gebrochenen Verschlüsselungsalgorithmus bei weitem nicht trivial, aber eben möglich.

Damit dies nicht passiert, beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich die Entwicklung und macht bei Bedarf die Vorgaben für längere Schlüssel oder neue Algorithmen, die dann auch die Grundlage für neu ausgestellte Zertifikate sind. Veröffentlicht werden die Vorgaben auf der Internet-Seite der Bundesnetzagentur. „Bei Bedarf“ heißt aber auch, dass neue Zertifikate mit dem gleichen Algorithmus und der gleichen Schlüssellänge ausgegeben werden, wenn es keinen Grund für eine Veränderung gibt.

Auf die bereits geleisteten Signaturen hat der Zertifikatablauf keinen Einfluss, so wie traditionell unterschriebene Verpflichtungen und Willenserklärungen auch nicht deshalb ungültig werden, weil der Personalausweis mit dem man sich ursprünglich identifiziert hat, durch ein neues Exemplar ersetzt wurde.

Die Signaturverordnung spricht davon, dass der „Sicherheitwert der vorhandenen Signatur“ geringer wird. Dies ist vergleichbar mit dem Vergilben eines Thermopapierfax. Die Aussage des Faxes ist klar, so lange das Fax gut lesbar ist. So lange wird auch kaum jemand die Inhalte anzweifeln. Fängt es jedoch an zu

vergilben sind Text und Unterschrift schwer zu erkennen und schon ergeben sich erste Zweifel an den Aussagen, so dass Diskussionen entstehen können. Ähnliche Diskussionen können sich ergeben, wenn jemand feststellt, dass eine elektronische Signatur mit einem Algorithmus erstellt wurde, der mittlerweile gebrochen wurde. Prinzipiell gilt die Signatur nach wie vor, aber man muss evtl. darlegen warum das Ergebnis nicht manipuliert worden sein kann.

Dabei ist zu bedenken, dass auch bisher Manipulationen möglich waren und dennoch - laut erfahrener Rechtsanwälte - nur extrem selten die Integrität eines Beweisdokumentes angezweifelt wird.

Woher kommt also die Aussage, dass Signaturen begrenzt gültig wären und alle zwei bis drei Jahre eine Nachsignatur erforderlich wäre?

Weil der §17 der Signaturverordnung eine Nachsignatur mitsamt einem Zeitstempel empfiehlt, „wenn diese [Daten] für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind.“ Dabei ist dieser §17 der Signaturverordnung eine sehr offensive Interpretation des §6 des Signaturgesetzes, bei dem es eigentlich um die Unterrichtsverpflichtung der Trust Center gegenüber ihren Kunden geht. Darin heißt es, das Trust Center „hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur *bei Bedarf* neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.“

„Bei Bedarf“ ist in den 1 ½ Seiten Kommentar, die Bröhl&Tettenborn¹ dem §6 widmen mit keinem Wort erläutert. Der Kommentar zu §17 Signaturverordnung weist hingegen darauf hin, dass damit eine Anpassung an die Signaturverordnung von 1997 erfolgte. Die EU-Richtlinie, die eigentliche Grundlage für das Signaturgesetz von 2001, kennt nämlich kein Nachsignieren und in anderen Ländern² ist dies auch kein Diskussionspunkt.

Da die Signaturverordnung das Signaturgesetz detailliert, ist zunächst die Frage nach dem Bedarf (§6 SigG) prinzipiell zu klären und dann zu prüfen, ob die Signatur für „längere Zeit in signierter Form“ (§17 SigV) benötigt werden. Dabei geht es also einerseits um die Zeitspanne zwischen Signatur und Signaturprüfung und andererseits um die Frage, ob danach die Signatur noch zur Prüfung der Integrität erforderlich ist.

Typischerweise wird eine Signatur beim Eingang eines Dokumentes in das Unternehmen geprüft und typischerweise ist die Signatur kurz vorher erstellt worden. Die Signatur dient somit der „Verkehrssicherheit“ über ungesicherte Netze und ist zu diesem Zweck unzweifelhaft sehr sinnvoll.

Was ist aber mit der Archivierung der Unterlagen innerhalb der Unternehmen?

Viele Firmen verfügen bereits über so genannte „revisionssichere“ elektronische Archive (DMS oder ECM). „Revisionssicher“ heißt dabei, dass Veränderungen vermieden - nicht nur erkannt - werden. Warum sollen die Inhalte dieser Archive

¹ Bröhl&Tettenborn, Das neue Recht der elektronischen Signaturen, Kommentierende Darstellung von Signaturgesetz und Signaturverordnung, Bundesanzeiger Verlag, 2001

² Ausnahme Österreich

zusätzlich noch nachsigniert werden? Dies entspricht dem Umschnallen eines Gürtels, obwohl die Hosenträger schon gut halten.

Lediglich wenn Dokumente die Unternehmensgrenzen verlassen, ist wieder die Verkehrsfähigkeit gefordert, bei der die Signatur die bevorzugte Technologie darstellt. Wenn kein revisionssicheres Archiv vorhanden ist, ist natürlich ebenfalls die Signatur eine interessante Alternative zur Verifizierung der Integrität. Allerdings muss nochmals betont werden, dass die Signatur Veränderung erkennbar macht, aber nicht verhindert. Insofern kann sie ein revisionssicheres Archiv nicht wirklich ersetzen.

Das kontinuierliche Nachsignieren großer revisionssicherer Archivbestände ist aber nicht sinnvoll und nicht wirtschaftlich, weil kein Mehrwert generiert, sondern lediglich der Status Quo erhalten wird. Auch wenn das viel diskutierte ArchiSig-Verfahren die Aufgabe unzweifelhaft relativ elegant löst, so sind der Aufwand und die Gesamtkosten in der Praxis bei großen Beständen und regelmäßigem Nachsignieren nicht zu unterschätzen. Hat man keine großen Bestände, sondern ist ein kleines mittelständisches Unternehmen, ist der Aufwand erst recht nicht zu rechtfertigen. Zumindest bei den elektronischen Rechnungen haben die Behörden Einsicht walten lassen und verlangen keine Nachsignatur.

Fazit: So wie wir uns nicht auf die Veränderung des Schriftzugs unserer Unterschrift seit der Volljährigkeit zurückziehen können, sondern für gezeichneten Kredite, Bürgschaften und beliebige Verträge bis zum Zeitungsabonement gerade stehen müssen, so gilt auch die qualifizierte elektronische Unterschrift zunächst mal unbegrenzt. Ob Nachsignieren Pflicht oder Kür oder überflüssig ist, darf und muss jedes Unternehmen selbst entscheiden.