# 1000mal signiert ...

## Aspekte der qualifizierten „Massensignatur“

**Digitale Signaturen versprechen in Wirtschaft und Verwaltung immense Einsparpotenziale, besonders dort, wo mehr als nur ein paar Belege zu bearbeiten sind. Doch das massenhafte Erzeugen qualifizierter elektronischer Signaturen wirft auch spezifische Probleme und Fragen auf – juristisch wie technisch und organisatorisch.**

George Washington

*Von Detlef Hühnlein, Michelau, und Yvonne Knosowski, Siegen*

Dass man mit Automatisierung Geld sparen kann, ist nichts Neues. Neu sind hingegen die spezifischen Probleme, wenn man qualifizierte elektronische Signaturen gemäß dem deutschen Signaturgesetz (SigG [1]) automatisiert erzeugen will. Um hierzulande beispielsweise eine (ausschließlich) elektronisch erhaltene Rechnung steuerlich geltend machen zu können, muss diese jedoch eine solche qualifizierte elektronische Signatur tragen (§ 14, Abs. 4, Satz 2 UStG).

Dem großen Einsparpotenzial beim Aussteller stehen somit möglicherweise hohe Prozesskosten gegenüber: Müsste für die Erzeugung jeder einzelnen Signatur von einem Operator eine PIN eingegeben werden, so würde der erhöhte Personalbedarf die möglichen Einsparungen durch die elektronische Abwicklung drastisch reduzieren oder gar zunichte machen. Ohne „Massensignatur“, also automatisiertes Erzeugen qualifizierter elektronischer Signaturen, rechnet es sich nicht.

Das Signaturgesetz benennt die automatisierte Signaturerstellung nicht explizit, verbietet sie aber auch nicht; insgesamt ist die Nutzung des Signaturschlüssels durch den Signaturschlüssel-Inhaber nicht Gegenstand des SigG. Die Begründung zu § 15 der Signaturverordnung (SigV) nimmt jedoch Bezug auf die automatisierte Signaturerstellung: „Insbesondere bei der automatischen Erzeugung von Signaturen (Massensignaturen) muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck ... und durch eine zuvor *geprüfte und abgenommene Anwendung* vorgenommen werden können.“ [2]

### Rechtliches

§ 15 Abs. 2 SigV spezifiziert die Anforderungen an Signaturanwendungskomponenten und gibt sicherheitstechnische Hinweise, damit eine Signatur nur durch die berechtigte Person erzeugt werden kann und nur über die Daten erzeugt wird, welche diese Person signieren will. Es handelt sich also um Maßnahmen, die den Signaturschlüssel-Inhaber vor dem Missbrauch seines Signaturschlüssels schützen sollen. Welche Art von „Prüfung und Abnahme“ in der Begründung gemeint ist, bleibt an dieser Stelle allerdings unklar. Die Formulierung könnte vermuten lassen, dass hier auf § 15 Abs. 7 SigG Bezug genommen wird, wonach Produkte für qualifizierte elektronische Signaturen bei der freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern „geprüft und ... bestätigt“ sein müssen.

Bei näherer Betrachtung zeigen sich jedoch Widersprüche zu anderen SigG-Paragraphen und der Begründung des ursprünglichen Regierungsentwurfs, die klar aussagt, dass die Nutzung „geeigneter Signaturanwendungskomponenten in das Ermessen des Signaturschlüssel-Inhabers gestellt bleibt“ und dass „die Verwendung von geeigneten Signaturanwendungskomponenten nicht Voraussetzung für die Erzeugung einer qualifizierten elektronischen Signatur ist“.

Da somit keine Verpflichtung zur Nutzung bestimmter (z. B. geprüfter und bestätigter) Signaturanwendungskomponenten besteht, ist die Forderung bei den Massensignaturen vermutlich derart zu verstehen, dass deren Anwender durch eine (möglicherweise selbst definierte) Überprüfung und Abnahme sicherstellen soll, dass die eingesetzte Anwendung nur solche Daten sig-

niert, die sie auch signieren soll. Die zusätzliche Warnung trägt damit den höheren Gefahren bei der Massensignatur Rechnung.

Auch wenn kein Zwang zum Einsatz zertifizierter Lösungen besteht, sollte man sich gut überlegen, welche Komponenten man einsetzt, schon gar bei Massensignaturen. Die Begründung zu § 15 Abs. 2 SigV geht beispielsweise näher darauf ein, was der Gesetzgeber erwartet. Darin befinden sich auch Anhaltspunkte für Massensignaturen:

_____ Damit die Erzeugung einer Signatur nur durch die berechtigte Person erfolgen kann, dürfen bei der Aktivierung der Signaturerstellungseinheit die Identifikationsdaten (z. B. die PIN) beim Vergleich mit den auf der Signaturerstellungseinheit gespeicherten Referenzdaten nicht auslesbar oder speicherbar sein. Ihre Geheimhaltung ist zu jedem Zeitpunkt zu gewährleisten.

_____ Die Signaturkomponente darf nicht ohne Anwendung der Identifikationsdaten genutzt werden können, es sei denn, Signaturen sollen für ein festes Zeitfenster oder eine bestimmte Anzahl ohne jeweilige Identifizierung erzeugt werden. In diesem Falle ist sicherzustellen, dass Unberechtigte keine Signaturen veranlassen können.

_____ Die Erzeugung einer Signatur muss durch einen Warnhinweis vorher angezeigt werden. Insbesondere bei der automatischen Erzeugung von Signaturen („Massensignaturen") muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können.

## Sicherheit

Zudem fordert § 15 Abs. 4 SigV, dass „sicherheitstechnische Veränderungen an technischen Komponenten ... für den Nutzer erkennbar werden." Bezüglich der Beschränkung automatisierter Signaturen auf Zeitfenster oder eine vorgegebene Signaturzahl gibt im Übrigen die Regulierungsbehörde für Telekommunikation und Post (www.RegTP.de) zu bedenken (Frage 18 der FAQ, [3]):

_____ Trotz Verwendung dieser technischen Hilfsmittel werden die Erklärungen aus den signierten Dokumenten dem Absender zugerechnet. Daher sollte bei derartigen „automatisch" erstellten Signaturen immer ein besonderer Schutz gegen Missbrauch implementiert werden. Dieser Schutz sollte sich an dem Aktivierungszeitraum orientieren, was

## Zeitstempel statt Signatur?

Im Zusammenhang mit der Massensignatur kommt häufig auch die Frage auf, ob ein qualifizierter Zeitstempel unter Umständen eine qualifizierte Signatur ersetzen kann. Kann man nicht einfach die heute bereits existierenden, typischerweise hoch performant ausgelegten, Zeitstempelsysteme verwenden, um massenhaft Signaturen zu erstellen? Schon gar, wenn man bedenkt, dass sich ein erzeugter Zeitstempel bei manchen derzeit schon auf dem Markt befindlichen Produkten technisch nicht von einer Signatur unterscheidet: Es kann durchaus zwei Datensätze geben, deren Formate sich syntaktisch nicht voneinander unterscheiden, wovon der eine semantisch aber (zusätzlich mit einer Zeitinformation versehene) *signierte* Daten und der andere *mit einem Zeitstempel versehene* Daten darstellt.

Laut Signaturgesetz (SigG) ist qualifizierter Zeitstempel (§ 2 Nr. 14 SigG) lediglich „eine elektronische Bescheinigung eines Zertifizierungsdiensteanbieters ... darüber, dass ihm bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben." Ein qualifizierter Zeitstempel bestätigt also nicht, dass die darin enthaltenen Daten „korrekt" sind oder dass eine Person dem Inhalt dieser Daten zugestimmt hat. Jeder legitime Nutzer des Zeitstempeldienstes kann einen qualifizierten Zeitstempel an beliebige Daten anbringen lassen. Durch das Erstellen dieser Signatur ist demnach mitnichten eine „Unterschrift" im Sinne einer Willenserklärung erfolgt.

### Zeitdokumentation ist keine Willenserklärung

Der Zertifizierungsdiensteanbieter – präziser: die natürliche Person, für die das qualifizierte Zertifikat des Zeitstempeldienstes ausgestellt wurde – hätte ansonsten etwas „unterschrieben", dessen Inhalt er gar nicht kennt. Ein Zertifizierungsdiensteanbieter wird deshalb jeden qualifizierten Zeitstempel, den er ausstellt, deutlich als solchen kennzeichnen, um Missinterpretationen vorzubeugen. Üblicherweise enthält das zugehörige Zertifikat ein eindeutiges Pseudonym, welches den intendierten Zweck darlegt. Denkbar wäre auch, im Zertifikat ein spezielles Feld „Verwendungszweck" zu nutzen.

Technisch betrachtet bleibt es denkbar, geeignete existierende Produkte für qualifizierte Zeitstempel zur massenhaften qualifizierten elektronischen Signatur einzusetzen. Jedoch werden dann in der Regel darin Signaturkarten zum Einsatz kommen, die nicht für die Ausstellung qualifizierter Zeitstempel vorgesehen sind.

von einem verschlossenen Stahlschrank für Karte und Kartenleser, bis hin zur TrustCenter-Umgebung reichen kann.

Letztlich muss man vor allem der generellen Bedrohung des Missbrauchs eines Signatursystems entgegenwirken und durch geeignete Maßnahmen verhindern, dass ein Angreifer unlegitimierte Signaturen erstellen kann. Es ist dafür zu sorgen, dass das Signaturerstellungssystem selbst integer ist (ggf. durch Evaluierung) und zudem in einer vertrauenswürdigen Einsatzumgebung angewandt wird. So ist beispielsweise durch Zutrittskontrollanlagen, Benutzerauthentifizierung, Maßnahmen der Netzwerk- und Systemsicherheit (Netzsegmentierung, Firewall- und Intrusion-Detection-Systeme, Systemintegritäts- und Virenschutzmechanismen etc.) und nicht zuletzt organisatorische Maßnahmen für ein vertrauenswürdig betriebenes Gesamtsystem zu sorgen.

### Zertifizierungen

Signaturanwendungskomponenten mit einem von der RegTP vergebenen Gütesiegel genügen einer einheitlichen Spezifikation hinsichtlich der zu beachtenden Einsatzumgebung (s. [4]). Auch gemäß ITSEC oder Common Criteria (CC) geprüfte Komponenten müssen in der mitgelieferten Dokumentation Hinweise auf die korrekte und sichere Nutzung des Produktes enthalten. Da es sich dabei aber gegebenenfalls nur um Teilkomponenten des Datenerzeugungs- und Signaturprozesses handelt, müssen auch in diesem Fall, trotz der unabhängigen Prüfung, weitere Aspekte zum Schutz gegen Missbrauch betrachtet werden. Beispielsweise kann schon das System angreifbar sein, das die Daten zu dem zu signierenden Datensatz zusammenfügt.

Analog kann eine Manipulation auf dem Übertragungsweg von diesem System zur Signatur-Anwendung erfolgen. Denkbar wäre, dass die Signatur-Anwendung eine Plausibilitätsprüfung an den zu signierenden Daten durchführt, was jedoch auch nicht gegen alle möglichen Angriffe wirkt. Auch bei der Handhabung der eingesetzten Signaturkarten (und evtl. vorhandener Ersatzkarten) sind eine Reihe von Bedrohungen zu berücksichtigen.

### Grundschutz

Zur Befriedigung grundlegender Schutzbedürfnisse kann man die Vorgehensweise des IT-Grundschutzhandbuches (www.bsi. bund.de/gshb/) oder anderer Standards für Sicherheitsmanagementsysteme verwenden, um ein umfassendes Sicherheitskonzept zu erstellen. Obwohl durch die standardisierten Bedrohungen und Maßnahmen des IT-Grundschutzhandbuches auf ressourcenschonende Weise ein grundlegendes Sicherheitsniveau erreicht werden kann, besteht natürlich nicht die Garantie, dass die vorgeschlagenen Standardmaßnahmen auch wirklich angemessen sind.

Werden durch Massensignatur-Systeme potenziell sehr werthaltige Dokumente verarbeitet, sodass ein Missbrauch zu beträchtlichen Schäden führen oder gar existenzbedrohende Ausmaße annehmen kann, so empfiehlt sich zusätzlich die Anwendung der im IT-Sicherheitshandbuch des BSI [5] beschriebenen Methodik, wonach die IT-Grundschutzanalyse durch eine ausgefeiltere Bedrohungs- und Risikoanalyse ergänzt wird und bei der Erstellung des Sicherheitskonzeptes zusätzlich eine Abschätzung des Restrisikos durchzuführen ist.

Weiterhin kann eine Einschränkung des Wirkungsumfangs des genutzten qualifizierten Zertifikates

## Literatur

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, 2001-05-16, BGBl. 2001 Teil I Nr. 22, S. 876, etwa auf www.iid.de/iukdg/gesetz/SigAendG2.pdf

[2] Begründung zur Signatur-Verordnung, etwa auf www.iid.de/iukdg/aktuelles/begr_verordnung.pdf

[3] Regulierungsbehörde für Telekommunikation und Post (RegTP), Frequently Asked Questions, www.regtp.de/tech_reg_tele/start/in_06-02-03-00-00_m/index.html

[4] RegTP, Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten, www.regtp.de/imperia/md/content/tech_reg_t/digisign/118.pdf

[5] BSI (Hrsg.), IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, Bundesdruckerei, Bonn 1992, Bezugsinformationen per Telefon 0228 382020

[6] C. Pavlovski, C. Boyd, Efficient Batch Signature Generation using Tree Structures, International Workshop on Cryptographic Techniques and E-Commerce, CrypTEC'99, City University of Hong Kong Press, S. 70, etwa auf http://sky.fit.qut.edu.au/~boydc/papers/treefinal.ps

[7] A. Bovenschulte, M. Eifert, Rechtsfragen der Anwendung technischer Produkte nach Signaturgesetz, DuD 2/2002

[8] G. Bröhl, A. Tettenborn, Das neue Recht der elektronischen Signaturen: kommentierende Darstellung von Signaturgesetz und Signaturverordnung, Bundesanzeiger-Verlag, Bonn 2001, ISBN 3-89817-045-4

durch geeignete Attribute und Beschränkungen im Zertifikat zum Einsatz kommen, was jedoch nicht präventiv wirkt. Zurzeit sind solche Attribute und Beschränkungen jedoch nur unvollständig standardisiert und werden zudem nicht von jedem Zertifizierungsdiensteanbieter angeboten.

## Performance

Ein weiteres Problemfeld bei Systemen zur Massensignatur sind Aspekte der performanten Realisierung. Muss die Lösung eine große Anzahl an Signaturen in kurzer Zeit erzeugen können, so existieren hierfür grundsätzlich verschiedene Möglichkeiten:

### Leistungsfähigere Signaturerstellungseinheiten

An die Stelle einer Chipkarte, wie sie heute typischerweise zur Signatur eingesetzt wird, könnte ein leistungsfähigeres Hardware-Sicherheits-Modul (HSM) treten. Da das SigG bei qualifizierten elektronischen Signaturen aber neben der Verwendung eines qualifizierten Zertifikates auch den Einsatz einer sicheren Signaturerstellungseinheit fordert (§ 2 Nr. 10 SigG), sind die entsprechenden Anforderungen aus SigG und SigV zu beachten (§ 17 oder § 23 SigG).

Gemäß Anlage 1 zur SigV sind sichere Signaturerstellungseinheiten beispielsweise gemäß ITSEC E3 hoch oder EAL4 zu prüfen (letzteres einschließlich der Prüfung gegen hohes Angriffspotenzial und einer vollständigen Missbrauchsanalyse) und zwingend von einer zugelassenen Stelle zu „bestätigen" (§ 18 SigG). Derzeit können lediglich Chipkarten eine solche Prüfung und Bestätigung vorweisen.

### Parallelisierung

Eine einfache, und in der Praxis häufig eingesetzte, Methode zur Steigerung des Durchsatzes von Signatursystemen besteht in der naiven Parallelisierung: Statt einer Chipkarte werden mehrere parallel betrieben, die Signatur-Anwendungssoftware verteilt die zu signierenden Daten auf die parallel angeordneten Chipkarten. Dieses Szenario stellt allerdings besondere Anforderungen an die Leistungsfähigkeit und Zuverlässigkeit der Serverkomponente. Unterstellt man, dass eine ideale Parallelisierung möglich ist und die Erstellung einer Signatur (inklusive Kommunikation) etwa eine Sekunde dauert, dann kann täglich die in Tabelle 1 aufgeführte Anzahl an Signaturen erstellt werden.

| Anzahl parallel arbeitender Chipkarten | Anzahl möglicher Signaturen pro Tag |
|---|---|
| 1 | 86 400 |
| 5 | 432 000 |
| 10 | 864 000 |
| 15 | 1 296 000 |
| 20 | 1 728 000 |
| 50 | 4 320 000 |
| 100 | 8 640 000 |

*Tabelle 1: Anzahl möglicher Signaturen pro Tag bei parallelem Betrieb mehrerer Chipkarten (ideale Parallelisierung bei 1 Sek. Signaturzeit vorausgesetzt)*

### Stapelsignaturen

Ist auch die durch Parallelisierung erreichbare Leistungsfähigkeit nicht ausreichend, so bleiben im Prinzip noch algorithmische Optimierungen und Stapelverarbeitungsstrategien. Da die mathematische Signaturerzeugung (Errechnen der Signatur unter Verwendung des geheimen Schlüssels und des Hashwertes der Nachricht) auf einer Chipkarte durchgeführt wird, scheiden algorithmische Optimierungen jedoch aus.

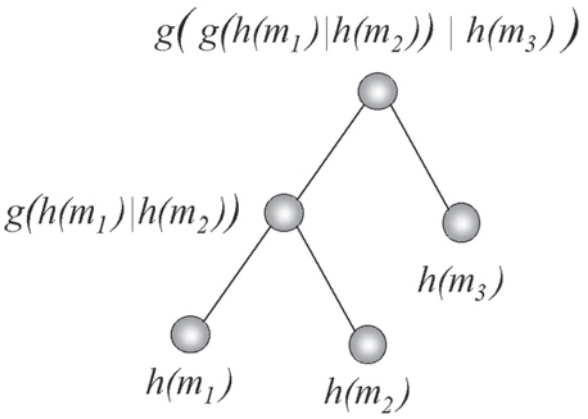


*Abbildung 1: Baumartig aufgebaute Hashketten. Sofern die beiden verwendeten Hashfunktionen g und h kollisionsresistent sind, lässt sich zeigen, dass eine Stapelsignatur der Wurzel eine gleichermaßen sichere Signatur liefert wie gewöhnliche Signaturen über alle „Blätter" des Hash-Baumes [6].*

Denkbar wäre es, durch die Bildung von baumartig aufgebauten Hashketten mittels einer mathematischen Signaturerzeugung (Signatur der Wurzel, vgl. Abb. 1) einen ganzen „Stapel" von Hashwerten (alle Blätter) gleichzeitig zu signieren (wie beispielsweise in [6] oder unabhängig davon durch Brandner/Pordesch auf der ISSE 2002 vorgeschlagen). Während dieser Ansatz theoretisch sehr ansprechend ist, spricht doch das Fehlen entsprechender Standards derzeit gegen eine entsprechende Umsetzung, sodass derartige Stapelsignaturen im Moment noch Zukunftsmusik sind. ■

*Detlef Hühnlein (detlef.huehnlein@secunet.com) und Yvonne Knosowski (yvonne.knosowski@secunet.com) sind Senior Consultants bei der secunet Security Networks AG.*