Rechtliche Rahmenbedingungen der „Komfortsignatur“

Detlef Hühnlein

secunet Security Networks AG
Sudetenstrasse 16
D-96247 Michelau

Zusammenfassung

Diese Arbeit beleuchtet die rechtlichen Rahmenbedingungen der „Komfortsignatur“ in Deutschland, bei der die Identifikation des Signaturschlüsselinhabers (z.B. mit einer PIN) und individuelle Willenserklärung (z.B. durch Erfassen eines Fingerabdrucks) voneinander entkoppelt sind, so dass qualifizierte elektronische Signaturen für häufig wiederkehrende Geschäftsvorfälle (z.B. Signatur von elektronischen Rezepten im Gesundheitswesen) in einer komfortablen Art und Weise erstellt werden können. Die Betrachtung der rechtlichen Rahmenbedingungen und der daraus resultierenden Prüfungsanforderungen zeigen, dass es grundsätzlich möglich ist, „Komfortsignatur“-Systeme im Einklang mit den Anforderungen des Signaturgesetzes und der Signaturverordnung zu gestalten.

1 Einleitung

Im Zuge der Einführung der elektronischen Gesundheitskarte müssen Leistungserbringer (z.B. Ärzte, Apotheker) im Gesundheitswesen künftig in verschiedenen Geschäftsprozessen qualifizierte elektronische Signaturen erzeugen und prüfen. Beispielsweise muss ein Arzt eine elektronische Verschreibung von Arzneimitteln (eRezept) gemäß § 2 Abs. 1 Nr. 10 AMVV mit einer qualifizierten elektronischen Signatur gemäß Signaturgesetz (§ 2 Nr. 3 SigG) versehen. Umgekehrt leitet sich die Pflicht zur Prüfung dieser Signatur bei der Dispensierung[1] der Verordnung aus § 17 Abs. 5 Satz 2 ApBetrO ab. Da für die Erzeugung einer qualifizierten elektronischen Signatur im Regelfall die Eingabe einer sechsstelligen PIN nötig ist (vgl. Abschnitt 2.1), wird eine starke Beeinträchtigung der Abläufe in der Praxis durch die Erstellung von qualifizierten elektronischen Signaturen für elektronische Rezepte befürchtet[2].

[1] Für die Dispensierung des Arzneimittels in der Apotheke ist gemäß § 17 Abs. 6 Nr. 2 ApBetrO *keine* eigenhändige Unterschrift bzw. qualifizierte elektronische Signatur nötig. Es genügt vielmehr das Hinzufügen eines Namenszeichen bzw. einer elektronischen Signatur gemäß § 2 Nr. 1 SigG, wobei „der Apothekenleiter die Rückverfolgbarkeit zum jeweiligen Unterzeichner und deren Dokumentation sicherzustellen hat“. Gemäß § 22 Abs. 1 Satz 3 ApBetrO dürfen an der Dokumentation „keine Veränderungen vorgenommen werden, die nicht erkennen lassen, ob sie bei oder nach der ursprünglichen Eintragung vorgenommen worden sind.“

[2] Beispielsweise äußerte sich kürzlich ein Vertreter der Ärzteschaft [ÄZO06] wie folgt: "Jetzt unterschreibt ein Arzt die Rezepte schnell mal am Tresen, das geht zack-zack. In Zukunft muss er für jedes Rezept eine sechsstellige PIN eingeben. […] Wenn das bei der flächendeckenden Einführung der Karte immer noch so ist, dann ist das elektronische Rezept tot."

P. Horster (Hrsg.) ·DACH Security (2007) pp.

Als mögliche Alternative für die jeweilige Eingabe der sechsstelligen PIN für jedes Rezept wurde das in Abbildung 1 dargestellte Verfahren zur „Komfortsignatur“ diskutiert (vgl. [KiSc06]). Hierbei wird in einem ersten Schritt die sichere Signaturerstellungseinheit in einer sicheren Umgebung gesteckt und durch die Eingabe der PIN für die generelle Nutzung aktiviert. Jede individuelle Signatur (Schritt 2 bis n) wird nun durch zusätzliche Mechanismen, wie z.B. biometrische Verfahren, ein RFID-Token oder einfach eine kürzere (z.B. vierstellige) PIN ausgelöst. Aktuell wird darüber diskutiert, ob ein solches Verfahren grundsätzlich konform zu den rechtlichen Rahmenbedingungen des deutschen Signaturgesetzes und der Signaturverordnung sein kann und wie eine Realisierung der „Komfortsignatur“ im Detail aussehen müsste.

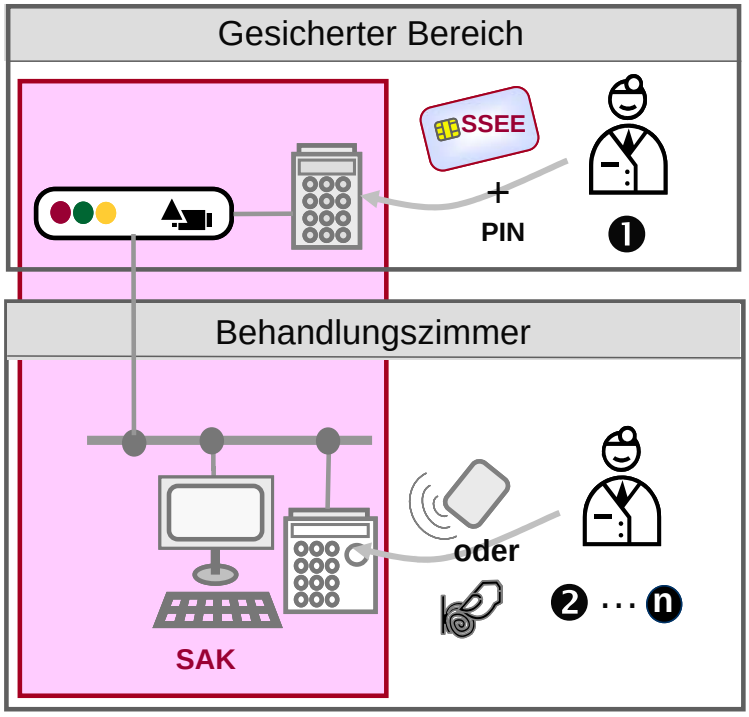

Abbildung 1: "Komfortsignatur"-System

Diese Arbeit trägt die rechtlichen Rahmenbedingungen der „Komfortsignatur“ zusammen und beleuchtet einige daraus resultierende technische und organisatorische Aspekte einer möglichen Realisierung und Prüfung.

An der Erzeugung von qualifizierten elektronischen Signaturen sind sichere Signaturerstellungseinheiten (SSEE) gemäß § 2 Nr. 10 SigG und Signaturanwendungskomponenten (SAK) gemäß § 2 Nr. 11 SigG beteiligt. Deshalb werden in den Abschnitten 2 und 3 die für die „Komfortsignatur“ relevanten rechtlichen Rahmenbedingungen für diese Komponenten zusammengetragen, um zu untersuchen, ob die Realisierung eines solchen Systems im Einklang mit den Vorgaben der deutschen Signaturgesetzgebung möglich ist. In Abschnitt 4 werden schließlich die wesentlichen Ergebnisse dieser Arbeit zusammengefasst.

2 Sichere Signaturerstellungseinheiten

Gemäß § 2 Nr. 10 SigG sind „’sichere Signaturerstellungseinheiten’ Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die min-

destens die Anforderungen nach § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung gemäß § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind“.

Für die Erzeugung von qualifizierten elektronischen Signaturen sind gemäß § 17 Abs. 1 Satz 1 SigG „sichere Signaturerstellungseinheiten einzusetzen, die […] *gegen unberechtigte Nutzung der Signaturschlüssel schützen.*“ Diese grundsätzliche Anforderung wird durch § 17 Abs. 1 SigV folgendermaßen präzisiert: „Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch *Besitz und Wissen* oder durch *Besitz und ein oder mehrere biometrische Merkmale* angewendet werden kann.“

Für die Identifikation des Signaturschlüsselinhabers gegenüber der sicheren Signaturerstellungseinheit sind drei grundsätzliche Möglichkeiten zu unterscheiden:

- Identifikation durch Besitz und Wissen
- Identifikation durch Besitz und Biometrie
- Identifikation durch Besitz und Wissen und zusätzlicher Biometrie

Bei all diesen Varianten muss der Signaturschlüsselinhaber also im Besitz der sicheren Signaturerstellungseinheit sein. Gemäß § 854 Abs. 1 BGB wird der Besitz einer Sache „durch die Erlangung der tatsächlichen Gewalt über die Sache erworben.“ Daraus und aus der Definition der fortgeschrittenen elektronischen Signatur in § 2 Nr. 2 c) SigG leitet sich ab, dass der Signaturschlüsselinhaber die sichere Signaturerstellungseinheit unter seiner alleinigen Kontrolle halten muss. Dies bedeutet allerdings nicht, dass er die Signaturkarte bei sich tragen muss, sondern es wäre auch denkbar, dass die Karte – wie in Abbildung 1 angedeutet - an einem nur für ihn zugänglichen Ort gesteckt ist und der Zugriff auf die Karte durch weitere technische und organisatorische Maßnahmen geschützt ist.

2.1 Identifikation durch Besitz und Wissen

Neben dem Besitz der Karte erfolgt die Identifikation des Signaturschlüsselinhabers in diesem Fall durch Wissen, d.h. durch die Kenntnis seiner persönlichen Identifikationsdaten. Gemäß § 15 Abs. 2 Nr. 1 a) SigV müssen Signaturanwendungskomponenten (siehe auch Abschnitt 3) gewährleisten, dass „die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden“. Als Identifikationsdaten können dezimale Personal Identification Numbers (PIN) oder beliebige aus ASCII-Zeichen bestehende Passwörter dienen. Wie lang eine PIN oder ein Passwort mindestens sein muss, leitet sich aus der in der Signaturverordnung geforderten Stärke der Sicherheitsfunktionen ab.

Gemäß Anlage 1 I. 1.1. b) SigV muss die Prüfung der sicheren Signaturerstellungseinheiten mindestens die Prüftiefe [CC] *EAL 4* oder [ITSEC] *E 3* umfassen. Außerdem werden in Abschnitt I. 1.2. der Anlage die Anforderung bzgl. der Schwachstellenbewertung und der Mechanismenstärke dahingehend präzisiert, dass bei der Prüfung gemäß [ITSEC] die Mechanismenstärke *„hoch“* sein muss und bei [CC] zusätzlich zur hohen Stärke der EVG-Sicherheitsfunktionen (AVA_SOF) „gegen ein *hohes Angriffspotenzial* zu prüfen und eine *vollständige Missbrauchsanalyse* durchzuführen“ ist. Wie in der amtlichen Begründung [SigVBeg] zu § 11 Abs. 3 SigV erläutert, bedeutet das, dass bei der Prüfung der sicheren Signaturerstellungseinheiten neben den Anforderungen aus EAL 4 zusätzlich die aus EAL 6 ent-

liehenen Vertrauenswürdigkeitskomponenten AVA_VLA.4 (Hohe Widerstandsfähigkeit) und AVA_MSU.3 (Analysieren und Testen auf unsichere Zustände) gefordert sind.

Die hohe Stärke der EVG-Sicherheitsfunktionen (SOF-hoch) ist in [CC] Abschnitt 2.3 dadurch definiert, dass „die Analyse zeigt, dass die Funktionen einen geeigneten Schutz gegen geplantes oder organisiertes Brechen der EVG-Sicherheit durch Angreifer bieten, die über ein hohes Angriffspotential verfügen.“ Nach Table B.2 (Anhang B.8) geht man bei einer Stärke der EVG-Sicherheitsfunktionen von SOF-hoch davon aus, dass ein erfolgreicher Angriff in der Praxis nicht durchführbar ist („successful attack beyond practicality“). Vor diesem Hintergrund legte man unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik bei der Erstellung des Maßnahmenkatalogs für das erste deutsche Signaturgesetz im Jahr 1997 [BSI97] (vgl. Maßnahme M-Chip 7.1, Identifizierung und Authentifizierung des Benutzers, Seite 244) fest, dass eine hohe Stärke der EVG-Sicherheitsfunktionen (bzw. Stärke der Sicherheitsmechanismen gemäß [ITSEC]) den Einsatz einer 6-stelligen PIN mit einem Fehlbedienungszähler von 3 und einer mindestens 8-stelligen PUK erforderlich macht. Auch wenn dieser Maßnahmenkatalog durch die Novellierung des Signaturgesetzes streng genommen nicht mehr verbindlich ist, so fußt die heutige Bestätigungspraxis bzgl. der Frage der notwendigen PIN-Länge immer noch auf der damaligen Festlegung. Darüber hinaus sind jedoch auch alternative Verfahren denkbar, durch die eine unbefugte Nutzung des Signaturschlüssels gewährleistet ist, sofern im Zuge der Evaluierung der Nachweis der Stärke der EVG-Sicherheitsfunktionen durch das in [CEM] Anhang B.8 erläuterte Verfahren erbracht wird.

Die Identifikation durch Besitz und Wissen ist der heute in der Praxis gebräuchliche Fall – *alle* existierenden sicheren Signaturerstellungseinheiten (vgl. [BNAProd]) nutzen zur Identifikation des Signaturschlüsselinhabers entsprechende PINs (bzw. ASCII-Passworte).

Zur Frage, ob die PIN für jede zu erstellende Signatur eingegeben werden, muss führt die amtliche Begründung [SigVBeg] zu § 15 Abs. 1 SigV im vierten Absatz folgendes aus:

„Sichere Signaturanwendungskomponenten können so gestaltet werden, dass optional vor jeder Signatur, nach einer zuvor festgelegten Anzahl von Signaturen oder nach bestimmtem Zeitablauf bei Nichtbenutzung der Signaturerstellungseinheit die Identifikationsdaten erneut eingegeben werden müssen. Es liegt im *Ermessen des Nutzers,* wie er – *abhängig von seinem individuellen Bedarf und der Anwendungsumgebung* – verfährt. Im Regelfall sollte vor jeder neuen Signatur auch eine erneute Identifikation erfolgen, oder es sollte nur ein kurzes ‚Zeitfenster’ geöffnet bleiben, innerhalb dessen weitere Signaturen möglich sind.“

Hieraus - wie auch aus den Betrachtungen zur Signaturanwendungskomponente in Abschnitt 3 - geht hervor, dass es im Sinne des Verordnungsgebers ist, dass ein Nutzer - abhängig von seinem individuellen Bedarf und der Anwendungsumgebung - mit einer Eingabe der PIN auch mehrere Signaturen erzeugen und die Signaturerstellungseinheit für einen bestimmten Zeitraum für die Erstellung von Signaturen aktivieren kann. Außerdem erscheint es erwähnenswert, dass der Verordnungsgeber davon ausgeht, dass die Deaktivierung der Signaturerstellungseinheit nach einer bestimmten Anzahl erstellter Signaturen oder nach einer bestimmten Zeit durch die Signaturanwendungskomponente – also nicht zwingend durch die sichere Signaturerstellungseinheit selbst – geschieht. Demzufolge ist die Existenz von sicheren Signaturerstellungseinheiten, die nach einer einmaligen Identifikation technisch dazu in der Lage sind eine unbegrenzte Anzahl an Signaturen erstellen zu können durchaus im Sinne des Verordnungsgebers.

Betrachtet man die Bestätigungsurkunden der sicheren Signaturerstellungseinheiten näher (vgl. [BNAProd]), so ist ersichtlich, dass auch eine Reihe von sicheren Signaturerstellungseinheiten existieren, die eine solche „Massensignatur-Fähigkeit“ besitzen. Etwa die Hälfte aller heute existierenden sicheren Signaturerstellungseinheiten kann – z. T. mit zusätzlichen Bedingungen an das Auslieferungsverfahren und die Einsatzumgebung – in einer Massensignatur-fähigen Konfiguration betrieben werden. Die individuellen Anforderungen hierzu sind in der jeweiligen Bestätigungsurkunde aufgeführt.

Während die Ausgabe solcher Karten an gewöhnliche Signaturschlüsselinhaber - außerhalb von besonders geschützten Trust Center Umgebungen – teilweise mit besonderen Auflagen (persönliche Übergabe, ausführliche Unterrichtung zu spezifischen Risiken der Massensignatur etc.) verbunden oder gar in der Bestätigung ausgeschlossen ist, so ist die generelle Existenz von Massensignatur-Karten, die zur Komfortsignatur eingesetzt werden können, nicht nur im Sinne des Verordnungsgebers, sondern auch in der Praxis gegeben.

In der Spezifikation des elektronischen Heilberufsausweises ist die für die Komfortsignatur notwendige Massensignatur-Fähigkeit bereits berücksichtigt (vgl. [HBA-1], Seite 17):

„For the usage of the private key for qualified electronic signatures, a ‘security status evaluation counter’ shall be supported, i.e. it shall be possible to configure that

- each time or
- after n times (n in the range 1 ... 254) or
- only once

before using the private signature key a user verification with PIN.QES is required during a session. The initial value of this ‘security status evaluation counter’ will be fixed during personalization. The security status evaluation counter and its initial value is related to objects like a private key, but refers to the PIN management.”

Das Schutzprofil [HBA-PP] umfasst nicht die Funktionalität für die Nutzung des Heilberufsausweises als sichere Signaturerstellungseinheit. Da auch die Schutzprofile für sichere Signaturerstellungseinheiten [SSCD-PP] nicht näher auf Aspekte der Massensignatur-fähigen Personalisierung eingehen, können die detaillierten Anforderungen an den Ausgabeprozess und der Einsatzumgebung – unter Berücksichtigung der sonstigen Rahmenbedingungen aus dem Signaturgesetz und der Signaturverordnung - vollständig im Rahmen der Bestätigung durch eine Stelle gemäß § 18 SigG in Abstimmung mit der Bundesnetzagentur als zuständiger Behörde gestaltet werden.

2.2 Identifikation durch Besitz und Biometrie

Gemäß § 15 Abs. 1 Satz 1 SigV kann die Identifikation des Signaturschlüsselinhabers auch durch „Besitz und ein oder mehrere biometrische Merkmale“ erfolgen. Allerdings gibt § 15 Abs. 1 Satz SigV hierzu folgendes zu bedenken: „Bei Nutzung biometrischer Merkmale muss hinreichend sichergestellt sein, dass eine *unbefugte Nutzung des Signaturschlüssels ausgeschlossen* ist und eine dem wissensbasierten Verfahren *gleichwertige Sicherheit* gegeben sein.“ Somit muss auch in diesem Fall eine hohe Stärke der Sicherheitsfunktionen erreicht werden.

Die folgenden Angaben aus [BEM] (Table 11) können hier als Anhaltspunkt[3] dienen:

Stärke der EVG-Sicherheits-funktionen	Maximale False Acceptance Rate (FAR)
SoF-niedrig	0.01 (1 von 100)
SoF-mittel	0.0001 (1 von 10.000)
SoF-hoch	0.000001 (1 von 1000.000)

Tabelle 1: SoF und FAR

Demnach müsste zum Erreichen einer hohen Stärke der EVG-Sicherheitsfunktionen eine False Acceptance Rate von etwa 1 zu einer Million erreicht werden. Um dies im Rahmen einer Evaluation mit einer Sicherheit von 95 % nachweisen zu können, dürfte bei rund 3 Millionen Stichproben kein einziger Fehler auftreten. Wohl insbesondere aus diesem Grund gibt es bislang kein Produkt, das eine [CC]-Evaluierung mit der notwendigen Stärke der EVG-Sicherheitsfunktionen vorweisen kann. Insbesondere existiert also derzeit auch keine sichere Signaturerstellungseinheit, die die Anforderung des Signaturgesetzes *allein* mit biometrischen Mitteln erfüllen würde.

2.3 Identifikation durch Besitz und Wissen und Biometrie

Neben der oben erläuterten Identifikation des Signaturschlüsselinhabers durch Besitz und Wissen oder Besitz und Biometrie ist auch eine Kombination der beiden Verfahren möglich. Wie in Anlage 1 I 1.2 Satz 3 SigV erläutert, „genügt für den Mechanismus zur Identifikation durch biometrische Merkmale eine Bewertung der Sicherheitsmechanismen mit *‚mittel’*, wenn diese *zusätzlich* zur Identifikation durch Wissensdaten genutzt werden.“

Unklar bleibt hier, ob es ausreichend ist, dass die Identifikation durch Wissensdaten für sich genommen bereits die Mechanismenstärke „hoch“ erreichen muss, also eine sechsstellige PIN nötig ist, oder ob durch die Kombination mit dem biometrischen Verfahren, das für sich betrachtet eine mittlere Mechanismenstärke erreichen muss, auch eine kürzere PIN denkbar wäre.

Für den praktischen Einsatz ist aber auch dieses Verfahren derzeit nur bedingt geeignet, da es derzeit scheinbar auch keine gemäß [ITSEC] oder [CC] evaluierten biometrischen Produkte gibt, für die eine mittlere Mechanismenstärke nachgewiesen werden konnte.

Allerdings scheint ein solcher Nachweis unter statistischen Gesichtspunkten nicht grundsätzlich unmöglich zu sein. Insbesondere wenn bei der Evaluation das in [BEM] erläuterte Verfahren der sog. „Cross Comparison“, bei dem jedes Testmuster mit allen gespeicherten Ver-

[3] Die Zuordnung zwischen der Stärke der EVG-Sicherheitsfunktionen und der False Acceptance Rate ist nicht verbindlich geregelt. Rz. 75 in [BEM] führt hierzu folgendes aus: „*Strength of Function (SOF) is an important part of the evaluation of a biometric device. It is related to False Accept Rate (FAR), but the correspondence between FAR and SOF is not simple or clearly defined.*“

gleichsmuster konfrontiert wird, verwendet werden kann, so könnten die mindestens notwendigen 30.000[4] Testmuster bereits mit rund 250[5] Probanden generiert werden.

3 Signaturanwendungskomponenten

„Signaturanwendungskomponenten“ sind in § 2 Nr. 11 SigG definiert als „Software- und Hardwareprodukte, die dazu bestimmt sind,

a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder

b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen“.

Aus dem Signaturgesetz erwächst für eine Signaturanwendungskomponente im Hinblick auf die „Komfortsignatur“ also insbesondere die Anforderung die *zu signierenden Daten der Erzeugung der Signatur* in der sicheren Signaturerstellungseinheit *zuzuführen*.

Weitere Anforderungen sind in § 17 Abs. 2 SigG definiert:

„Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. auf welche Daten sich die Signatur bezieht,
2. ob die signierten Daten unverändert sind,
3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.

Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.“

Im Kontext der „Komfortsignatur“ muss die Signaturanwendungskomponente also insbesondere *klar erkennbar machen, dass eine Signatur erzeugt werden soll.*

Die Begründung [SigGBeg] zu § 17 Abs. 2 SigG stellt weiterhin klar, dass mit dieser Vorschrift Anhang IV der Richtlinie [EGSRL] umgesetzt wird. Da es sich hierbei nur um eine Empfehlung handelt, ist dieser Anhang „zwar nicht verbindlich umzusetzen, eine Umsetzung

[4] Tritt bei rund 30.000 unabhängigen Testmustern *kein* Fehler auf, so kann mit einer Sicherheit von 95 % geschlossen werden, dass die FAR kleiner als 10^{-4} ist, womit eine mittlere Mechanismenstärke nachgewiesen wäre.

[5] Unterstellt man, dass man mit 250 zufällig gewählten Testpersonen beim jeweiligen Vergleich der aktuellen Testmuster mit allen gespeicherten Vergleichsmustern (250·249)/2= 31125 weitgehend unabhängige Kombinationen erhält, so könnte der Nachweis der mittleren Mechanismenstärke im Idealfall bereits mit rund 250 Testpersonen durchgeführt werden.

ist jedoch nach Artikel 3 Abs. 6 [EGSRL] ausdrücklich erwünscht, um die Entwicklung und die Nutzung von Signaturprüfeinheiten zu fördern. Die Vorschrift nimmt darüber hinaus eine Präzisierung dahingehend vor, dass alle bei Anwendung (Erzeugung oder Prüfung) qualifizierter elektronischer Signaturen relevanten Sicherheitsaspekte erfasst werden.“

Weiterhin wird in der Begründung klargestellt, dass der Einsatz geeigneter Signaturanwendungskomponenten im Ermessen des Signaturschlüssel-Inhabers liegt:

„Die Nutzung geeigneter Signaturanwendungskomponenten bleibt in das *Ermessen der Signaturschlüssel-Inhaber* gestellt. Unabhängig davon wird mit Satz 2 die Notwendigkeit zum Einsatz geeigneter Signaturanwendungskomponenten unterstrichen. Mit der Formulierung ‚soll’ in Satz 3 wird im Hinblick auf die Richtlinie und unterschiedlichen Auslegungsmöglichkeiten des Signaturgesetzes zugleich klargestellt, dass die Verwendung von geeigneten Signaturanwendungskomponenten nicht Voraussetzung für die Erzeugung einer qualifizierten elektronischen Signatur ist. Dies ergibt sich schon daraus, dass aus einer elektronischen Signatur nicht ersichtlich ist, welche Signaturanwendungskomponente bei ihrer Erzeugung zum Einsatz kam. Hinzu kommt, dass im Einzelfall auch ‚andere geeignete Maßnahmen’ (z.B. PC oder Laptop unter ständiger Kontrolle und ohne Anschluss an ein Kommunikationsnetz) ausreichend Sicherheit bieten können.“

Hierdurch verdeutlicht der Gesetzgeber (siehe auch [BrTe01] und [BoEi02]), dass bei der Realisierung von „gesetzeskonformen“ Signaturanwendungskomponenten ein gewisser Handlungsspielraum existiert. Insbesondere ist die Abgrenzung zwischen dem Evaluationsgegenstand (EVG) der Signaturanwendungskomponente, bei der die Prüfungsanforderungen aus Anlage 1 der Signaturverordnung zu beachten sind (z.B. [CC] EAL 3 +[6]), und deren Einsatzumgebung *nicht* klar definiert. Demnach würde selbst ein „Komfortsignatur“-System, bei dem die Freischaltung der sicheren Signaturerstellungseinheit *innerhalb* des EVG geschieht, die Willenserklärung für die Erstellung der Signatur aber mittels Biometrie, Besitz eines RFID-Tokens o.ä. *außerhalb* des EVGs der Signaturanwendungskomponente bzw. der sicheren Signaturerstellungseinheit realisiert wird, *nicht* gegen verbindliche Anforderungen des Signaturgesetzes verstoßen.

Allerdings verdeutlicht der Wortlaut der Begründung auch, dass im Evaluationsgegenstand der Signaturanwendungskomponente „alle bei Anwendung (Erzeugung oder Prüfung) qualifizierter elektronischer Signaturen relevanten Sicherheitsaspekte erfasst werden“ sollen. Demnach sollte auch der – zweifellos sicherheitsrelevante - Akt der Willensbekundung Teil des Evaluationsgegenstands sein und demnach einem Angreifer mit hohem Angriffspotenzial widerstehen. Kommen hierbei zusätzlich zur Identifikation durch Wissensdaten biometrische Mechanismen zum Einsatz, so ist für diese mindestens eine mittlere Stärke der Sicherheitsfunktionen nachzuweisen (vgl. Abschnitt 2.3).

Ein „Komfortsignatur“-freundliches Schutzprofil für eine Signaturanwendungskomponente könnte demnach so gestaltet sein, dass es eine Trennung der Identifikation durch Besitz und Wissen und der späteren Willenserklärung grundsätzlich ermöglicht und es dem Hersteller bei

[6] Wie bei den in Abschnitt 2 betrachteten sicheren Signaturerstellungseinheiten müssen bei einer Prüfung gemäß [CC] die aus EAL 6 entliehenen Vertrauenswürdigkeitskomponenten AVA_MSU.3 und AVA_VLA.4 berücksichtigt werden. Außerdem sind hier die durch die Abhängigkeit mit AVA_VLA.4 resultierenden Komponenten ADV_IMP.1 und ADV_LLD.1 aus EAL 4 zu beachten.

Bedarf überlässt im Rahmen der Evaluation nachzuweisen, dass der Akt der Willenserklärung einem Angreifer mit hohem Angriffspotenzial widersteht.

§15 Abs. 2 und Abs. 4 SigV machen weitere Angaben zu den Anforderungen an Signaturanwendungskomponenten:

„(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur
   a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
   b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
   c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
2. bei der Prüfung einer qualifizierten elektronischen Signatur
   a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
   b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“

Für die „Komfortsignatur“ sind hier insbesondere die Anforderungen in Nr. 1 bedeutsam. Die Begründung [SigVBeg] zu §15 Abs. 2 SigV geht nun näher darauf ein, was dies im Einzelnen bedeutet:

„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 (Nummer 1 Buchst. a)). 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* (Nummer 1 Buchst. b)). Die Erzeugung einer Signatur muss durch einen *Warnhinweis* vorher angezeigt werden (Nummer 1 Buchst. c)). 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.“.

Demnach ist es im Sinne des Verordnungsgebers, dass der Signaturschlüssel-Inhaber die sichere Signaturerstellungseinheit durch einmalige Eingabe der Identifikationsdaten „für ein festes Zeitfenster oder eine bestimmte Anzahl“ an Signaturen aktiviert. Allerdings ist in diesem Fall anderweitig sicherzustellen, dass „Unberechtigte keine Signaturen veranlassen können“. Sofern die dafür notwendige Funktionalität Teil des Evaluationsgegenstandes ist, ist hierbei die Widerstandsfähigkeit gegen einen Angreifer mit hohem Angriffspotenzial nachzuweisen. Außerdem muss „die Erzeugung einer Signatur durch einen Warnhinweis vorher angezeigt werden“. Im Kontext der Komfortsignatur impliziert dies, dass die generelle Aktivierung der sicheren Signaturerstellungseinheit mit einem deutlichen Warnhinweis versehen

sein sollte und auch das Auslösen der jeweiligen Signaturerzeugung ein willentlicher Akt sein sollte.

Ähnlich wie bei der Massensignatur (vgl. [HüKn03], [RoFD03]) sollte „sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck“ (z. B. nur Signatur von gewöhnlichen[7] elektronischen Rezepten) „und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können.“ Demnach können auch hier weitere organisatorische Maßnahmen, wie z.B. eine Beschränkung[8] des Verwendungszwecks des spezifischen „Komfortsignatur“-Zertifikates gemäß § 7 Abs. 1 Nr. 7 SigG für die Signatur von elektronischen Rezepten oder die stichprobenartige Überprüfung der im Laufe eines Tages erstellten Signaturen, vorgesehen werden. Alternativ dazu ist auch eine technische Lösung denkbar, bei der die Signaturanwendungskomponente nur für bestimmte Dokumententypen, die beispielsweise anhand ihres XML-Schematas erkannt werden können, die Erzeugung einer Signatur mit der freigeschalteten Signaturerstellungseinheit anstößt.

Die Antwort zu Frage 18 der FAQ der BNetzA[9], die sich auf die „Massensignatur“ bezieht, sollte auch im Kontext der „Komfortsignatur“ berücksichtigt werden:

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

4 Zusammenfassung

Während das Signaturgesetz und die Signaturverordnung in Deutschland für die Identifikation des Signaturschlüsselinhabers (vgl. Abschnitt 2) unterschiedliche Verfahren zulassen, ist derzeit nur die in Abschnitt 2.1 diskutierte Identifikation durch Besitz und Wissen in der Praxis umgesetzt. Auf dieser Basis kann bereits heute ein „Komfortsignatur“-System im Einklang mit den Anforderungen von SigG und SigV gestaltet werden, bei dem die Mechanismen zur individuellen Willenserklärung (mit RFID-Token, Biometrie etc.) in der Signaturanwendungskomponente anstatt in der sicheren Signaturerstellungseinheit realisiert werden. Für die Zukunft ist es jedoch vorstellbar, dass auch geprüfte und bestätigte sichere Signaturerstellungseinheiten mit biometrischen Verifikationsmechanismen auf der Chipkarte existieren werden. Damit hier eine reibungslose Migration ermöglicht wird, sollte diese Zukunftsperspektive – wie beim eCard-API-Framework [BSI07] und dem entsprechenden Standard für die „European Citizen Card“ [CEN15480-3] geschehen – bereits beim Design heutiger Systeme berücksichtigt werden.

---

[7] Beispielsweise erscheint es sinnvoll, für die Signatur von Betäubungsmittelrezepten eine Einzelsignatur zu fordern.

[8] Um dies zu erreichen, könnte beispielsweise die folgende Beschränkung in das qualifizierte Zertifikat aufgenommen werden: "Diese Signatur ist nur für Verordnungen von Heilmitteln vorgesehen, die nicht dem Betäubungsmittelgesetz unterliegen."

[9] Siehe http://www.bundesnetzagentur.de/enid/FAQ/Antwortss8_wt.html

5 Danksagung

Die vorliegende Arbeit profitierte vom fruchtbaren Gedankenaustausch mit einer Reihe von Personen. Besonders herzlich sei Dr. Harald Ahrens, Klaus Keus, Dr. Gunter Lassmann, Thomas Stange und Dr. Christoph Sutter gedankt.

Literatur

[ÄZO06] Ärztezeitung: *Neue Gesundheitskarte kommt nur im Kriechgang voran*, Ärztezeitung online vom 16.06.2006, via http://www.aerztezeitung.de/docs/2006/06/16/02ao1601.asp?cat=/computer

[AMVV] *Verordnung über die Verschreibungspflicht von Arzneimitteln (Arzneimittelverschreibungsverordnung*, AMVV), via http://www.gesetze-im-internet.de/amvv/index.html

[ApBetrO] *Verordnung über den Betrieb von Apotheken (Apothekenbetriebsordnung, ApBetrO)*, via http://www.gesetze-im-internet.de/apobetro_1987/index.html

[BEM] Common Criteria Biometric Evaluation Methodology Working Group: *Common Biometric Evaluation Methodology - Common Criteria Common Methodology for Information Technology Security Evaluation - Biometric Evaluation Methodology Supplement (BEM)*, Version 1.0, August 2002, via http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

[BGB] *Bürgerliches Gesetzbuch*, via http://bundesrecht.juris.de/bundesrecht/bgb/

[BNAProd] Bundesnetzagentur: *Produkte für qualifizierte elektronische Signaturen*, via http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/Produkte_pi.html

[BoEi02] A. Bovenschulte, M. Eifert: *Rechtsfragen der Anwendung technischer Produkte nach Signaturgesetz*, DuD, 2002, S. 76 - 78

[BrTe01] G. Bröhl, A. Tettenborn: *Das neue Recht der elektronischen Signaturen: kommentierende Darstellung von Signaturgesetz und Signaturverordnung*, Bundesanzeiger-Verlag, Köln, 2001

[BSI97] Bundesamt für Sicherheit in der Informationstechnik: *BSI Handbuch für digitale Signaturen – auf Grundlage von SigG und SigV von 1997*, Version 1.1, Stand: 18.11.1997, via http://www.bsi.de/esig/basics/techbas/masskat/bsikat.pdf

[BSI07] Bundesamt für Sicherheit in der Informationstechnik: *eCard-API-Framework*, Technische Richtlinie des BSI TR-03112, 2007

[CC] *Common Criteria for Information Technology Security Evaluation (CC)*, Version 2.1, August 1999, via http://www.bsi.de/cc/downcc21.htm

[CEM] *Common Methodology for Information Technology Security Evaluation*, Version 1.0, August 1999, CEM-99/045, Part 2: Evaluation Methodology, via http://www.bsi.de/cc/cem-pdf.zip

[CEN15480-3] CEN/TC 224/WG15: *Identification card systems — European Citizen Card — Part 3: European Citizen Card Interoperability using an application interface*, Working Draft for prCEN/TS 15480-3, 2007

[EGSRL] *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*

[HBA-1] *German Health Professional Card and Security Module Card - Part 1: Commands, Algorithms and Functions of the COS Platform*, Version 2.1.0, 21.02.2006, via http://www.bundesaerztekammer.de/30/eArztausweis/70Download/060221a_HPC_P1_COS_V2_1_0.pdf

[HBA-PP] Bundesamt für Sicherheit in der Informationstechnik: *Protection Profile — Professional Health Card (PP-HPC)*, PP-0018, via http://www.bsi.de/zertifiz/zert/reporte/PP0018b.pdf

[HüKn03] D. Hühnlein, Y. Knosowski: *Aspekte der Massensignatur*, In P. Horster (Hrsg.), D·A·CH-Security 2003, IT-Verlag, S. 293–307

[ITSEC] *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik*, August 1992, http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf

[KiSc06] W. Killmann, V. Schenk: *Konzept für die Komfortsignatur mit dem Heilberufsausweis*, Version 0.6, Stand: 06.07.2006

[SigG] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, vom 16.05.2001, BGBl. 2001 Teil I Nr. 22, S. 876 ff, via http://bundesrecht.juris.de/sigg_2001/index.html

[RoFD03] A. Roßnagel, S. Fischer-Dieskau: *Automatisiert erzeugte elektronische Signaturen*, MMR 3, 2004. S. 133, via http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/AR_SFD_MMR_autoSig.pdf

[SigGBeg] *Begründung zu SigG*, via http://www.dfn-pca.de/bibliothek/sigg/germany/begruendung-zum-signaturgesetz-2001-05-16.pdf

[SigV] *Verordnung zur elektronischen Signatur*, vom 16.11.2001 BGBl. 2001 Teil I Nr. 59, S. 3074 ff), via http://bundesrecht.juris.de/sigv_2001/index.html

[SigVBeg] Begründung zu SigV, via http://www.dfn-pca.de/bibliothek/sigg/germany/begruendung-zur-signaturverordnung-2001-11-16.pdf

[SSCD-PP] CEN: *Workshop Agreement CWA 14169 - Secure Signature-Creation Devices "EAL 4+"*, März 2002, via http://www.a-sit.at/pdfs/cwa14169.pdf
siehe auch: *Protection Profile - Secure Signature-Creation Device Type 3*, Version 1.05, via http://www.bsi.de/zertifiz/zert/reporte/PP0006b.pdf
Protection Profile - Secure Signature-Creation Device Type 2, Version 1.04, via http://www.bsi.de/zertifiz/zert/reporte/PP0005b.pdf
Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05, via http://www.bsi.de/zertifiz/zert/reporte/PP0004b.pdf