

# Die elektronische Mehrfachsignatur mit dem neuen Heilberufsausweis

Ulrich Waldmann

Die elektronische Gesundheitskarte kommt und mit ihr eine Vielzahl von Anwendungen der elektronischen Signatur. Das elektronische Rezept ist nur der Anfang, andere können und sollen folgen. Dadurch werden Ärzte, Apotheker, Zahnärzte etc. in Zukunft jeden Tag mit ihrem Heilberufsausweis unzählige Unterschriften leisten. Um den täglichen Umgang mit der elektronischen Signatur in Praxen und Kliniken zu erleichtern, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) technische Richtlinien für Stapel- und Komfortsignaturen herausgegeben. In Folge wurden die Spezifikationen der dezentralen Komponenten Heilberufsausweis (HBA), Security Module Card (SMC), Konnektor und eHealth-Terminal um die Mehrfachsignatur erweitert. Die Spezifikation eines RFID-Token zur willentlichen Auslösung der Komfortsignatur ist hinzugekommen, während alternative biometrische Verfahren derzeit noch nicht vorgesehen sind. Der HBA bietet für die Stapel- und Komfortsignatur gemeinsame Zugriffsbedingungen, so dass die Signaturanwendungskomponente des Konnektors als zentrale Steuerungsinstanz aufgewertet werden musste. Diese erzwingt den zeitlichen und räumlichen Zusammenhang aller mit der Signatur verbundenen Prozesse und muss sich als sichere Signaturumgebung gegenüber dem HBA ausweisen. Das sichere Zusammenspiel der Komponenten ermöglicht benutzerfreundliche Mehrfachsignaturen, deren Konformität mit dem Signaturgesetz allerdings noch bestätigt werden muss.

## Verwendung qualifizierter Signaturen

Mit Einführung der elektronischen Gesundheitskarte (eGK) und des Heilberufsausweises (HBA) muss ein Arzt gemäß § 2 [AMVV] jedes ausgestellte elektronische Rezept mit einer qualifizierten elektronischen Signatur gemäß § 2 [SigG] versehen. Der Apotheker muss diese Signatur gemäß § 17 [ApBetrO] bei der Dispensierung des Rezepts prüfen. Zum Signieren der dispensierten Verordnungen ist dagegen keine qualifizierte Signatur erforderlich, sondern die Organisationssignatur der Apotheke mit der SMC-B [HPC-P3] ausreichend, solange das Primärsystem die handelnde Person identifizieren kann. Der Apotheker muss jedoch mit dem HBA qualifiziert signieren, wenn er nach Rücksprache mit dem Arzt die Verordnung abändert hat. Das Signieren der Abrechnungsdaten durch den Apotheker war bisher nicht gefordert und ist auch noch nicht geplant.

Die qualifizierte Signatur wird überall dort eingesetzt werden, wo bereits jetzt eine rechtsgültige Unterschrift im Gesundheitswesen erforderlich ist. Insbesondere die Daten zukünftiger freiwilliger Anwendungen (z. B. der Notfalldatensatz in der eGK) werden zum Nachweis ihrer Integrität und Herkunft qualifiziert signiert sein. Da in den bisherigen Signaturprozessen vor jeder einzelnen Signatur eine sechsstellige PIN eingegeben werden muss, sind effektive Lösungen für „Vielsignierende“ gefragt, die nach der Authentisierung mit der Signatur-PIN mehrere (aber nicht beliebig viele) Signaturen ermöglichen, ohne jedoch die Sicherheit und rechtliche Bedeutung der Signatur zu gefährden. Die Zulassung der Mehrfachsignatur für das Gesundheitswesen und den HBA könnte dabei für die Akzeptanz und Benutzerfreundlichkeit der elektronischen Abläufe in Arztpraxis und Apotheke entscheidend sein.

## Qualifizierte Mehrfachsignaturen

Die Technischen Richtlinien für die Stapelsignatur und für die Komfortsignatur mit dem Heilberufsausweis, siehe [TR-03114] und [TR-03115], beschreiben technische Lösungen für Mehrfachsignaturen für die besonderen Einsatzumgebungen des Gesundheitswesens. Die Richtlinien bilden die Grundlage für die technischen Spezifikationen, insbesondere [HPC-P2], [gemKon], [gemKT], [gemSMC-K] und [gemTok], die Herstellung der Signaturanwendungskomponenten (SAKs) und den Ablauf der Signaturprozesse bei den zukünftigen Anwendern. Die Sicherheitsanforderungen orientieren sich an den Vorgaben im Signaturgesetz [SigG] und in der Signaturverordnung [SigV] für qualifizierte elektronische Signaturen. Die Richtlinien wurden im Auftrag des BSI von T-Systems erarbeitet. Die Bundesnetzagentur muss nun bestätigen, dass die Lösungsansätze für die Mehrfachsignatur grundsätzlich für die qualifizierte elektronische Signatur geeignet sind.

Die rechtlichen Rahmenbedingungen für die Mehrfachsignatur werden in [Hhn07] untersucht und grundsätzlich als ausreichend gesehen: Es sei im Sinne des Ordnungsgebers, wenn der Signaturschlosselinhaber seine Signaturkarte durch einmalige Eingabe der Identifikationsdaten (PIN) für ein festes Zeitfenster oder eine bestimmte Anzahl an Signaturen aktiviert. Die Mechanismen zur individuellen Willenserklärung (z. B. mittels RFID-Token oder Biometrie) könnten SigG-konform auch außerhalb der Signaturkarte realisiert werden. Hinzu kommt, dass einige im Banken- und Notarumfeld eingesetzte Signaturkarten bereits für qualifizierte Mehrfachsignaturen bestätigt wurden, siehe „Multisignatur“ in [Tœ-VIT05] und [TœVIT08]. In den Bestimmungen wird darauf hingewiesen, dass die Mehrfachsignatur ausschließlich in besonders gesicherten Umgebungen (z. B. in einem Trust Center) und nur mit hinreichend geeigneten Signaturanwendungs-Komponenten eingesetzt werden darf.

Im Folgenden werden die wichtigsten Maßnahmen vorgestellt, mit denen die Benutzerfreundlichkeit der Signaturprozesse mittels Mehrfachsignaturen erhöht und die Sicherheit gewährleistet werden kann.

### Einfach-, Stapel- und Komfortsignatur

Als sichere SSEE gemäß Signaturgesetz dient der Heilberufsausweis, auf dem der Signaturschlüssel sicher hinterlegt ist. Der HBA soll zukünftig sowohl für Einfach-, als auch für Mehrfachsignaturen ausgelegt sein, wobei der Signaturschlüssel nur nach Authentisierung des Inhabers – durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale – [SigV] angewendet werden darf.

Die Einfachsignatur ist die qualifizierte elektronische Signatur, die gemäß [SigG] und [SigV] mit einer bestmöglichen Signaturkarte erzeugt wird. Dem Benutzer werden zunächst die zu signierenden Daten (DTBS) angezeigt. Nach erfolgreicher Präsentation der Signatur-PIN erlaubt die Signaturkarte die Erzeugung genau einer Signatur. Die Einfachsignatur ist für den HBA in normaler Umgebung vorgesehen und kann innerhalb und außerhalb des elektronischen Gesundheitswesens (LAN des Leistungserbringers) verwendet werden. Die PIN-Eingabe erfolgt gewöhnlich lokal, d. h. direkt am HBA-Terminal, da die Voraussetzungen für eine entfernte PIN-Übertragung mit Secure Messaging nicht unbedingt gegeben sind.

Die Mehrfachsignatur meint, dass der HBA nach erfolgreicher PIN-Eingabe nicht nur eine, sondern eine endliche Anzahl Signaturen zulässt. Dies soll auf eine gesicherte Umgebung beschränkt sein, welche durch die Signaturanwendungskomponente des Konnektors (SAK-Konnektor) kontrolliert und mittels integrierten Sicherheitsmoduls SMC-K gegenüber dem HBA nachgewiesen wird. Die PIN kann sowohl lokal, als auch entfernt eingegeben werden, so dass der Anwender seinen HBA in einem gesicherten Bereich zentral aufbewahren und Signaturen von verschiedenen Arbeitsplätzen aus erstellen kann. Zwei Varianten der Mehrfachsignatur, die Stapelsignatur und die Komfortsignatur, decken die wichtigsten Anwendungsfälle ab. Die Stapelsignatur ermöglicht mehrere Signaturen unmittelbar hintereinander nach dem Anzeigen der zu signierenden Dokumente (Stapel) und der darauf folgenden einmaligen Eingabe der PIN. Unmittelbar nachdem der gesamte Stapel signiert wurde, wird die PIN-Authentisierung automatisch gelöst.

Die Komfortsignatur geht in der Benutzerfreundlichkeit über die Stapelsignatur hinaus: Das Signieren mehrerer Dokumente kann nach einmaliger PIN-Eingabe über einen längeren Zeitraum (z. B. Arbeitstag) erfolgen, d. h. es können zeitlich versetzt mehrere Stapel signiert werden. Die PIN-Eingabe erfolgt ganz am Anfang, also vor dem Anzeigen der Dokumente, die zu dem Zeitpunkt noch gar nicht bekannt sein müssen. Sobald der Benutzer das Signieren eines Dokuments oder Dokumentenstapels auslösen möchte, muss er sich mittels RFID-Token oder Biometriemodul authentisieren (– Willensbekundung –). Der Sicherheitszustand dieser zusätzlichen Benutzerauthentisierung wird nach dem Signieren automatisch gelöst. Der Status der PIN-Authentisierung bleibt dagegen im HBA erhalten, bis er vom Benutzer oder automatisch durch die SAK-Konnektor nach anderen Kriterien (z. B. nach einer definierten Zeit) gelöst wird. Es ist deshalb aus Sicht des HBA möglich, ohne erneute Eingabe der PIN einen weiteren Stapel von Dokumenten zu signieren. Da der Signaturschlüssel des HBA über lange Zeit frei geschaltet ist, sind zusätzliche durch die SAK-Konnektor kontrollierte Sicherheitsmaßnahmen (außerhalb des HBA) notwendig...

Ä

### Dokumentinformationen zum Volltext-Download

Ä

Titel:

Die elektronische Mehrfachsignatur mit dem neuen Heilberufsausweis Artikel ist erschienen in:

Telemedizinführer Deutschland, Ausgabe 2009

Kontakt/Autor(en): Ulrich Waldmann

ulrich.waldmann@sit.fraunhofer.de

Tel.: +49 (0) 61 51 / 8 69 - 2 22

Fax: +49 (0) 61 51 / 8 69 - 2 24

Fraunhofer-Institut für Sichere

Informationstechnologie SIT

Rheinstr. 75

64293 Darmstadt      Seitenzahl:

6

Sonstiges:

4 Abb.

Dateityp/ -größe:

PDF / 225 kB

Click&Buy-Preis in Euro:

0,50

Ä Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. Ä

Hier gehts zum Click&Buy-Download...

Allgemeine Infos zu Click&Buy finden Sie hier... [^](#)