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 abgeändert 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 [Hühn07] untersucht und grundsätzlich als ausreichend gesehen: Es sei im Sinne des Verordnungsgebers, wenn der Signaturschlüsselinhaber 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 [TÜVIT05] und [TÜVIT08]. In den Bestätigungen wird darauf hingewiesen, dass die Mehrfachsignatur ausschließlich in besonders gesicherten Umgebungen (z. B. in einem Trust Center) und nur mit hinreichend geprüften Signaturanwendungs-Komponenten eingesetzt werden darf.

Im Folgenden werden die wichtigsten Maßnahmen vorgestellt, mit denen die

Autor: Ulrich Waldmann
Titel: Die elektronische Mehrfachsignatur mit dem neuen Heilberufsausweis
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 258-264

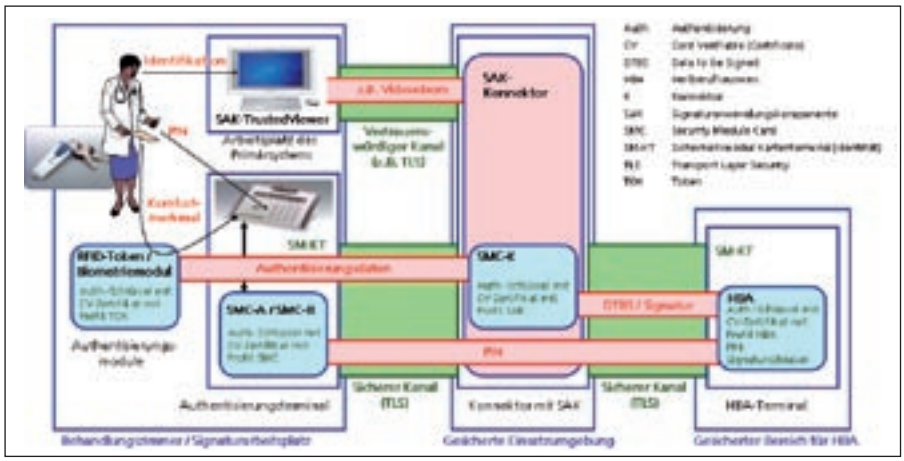

Abbildung 1: *Technischer Lösungsansatz für die Mehrfachsignatur*

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 bestätigten 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 Büroumgebung 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 gelöscht.

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 gelöscht. 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) gelöscht 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.

Technischer Lösungsansatz

Ziel des Lösungsansatzes ist es, durch das kontrollierte Zusammenspiel von HBA, Sicherheitsmodulen und den Signaturanwendungskomponenten (SAKs) sichere Stapel- und Komfortsignaturen zu ermöglichen, siehe Abbildung 1.

Die SAK-Konnektor kontrolliert die Identität des Benutzers und des Arbeitsplatzes, nimmt die vor-ausgewählten Daten vom Primärsystem entgegen und bereitet sie für den Trusted Viewer auf. Sie steuert den gesamten Signaturprozess, d.h. die Kontrolle der zu signierenden Daten, die PIN-Eingabe, die Signaturerzeugung etc., und nutzt das Sicherheitsmodul SMC-K als Schlüsselspeicher und zum Aufbau einer Secure Messaging Verbindung zum HBA.

Im Rahmen der Komfortsignatur wird zudem die gesonderte Benutzerauthentisierung mittels eines Komfortmerkmals (Präsentation eines RFID-Token oder eines biometrisches Merkmals) kontrolliert, um den Signaturvorgang auszulösen. In jedem Fall stellt die SAK-Konnektor sicher, dass der Signaturkarte ausschließlich Daten zugeführt werden, welche die berechtigte Person zum Signieren bestimmt hat („Willensakt“). Dazu bedient sie sich der zweiten Komponente, SAK-TrustedViewer, die als Software am Signaturarbeitsplatz eine Benutzerschnittstelle bietet und die vertrauenswürdige Anzeige der Daten gewährleistet. SAK-TrustedViewer und SAK-Konnektor sind über einen SAK-internen vertrauenswürdigen Kanal verbunden. Gemäß [gemKON] dient dazu eine TLS-Verbindung.

Zu den SAKs gehören schließlich die SICCT-konformen Kartenterminals (siehe [SICCT] und [gemKT]), die im Konnektor registriert sind und eine eigene kryptographische Identität besitzen. Terminals und Konnektor authentisieren sich gegenseitig und sichern die Kommunikation mit TLS. Der Benutzer gibt seine PIN lokal am HBA-Terminal oder entfernt über ein Authentisierungsterminal des Arbeitsplatzes ein. In jedem Authentisierungsterminal ist eine Sicherheitsmodulkarte SMC-A oder SMC-B gemäß [HPC-P3] verfügbar, die eine Secure Messaging Verbindung für die PIN-Übertragung an den HBA aufbauen kann. Jedes komfortsignaturfähige Terminal verfügt zusätzlich über eine kontaktlose Schnittstelle für den Token. Jede der eingesetzten Chipkarten RFID-Token, SMC-A, SMC-B, SMC-K und HBA besitzt einen Authentisierungsschlüssel und ein zugehöriges Card Verifiable Certificate (CV-Zertifikat), in dem eine Rollenkennung mit Profil TOK, SMC, SAK oder HBA hinterlegt ist. Die Rollenkennung jeder Karte wird in den internen Zugriffsregeln der anderen Karten für deren Schlüssel und Daten verwendet und wird in einer Card2Card-Authentisierung nachgewiesen.

Die folgenden Kapitel beschreiben die Prozesse der Stapel- und Komfortsignatur und gehen etwas ausführlicher auf besondere Eigenschaften der Komponenten ein.

Ablauf der Stapelsignatur

Abbildung 2 zeigt die wichtigsten Schritte zur Erstellung einer Stapelsignatur. Der HBA-Inhaber steckt den HBA z. B. zu Beginn des Arbeitstages in ein HBA-Terminal, wo die Karte gegen Entnahme und Missbrauch geschützt ist.

Schritt 1:
Auf dem Primärsystem des Arbeitsplatzes erstellt der Benutzer mehrere Dokumente und möchte sie schließlich signieren. Dazu identifiziert er sich über das Primärsystem gegenüber der SAK-Konnektor, die den Zusammenhang zwischen dem bekannten Benutzer, dem derzeitigen Signaturarbeitsplatz mit SAK-TrustedViewer, einem Authentisierungsterminal in der Nähe, dem HBA und dem aktuell genutzten HBA-Terminal herstellt.

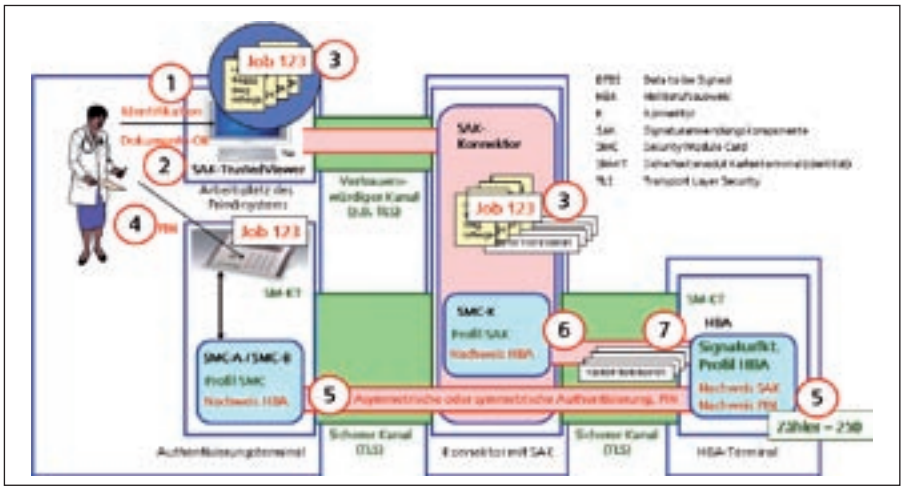

Abbildung 2: *Ablauf der Stapelsignatur*

Schritt 2:
Das Primärsystem übergibt die zu signierenden Dokumente an den Konnektor und dieser reicht sie an die SAK-Konnektor weiter. Die SAK-Konnektor überprüft die Syntax der XML-formatierten Dokumente und sendet eine eindeutige Repräsentation der Daten an die SAK-Trusted Viewer. Dort kann der Benutzer die Dateien betrachten und zum Signieren auswählen.
Schritt 3:
Die SAK-Konnektor berechnet alle Hash-Werte des zu signierenden Stapels. Sie generiert eine Jobnummer, die den Signaturprozess eindeutig identifiziert, und zeigt diese auf dem Trusted Viewer dem Benutzer an.
Schritt 4:
Der Benutzer wird zur PIN-Eingabe an einem Authentisierungsterminal in der Nähe des Arbeitsplatzes aufgefordert, wo ebenfalls die Jobnummer angezeigt wird. Durch den Vergleich beider Nummern kann sich der Benutzer sicher sein, seine PIN am richtigen Terminal einzugeben.
Schritt 5:
Mittels asymmetrischer Card2Card-Authentisierung wird eine Secure Messaging Verbindung zwischen SMC-A oder SMC-B im Authentisierungsterminal und der HBA aufgebaut. Die eingegebene PIN wird anschließend mit Secure Messaging (d.h. mit Sitzungsschlüsseln verschlüsselt und mit Prüfsumme geschützt) zum HBA übertragen, wo die PIN-Prüfung erfolgt. War die Benutzerauthentisierung erfolgreich, so wird auf dem HBA als Sicherheitsstatus ein Nutzungszähler, der so genannte Security Status Evaluation Counter (SSEC), auf einen vorkonfigurierten endlichen Wert (z. B. 250) gesetzt. Dieser Wert legt die maximale Anzahl der Signaturen fest, d.h. die maximale Größe des Stapels, der nach einmaliger PIN-Eingabe signiert werden kann. Der Zählerstand wird bei jeder Signaturerstellung (in Schritt 7) um eins erniedrigt.
Schritt 6:
Nach der erfolgreichen Benutzerauthentisierung baut die SAK-Konnektor mittels asymmetrischer Authentisierung eine Secure Messaging Verbindung zwischen Konnektor und HBA auf, wobei die SAK-Konnektor als Sicherheitsumgebung für die Mehrfachsignatur durch die Rollenkennung mit Profil SAK gegenüber dem HBA und umgekehrt die sichere Signaturerstellungseinheit durch die Rollenkennung mit Profil HBA gegenüber der SAK-Konnektor nachgewiesen wird.
Schritt 7:
Die Signaturbefehle mit den Hash-Werten der zu signierenden Dokumente (DTBS) werden nun mit Secure Messaging an den HBA gesendet, bis der gesamte Stapel signiert ist. Anschließend löscht die SAK den PIN-Status des HBA (z. B. durch Reset oder Selektion einer anderen Anwendung) und beendet die Secure Messaging Verbindung.

Registrierung eines Komfortmerkmals

Die Komfortsignatur erfordert die Vorbereitung gesonderter Authentisierungsmodule mit Komfortmerkmal (z. B.

RFID-Token) und weitere von der SAK kontrollierte Sicherheitsnahmen. Das ist notwendig, weil auf dem HBA keine anderen Zugriffsbedingungen für den Signaturschlüssel gelten sollen als für die Stapelsignatur und somit kein höherer Sicherheitsstatus in der Karte erreichbar ist. Die SAK-Konnektor kann zu jedem HBA mehrere Komfortmerkmale verwalten. Im Falle der Signaturauslösung mittels RFID-Token muss jeder Benutzer über einen eigenen Token verfügen, der zunächst folgendermaßen im Konnektor registriert wird, siehe Abbildung 3.

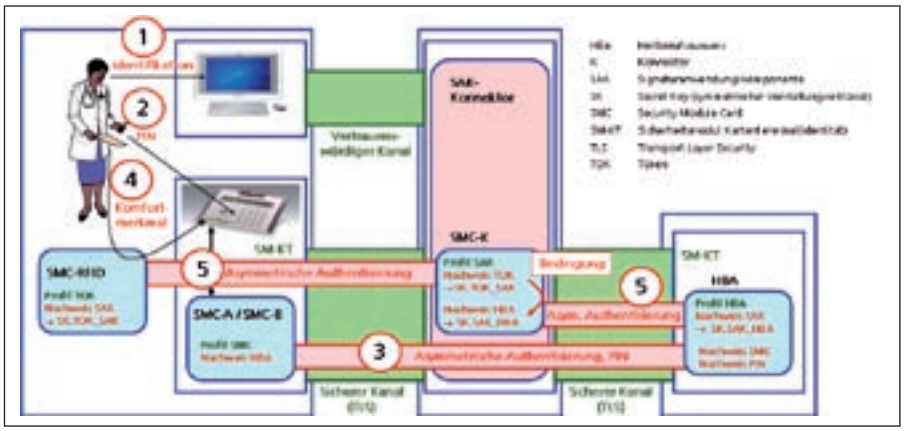

Abbildung 3: Registrierung eines Komfortmerkmals

Schritt 1:
Der Benutzer wählt die Funktion zur Registrierung eines RFID-Token (= SMC-RFID) aus und muss sich gegenüber der SAK identifizieren. Die SAK-Konnektor stellt den Zusammenhang zwischen dem bekannten Benutzer, dem derzeitigen Signaturarbeitsplatz mit SAK-TrustedViewer, einem Authentisierungsterminal in der Nähe, dem HBA und dem aktuell genutzten HBA-Terminal her.
Schritt 2:
Darauf fordert die SAK den Benutzer auf, seine PIN einzugeben. Das Aktivieren des RFID-Token ist somit an die erfolgreiche Eingabe der Signatur-PIN geknüpft, so dass gegenüber der SAK der Nachweis geführt wird, dass ein autorisierter Benutzer die Registrierung am Authentisierungsterminal durchführt.
Schritt 3:
Mittels asymmetrischer Card2Card-Authentisierung wird eine Secure Messaging Verbindung zwischen SMC-A oder SMC-B im Authentisierungsterminal und der HBA aufgebaut. Die eingegebene PIN wird anschließend mit Secure Messaging zum HBA übertragen, wo die PIN-Prüfung erfolgt. Damit wird erreicht, dass nach erfolgreicher PIN-Eingabe der HBA keinen weiteren Registrierungsprozess (z. B. mit einem fremden RFID-Token) durchlaufen kann, ohne dass die PIN erneut eingegeben wird.
Schritt 4:
Der autorisierte Benutzer muss am Authentisierungsterminal den RFID-Token präsentieren, um gemeinsame Vorstellungsschlüssel (Introduction Keys) zwischen RFID-Token und SAK einerseits, SAK und HBA andererseits zu vereinbaren.
Schritt 5:
Für diese so genannte Vorstellungsrunde verwenden die Komponenten RFID-Token, SAK-Konnektor und HBA ihren asymmetrischen Authentisierungsschlüssel (und die entsprechenden CV-Zertifikate), mit denen in einer gegenseitigen Authentisierung symmetrische Sitzungsschlüssel vereinbart werden. Diese Schlüssel sind jedoch keine temporären Secure Messaging Schlüssel, sondern werden als Vorstellungsschlüssel persistent gespeichert.

Für den eigentlichen Signaturprozess erfolgt dann eine symmetrische Authentisierung mit dem vereinbarten Vorstellungsschlüssel, siehe nächster Abschnitt. Im Kontext der Komfortsignatur ist die erfolgreiche Vereinbarung des Vorstellungsschlüssels zwischen RFID-Token und SAK Voraussetzung für die Vereinbarung des Vorstellungsschlüssels zwischen SAK und HBA, um eine durchgehende Authentisierung und eindeutige Zuordnung von RFID-Token zu einem HBA zu erzwingen.

Ablauf der Komfortsignatur

Der HBA-Inhaber hat die Karte in ein HBA-Terminal gesteckt und möchte im Laufe des Arbeitstages Einzeldokumente oder Dokumentenstapel erstellen und gemäß Komfortsignatur signieren. Der Registrierungsprozess des Komfortmerkmals hat bereits zu einem früheren Zeitpunkt stattgefunden, d. h. die Komponenten besitzen den bei der Registrierung vereinbarten symmetrischen Vorstellungsschlüssel. Die Erstellung einer Komfortsignatur läuft in den folgenden Schritten ab, siehe Abbildung 4:

Schritt 1:
Zunächst identifiziert sich der Benutzer gegenüber Primärsystem und SAK, erstellt dann einige Dokumente und startet den Vorgang der Komfortsignatur.
Schritt 2:
Die SAK-Konnektor fordert den Benutzer nun direkt zur PIN-Eingabe an einem Authentisierungsterminal auf, falls die PIN nicht bereits beim Stecken des HBA präsentiert wurde.
Schritt 3:
In einer symmetrischen Card2Card-Authentisierung mit dem Vorstellungsschlüssel wird eine Secure Messaging Verbindung zwischen SMC-A oder SMC-B des Kartenterminals und der HBA aufgebaut. Die eingegebene PIN wird anschließend mit Secure Messaging zum HBA übertragen, wo die PIN-Prüfung erfolgt. War die Benutzerauthentisierung erfolgreich, so wird auf dem HBA wie bei der Stapelsignatur der Nutzungszähler SSEC auf den vorkonfigurierten Wert (z. B. 250) gesetzt.
Schritt 4:
Das Primärsystem übergibt die zu signierenden Dokumente an den Konnektor und dieser reicht sie an die SAK-Konnektor weiter. Die SAK-Konnektor überprüft die Syntax der XML-formatierten Dokumente und sendet eine eindeutige Repräsentation der Daten an die SAK-TrustedViewer. Dort kann der Benutzer die Dateien betrachten und zum Signieren auswählen.
Schritt 5:
Die SAK-Konnektor berechnet alle Hash-Werte des zu signierenden Stapels. Sie

generiert eine Jobnummer, die den Signaturprozess eindeutig identifiziert, und zeigt diese auf dem Trusted Viewer dem Benutzer an.

Schritt 6:
Die SAK fordert den Benutzer zur Präsentation des Komfortmerkmals an einem Authentisierungsterminal in der Nähe des Arbeitsplatzes auf, wo ebenfalls die Jobnummer angezeigt wird. Durch den Vergleich beider Nummern kann sich der Benutzer sicher sein, das RFID-Token am richtigen Terminal zu präsentieren.

Schritt 7:
Der RFID-Token (als „Proxy des Benutzers“) authentisiert sich mit dem symmetrischen Vorstellungsschlüssel gegenüber der SAK. Um die Authentisierungskette vom Token bis zum HBA sicherzustellen, führt die SAK erst nach erfolgreicher Authentisierung zwischen Token und SAK die symmetrische Authentisierung zwischen SAK und HBA aus. Dabei werden Secure Messaging Schlüssel zwischen SAK und HBA vereinbart.

Schritt 8:
Schließlich werden die DTBS des Stapels mit Secure Messaging an den HBA gesendet und signiert. Bei jeder Signatur wird der Wert des Nutzungszählers SSEC um eins erniedrigt. Nach Signatur des Stapels löscht die SAK die Secure Messaging Schlüssel und den Authentisierungsstatus ihrer Vorstellungsschlüssel, so dass für weitere Signaturen erneut eine Präsentation des Komfortmerkmals (RFID-Token) und eine symmetrische Authentisierung nötig sind.

Im Unterschied zum Stapelsignaturprozess löscht die SAK die PIN-Authentisierung im HBA nicht. Der Sicherheitsstatus bleibt erhalten, solange der Nutzungszähler SSEC größer null ist. Daher sind weitere Signaturen mittels Präsentation des Komfortmerkmals (unter Weglassung der Schritte 2 und 3) möglich. Das Löschen der PIN-Authentisierung kann aber auf Wunsch des Benutzers oder nach einer konfigurierten Zeitspanne erfolgen. Der Benutzer kann von jedem Arbeitsplatz aus die PIN zurücksetzen oder auch den Token desaktivieren, falls beispielsweise dieser verloren gegangen ist. Zur Desaktivierung des Token muss die SAK nur den zugehörigen symmetrischen Vorstellungsschlüssel löschen.

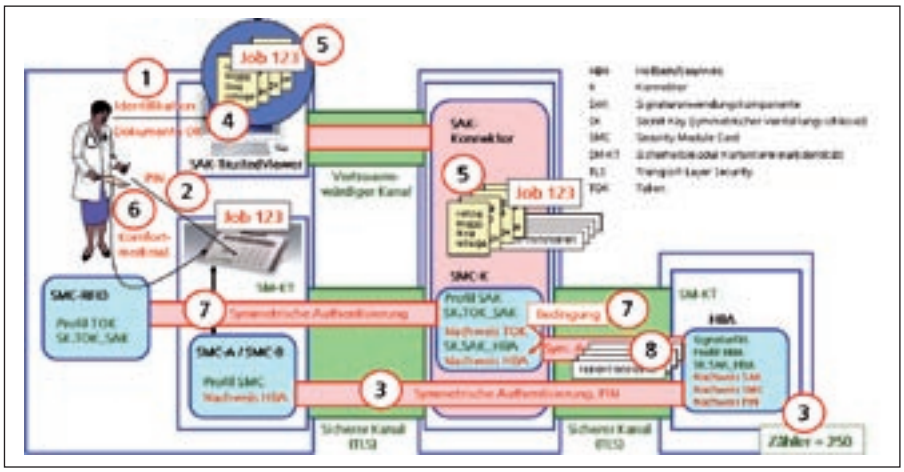

***Abbildung 4:** Ablauf der Komfortsignatur*

Mehrfachsignaturen aus Sicht des HBA

Der HBA prüft die gesicherte Einsatzumgebung der Mehrfachsignaturen in gleicher Weise für die Stapelsignatur und Komfortsignatur. Das wird durch die SMC-K erreicht, deren Authentisierungsschlüssel die Rollenkennung mit Profil SAK besitzt. Dieses Profil repräsentiert die gesicherte Signaturumgebung des Konnektors und muss gemäß Zugriffsregel des Signaturschlüssels gegenüber dem HBA nachgewiesen werden.

Die Einfachsignatur ist weiterhin wie bei einer gewöhnlichen Signaturkarte außerhalb der gesicherten Einsatzumgebung möglich. Zudem kann die Einfachsignatur in gesicherten Einsatzumgebungen mit der Stapel- und Komfortsignatur kombiniert werden. Der HBA bildet die Einfach- und Mehrfachsignatur auf zwei karteninterne Sicherheitsumgebungen (SE#1 und SE#2) der Signaturanwendung ab. SE#1 und SE#2 realisieren unterschiedliche Zugriffsregeln für den Signaturschlüssel und können von außen durch das Kartenkommando MSE: SET selektiert werden. In der aktuellen Spezifikation [HPC-P2] gelten für den Signaturschlüssel im HBA in Verbindung mit dem Kartenkommando PSO: COMPUTE DIGITAL SIGNATURE die folgenden Zugriffsbedingungen:

- Sicherheitsumgebung SE#1 für die Einfachsignatur
  - Authentisierung mit Signatur-PIN für genau eine Signatur
- Sicherheitsumgebung SE#2 für die Stapel- und Komfortsignatur
  - Authentisierung mit Signatur-PIN für maximal 250 Signaturen (Beispiel)
  - Externe Authentisierung mit Profil SAK
  - Übertragung der DTBS mit Secure Messaging

Für die gewöhnliche Einfachsignatur wird kein Secure Messaging gefordert, da Umgebungen außerhalb der Telematikinfrastruktur nicht über entsprechende Chipkarten zum Aufbau einer solchen Verbindung verfügen. Die Sicherheitsumgebung SE#1 des HBA lässt aber durchaus Secure Messaging zu. Aus Sicherheitsgründen sollte dennoch, wo es möglich ist, die Sicherheitsumgebung SE#2 gewählt werden, wobei auch Stapel aus einem einzigen Dokument möglich sind. Der HBA schreibt in keiner Sicherheitsumgebung vor, dass die PIN mit Secure Messaging übertragen wird. Das wird bei entfernter PIN-Eingabe von der SAK durchgesetzt.

Ob eine Stapel- oder eine Komfortsignatur erfolgt, entscheidet der Benutzer und wird außerhalb des HBA durch die SAK kontrolliert. Die SAK setzt für beide Varianten der Mehrfachsignatur im HBA die Sicherheitsumgebung SE#2, so dass der HBA beim Zugriff auf den Signaturschlüssel die sichere Signaturumgebung an der Rollenkennung mit Profil SAK erkennen muss und den Signaturbefehl nur im Secure Messaging Modus zulässt. Selbstverständlich werden die erreichten Sicherheitszustände bei einem Wechsel

der Sicherheitsumgebung gelöscht.

Die Zahl der möglichen Signaturen für die Mehrfachsignatur nach PIN-Authentisierung wird in der Bestätigung des HBA als Signaturkarte in Abhängigkeit von den konkreten Einsatzbedingungen und den technischen Lösungen für die Komfortsignatur in der SAK festgelegt, siehe Kapitel 3.3 in [TR-03115]. Der HBA implementiert die Anzahl der nach einer erfolgreichen PIN-Eingabe möglichen Signaturen als Security Status Evaluation Counter (SSEC). Der SSEC ist kartenintern nicht dem Signaturschlüssel, sondern der Signatur-PIN zugeordnet und kann als Parameter des PIN-Sicherheitsstatus in den beiden Sicherheitsumgebungen unterschiedlich konfiguriert werden. Der konfigurierte SSEC-Maximalwert (jedoch nicht der aktuelle Zählerstand) ist frei aus einer Datei des HBA auslesbar, damit die SAK die Signaturstapelgröße entsprechend optimieren kann.

Eigenschaften des RFID-Token

Die einmalige Präsentation des Tokens genügt für die Signaturen eines gesamten Stapels, so dass der Token nicht über die gesamte Durchführung der Stapelsignatur präsent sein muss. Wie wird nun sichergestellt, dass der Token nur vom rechtmäßigen Besitzer verwendet werden kann? Gemäß [TR-03115] muss „der Signaturschlüssel-Inhaber [...] die Kontrolle über den Token ausüben und ihn vor Missbrauch schützen. Die technische Ausführung des Tokens muss den Besitzer unterstützen, seinen Token vor Missbrauch zu schützen. Dieser Missbrauchschutz kann erfolgen durch

- die Aktivierung des Tokens durch eine 4-stellige PIN
- die Aktivierung des Tokens durch ein biometrisches Merkmal des Besitzers
- andere geeignete Sicherheitsmaßnahmen, die einen Verlust oder die unkontrollierte Nutzung verhindern."

Wird eine Token-PIN verwendet, so soll diese PIN durch den Token selbst geprüft und geschützt über die kontaktlose Schnittstelle übertragen werden. Einen solcher Token mit vierstelliger PIN zu zertifizieren wäre kein Problem, würde aber in der Praxis dem Komfortgedanken widersprechen. Der Kompromiss mit dem BSI sieht so aus, dass der Anwender die Sicherheitsmaßnahmen gegen den Missbrauch des Tokens selbst skalieren kann, d.h. eine Token-PIN auch deaktivierbar wäre. Damit entscheidet der Anwender, welche Maßnahmen gegen den Verlust und Missbrauch des Tokens greifen sollen.

Die aktuelle Spezifikation [gemTok] definiert den Token – dort SMC-RFID genannt – als eine vereinfachte SMC-K mit kontaktloser Schnittstelle nach [ISO14443]. Eine solche Proximity Card besitzt eine Lesereichweite von etwa 5 cm, bei der auch leistungsintensive kryptographische Prozesse wie Secure Messaging noch funktionieren. Zwei Varianten der SMC-RFID sind vorgesehen: Die erste Variante besitzt ein mindestens 4-stelliges Passwort zum Schutz der Authentisierungsfunktion, die zweite Variante kommt ohne dieses Passwort aus und benötigt äußere (z. B. organisatorische) Sicherheitsmaßnahmen. Die nach [TR-03115] mögliche Auslösung der Komfortsignatur mit einem biometrischen Merkmal ist in [gemTok] und [gemKT] noch nicht vorgesehen.

Ausblick

Die HPC/SMC-Spezifikation und die Spezifikationen der gematik wurden für das Release 2.3.4 an die Richtlinien für die Stapel- und Komfortsignatur angepasst. Für das Biometriemodul ist bisher keine separate Spezifikation geplant, obwohl auf lange Sicht Alternativen zur Benutzerauthentisierung mit dem Token wünschenswert sind. Daher sollten die Diskussionen um Token und Biometriemodul weitergeführt werden, z.B. über Maßnahmen gegen Verlust und Missbrauch des Tokens oder über Entwicklung und Nachweis einer ausreichenden Mechanismenstärke bei biometrischen Verfahren. Wichtige Sicherheitsmerkmale und Eigenschaften der Authentisierungsmodule sollten später als Anhänge in die Richtlinien einfließen.

Auf Basis der Spezifikationen entwickelt die Industrie Produkte (Chipkarten, Signaturkomponenten), welche evaluiert und vom BSI zertifiziert werden müssen. [SigV] schreibt die Evaluierung der Anwendungskomponenten und der Signaturkarten für die qualifizierte elektronische Signatur nach den Common Criteria auf EAL3 bzw. EAL4 vor, jeweils ergänzt um eine Prüfung auf Widerstandsfähigkeit gegen ein hohes Angriffspotential und eine vollständige Missbrauchsanalyse. Grundlage der Evaluierung sind zu erstellende Schutzprofile für HBA, SMC-A, SMC-B und möglicherweise weiterer Sicherheitsmodule, Konnektor und Kartenterminal. Dazu haben die Richtlinien mit Kapiteln über Sicherheitsbewertung, Missbrauchsanalyse und Sicherheitspolitiken bereits gute Vorarbeit geleistet. Die Produkte müssen vom BSI oder TÜV-IT als SigG-konforme Signaturkomponenten für die qualifizierte elektronische Signatur bestätigt werden. Welche Signatur- und Authentisierungslösungen sich in den verschiedenen Anwendungsumgebungen durchsetzen werden, werden schließlich die Benutzer in der täglichen Praxis entscheiden.

Literatur

[AMVV] Verordnung über die Verschreibungspflicht von Arzneimitteln (Arzneimittelverschreibungsverordnung, AMVV), www.gesetze-im-internet.de/amvv

[ApBetrO] Verordnung über den Betrieb von Apotheken (Apothekenbetriebsordnung, ApBetrO), www.gesetze-im-internet.de/apobetro_1987

[gemKon] gematik: Einführung der Gesundheitskarte – Konnektorspezifikation, Version 2.8.0, 12.06.2008

[gemKT] gematik: Einführung der Gesundheitskarte – Spezifikation eHealth-Kartenterminal, Version 2.6.1, 12.06.2008

[gemSMC-K] gematik: Einführung der Gesundheitskarte – Spezifikation der SMC-K, Version 1.1.0, 19.06.2008

[gemTok] gematik: Einführung der Gesundheitskarte – Spezifikation der SMC-RFID, Version 1.0.0, 19.06.2008

[HPC-P1] German Health Professional Card and Security Module Card, Part 1: Commands,

Algorithms and Functions of the COS Platform, Version 2.3.0, 04.07.2008

[HPC-P2] German Health Professional Card and Security Module Card, Part 2: HPC Applications and Functions, Version 2.3.0, 04.07.2008

[HPC-P3] German Health Professional Card and Security Module Card, Part 3: SMC Applications and Functions, Version 2.3.0, 04.07.2008

[Hühn07] Hühnlein, D.: Rechtliche Rahmenbedingungen der „Komfortsignatur", DACH Security, 2007

[ISO14443] ISO/IEC 14443 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards

[SICCT] TeleTrusT: SICCT Secure Interoperable ChipCard Terminal, Version 1.20, 19.11.2007

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), 16. Mai 2001, BGBl. I S. 876 ff.

[SigV] Verordnung zur elektronischen Signatur (deutsche Signaturverordnung – SigV), 16. November 2001, BGBl. I S. 3074 ff.

[TR-03114] BSI: Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis, TR-03114, Version 2.0, 22.10.2007, www.bsi.de/literat/tr/tr03114

[TR-03115] BSI: Technische Richtlinie für die Komfortsignatur mit dem Heilberufsausweis, TR-03115, Version 2.0, 19.10.2007, www.bsi.bund.de/literat/tr/tr03115

[TÜVIT05] Bestätigung der Signaturerstellungseinheit STARCOS 3.0 with Electronic Signature Application V3.0 der Giesecke & Devrient GmbH, TUVIT.93100.TE.09.2005, 16.09.2005, www.tuvit.de/certuvit/pdf/93100UD.pdf

[TÜVIT08] Bestätigung der Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.1.2 der Giesecke & Devrient GmbH, TUVIT.93166.TU.06.2008, 26.06.2008, www.tuvit.de/certuvit/pdf/93166UD.pdf

Kontakt
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