Ausweise als Träger für Signaturverfahren

Rotraud Gitter, Moritz Strasser

Staatliche Ausweise bieten eine einmalige Chance, verlässliche Infrastrukturen für E-Commerce und E-Government zu schaffen. Die Integration qualifizierter Signaturverfahren in bereits etablierte Ausweise kann dazu beitragen gegenwärtige Hürden zu überwinden und dadurch die kritische Masse zu erreichen, ab der die Verbreitung von signaturbasierten Anwendungen, über eine prototypische oder projektbezogene Umsetzung hinaus Erfolg versprechend erscheint. Der vorliegende Beitrag stellt die wirtschaftlichen und rechtlichen Rahmenbedingungen für eine Integration dar und zeigt mögliche Umsetzungsalternativen auf.[*]

Rotraud Gitter (LL.M.)

Wiss. Mitarbeiterin und Geschäftsführerin der Projektgruppe verfassungsverträgliche Technikgestaltung, Universität Kassel
E-Mail: r.gitter@uni-kassel.de

Moritz Strasser

Wiss. Mitarbeiter des Instituts für Informatik und Gesellschaft, Abteilung Telematik Albert-Ludwigs Universität Freiburg i.Br.
E-Mail: moritz.strasser@iig.uni-freiburg.de

[*] Die folgenden Überlegungen gehen u.a. auf Arbeiten zurück, die im Rahmen der „Machbarkeitsstudie Digitaler Personalausweis“ im Auftrag des Bundesministeriums für Wirtschaft und Arbeit 2003/04 erstellt wurden.

Einleitung

Qualifizierte Signaturen sind eine Basistechnologie des elektronischen Geschäftsverkehrs, mit der rechtsverbindliche und beweissichere Transaktionen über digitale Kommunikationswege gewährleistet werden können. Obwohl die rechtlichen Rahmenbedingungen geschaffen wurden und ein Angebot von Signaturverfahren durch Zertifizierungsdiensteanbieter besteht, werden diese in der Praxis jedoch nicht in nennenswertem Umfang nachgefragt.

Ursächlich für die geringe Verbreitung qualifizierter Signaturverfahren ist neben Akzeptanzhürden eine ungünstige Kosten-Nutzen-Relation. Das marktwirtschaftliche Durchsetzungspotenzial digitaler Güter, zu denen elektronische Signaturen zählen, ist abhängig von Skalen- und Netzeffekten.[1] Diese bedingen, dass erst bei hohen Absatzmengen der Nutzen des Gutes die Kosten übersteigen kann. Greifen Skalen- und Netzeffekte ineinander, kann nur eine stetig wachsende Verbreitung zu positiven Effekten führen, wobei die Verbreitungsgeschwindigkeit als ein kritischer Erfolgsfaktor zu sehen ist. Erst ab dem Überschreiten einer kritischen Anzahl treten positive Rückkopplungsschleifen zwischen Netz- und Skaleneffekten auf, die eine Verbreitung im Markt weiter antreiben.[2] Solange eine solche kritische Masse nicht erreicht ist, wirken Skalen- und Netzeffekte eher als Hürde für die Verbreitung.[3]

> Zum Erreichen der kritischen Anzahl, ab der das Angebot von signaturbasierten Anwendungen über eine prototypische oder projektbezogene Umsetzung hinaus Erfolg versprechend erscheint, sollten zusätzliche Verbreitungsstrategien angewendet werden. Eine viel versprechende Verbreitungsstrategie stellt die Integration qualifizierter Signaturverfahren in bereits etablierte Ausweisdokumente dar, die über eine hinreichende Verbreitung in der Bevölkerung verfügen und einen entsprechenden Vertrauensvorschuss genießen.

Im vorliegenden Beitrag werden die wirtschaftlichen und rechtlichen Rahmenbedingungen für eine Integration betrachtet und zwei Varianten vorgestellt.

1 Integration als Geschäftsmodell

Durch die Integration der Signaturfunktion in eine bestehende Ausweisinfrastruktur können Synergieeffekte erzielt werden, die zu einer Verbesserung der Kosten-Nutzen Relation führen und die Interoperabilität zwischen einzelnen Zertifizierungsdienstleistungen und Produkten für elektronische Signaturen erhöhen. Eine intensivere Nutzung von Signaturverfahren führt dann auch zu einer Vereinheitlichung von Produkten und Verfahren für elektronische Signaturen, wodurch sich Standards auf technischer und organisatorischer Ebene etablieren können.

1.1 Rahmenbedingungen

Die möglichst universelle Verwendbarkeit der zu integrierenden Signaturverfahren wird als eine notwendige Voraussetzung für eine weite Verbreitung angesehen.[4] Hierzu zählen die Möglichkeit, die Dokumentations- und Beweiseignung elektronischer Dokumente zu sichern und gesetzliche Formerfordernisse einzuhalten. Entsprechende Rechtsfolgen wie die Beweiserleichterung nach § 292a ZPO und die Angleichung von Formvorschriften im privaten und öffentlichen Bereich konnte der Gesetzgeber nur für die Verwendung qualifizierter Signaturen vorsehen, da nur für diese einheitliche gesetzliche Anforderungen ein hinreichendes Sicherheitsniveau gewähr-

[1] S. Shapiro/Varian Information Rules: A Strategic Guide to the Network Economy, 1999.

[2] S. Müller/Eymann/Kreutzer Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft, 2003.

[3] Für Signaturen s. Roßnagel, MMR 2003, 1f.

[4] S. Bürger/Esslinger/Koy, DuD 2004, 135; Gesellschaft für Informatik e.V./ Informationstechnische Gesellschaft im VDE, DuD 2003, 763.

leisten.[5] Aus ökonomischer Sicht können nicht-verifizierbare Verträge als entbehrlich angesehen werden.[6] Daher bringen nur qualifizierte Signaturen einen nachhaltigen Nutzen.

Für die Integration einer privatwirtschaftlich angebotenen Funktion in ein staatliches Ausweisdokument werden neben rechtlichen Bedingungen durch wirtschaftspolitische Aspekte Nebenbedingungen gesetzt. Unter dem Gesichtspunkt der Gewährleistung eines freien Wettbewerbs auf dem Markt für Zertifizierungsdiensteanbieter ergeben sich durch mögliche Wettbewerbsverzerrungen Konsequenzen, die bei der Gestaltung von Integrationsvarianten berücksichtigt werden müssen. Ein Wettbewerb unter den Zertifizierungsdiensteanbietern sichert auch einen Innovationswettbewerb, durch den neue Produkt- und Prozessvariationen hervorgebracht werden, die ohne den Markt unentdeckt oder zu mindestens ungenutzt blieben.[7] Der Wettbewerb als Entdeckungsverfahren stellt zu der fortlaufenden Entwicklung und der weltweiten Vernetzung des Internets ein passendes Konzept dar, das besonders für technologieabhängige Aufgaben auch in den Integrationsmodellen gesichert werden sollte.

1.2 Synergieeffekte

In den bisherigen Geschäftsmodellen werden Signaturkarten als eigenständige Produkte vertrieben. Mit einem eigenen Registrierungsprozess wird die Signaturfunktion auf separaten Chipkarten angeboten. Auf Basis heute technisch realisierbarer multifunktionaler Chipkarten ist es jedoch möglich, eine Signaturfunktion in bestehende und schon etablierte Karten zu integrieren.[8] Nutzen Signaturfunktion und Ausweis ein gemeinsames physikalisches Medium werden Synergien möglich, die zur Kostensenkung genutzt werden können.

Zertifizierungsdiensteanbieter müssen alle mit dem Angebot qualifizierter Signaturen und Zertifikate zusammenhängenden Dienstleistungen als Pflichtdienstleistungen anbieten. Hierzu zählen die Registrierung des Nutzers (Identifizierung, Namensgebung, Feststellung von Attributen), die Schlüsselerzeugung, die Personalisierung und Zertifizierung der Signaturschlüssel, Unterrichtung und Übergabe der sicheren Signaturerstellungseinheit an den Nutzer, das Betreiben eines Verzeichnis- und Sperrdienstes, und das Führen einer Dokumentation nach § 10 SigG.[9] Es handelt sich hierbei sowohl um technikneutrale als auch um technologieabhängige Aufgaben.

Bei Ausweisdokumenten und Signaturkarten ist es notwendig, vor Erstellung und Ausgabe einen Registrierungsprozess abzubilden, in dem die Identität der Personen erfasst und überprüft wird. Synergieeffekte können im Rahmen einer Integration durch die Übertragung einzelner Aufgaben des Zertifizierungsdiensteanbieters auf die Ausweisinfrastruktur erzielt werden. Durch die gemeinsame Nutzung bereits vorhandener Infrastrukturen können insbesondere weitere Kostenreduktion und Vereinfachung von Abläufen und Prozessen erreicht werden. Zusätzlich kann auch ein Bekanntheits- oder Vertrauensvorschuss für die noch relativ unbekannte elektronische Signatur mitgenommen werden, indem diese mit einem bereits bekannten und positiv besetzten Ausweis in Verbindung gebracht wird. Schließlich kann auch die organisatorische Sicherheit von Verfahren für elektronische Signaturen selbst erhöht werden.

Zum Beispiel stellt ein digitaler Personalausweis ein sehr verbreitetes Ausweisdokument mit ca. 65 Mio. Exemplaren dar.

> Neben einer sehr hohen Identifikations- und Fälschungssicherheit hat ein staatlicher Ausweis auch ein Vertrauens- und Funktionsäquivalent, durch das er sich als Trägermedium einer Signaturfunktion gegenüber anderen Karten und Ausweisen qualifiziert.

2 Signaturrechtliche Vorgaben

Die Integration von Signaturfunktionen in einen staatlichen Ausweis wäre zulässig. § 4 Abs. 5 SigG erlaubt Zertifizierungsdiensteanbietern, Pflichtaufgaben nach dem Signaturgesetz an Ausweis ausgebende Stellen zu übertragen. Voraussetzung hierfür ist, dass die Gesamtverantwortung für das ordnungsgemäße Angebot von Zertifizierungsdienstleistungen beim Zertifizierungsdiensteanbieter verbleibt. Sichergestellt wird dies durch die Pflicht zur Einbeziehung der Kooperationspartner in das Sicherheitskonzept, Kontrollrechte der Regulierungsbehörde und Dokumentationspflichten des Zertifizierungsdiensteanbieters sowie durch die Regelung der Haftung in § 11 Abs. 4 SigG.

2.1 Sicherheitskonzept

Voraussetzung für eine Ausgliederung von Zertifizierungsdienstleistungen ist, dass der Zertifizierungsdiensteanbieter die Erfüllung der ihm übertragenen Aufgaben durch externe Auftragnehmer nach § 4 Abs. 5 SigG in sein Sicherheitskonzept so einbezieht, dass er die Sicherheitsanforderungen des Signaturgesetzes gewährleisten kann.

Nach § 2 SigV stellt der Zertifizierungsdiensteanbieter im Sicherheitskonzept seine Organisation, seine Sicherheitsmaßnahmen, die eingesetzten technischen Produkte, Vorstellungen zur Sicherheit des Betriebes und Verfahren zur Beurteilung und Sicherstellung der Zuverlässigkeit des eingesetzten Personals sowie verbleibende Risiken dar.[10] Das Gesamtkonzept muss dabei so ausgerichtet sein, dass die gesetzlichen Sicherheitsvorgaben erfüllt und in der Praxis umgesetzt werden.[11]

Durch die Übertragung von Aufgaben der Zertifizierungsdiensteanbieter an Dritte können sich neue Risiken ergeben, die bereits bei der Erstellung und Planung des Sicherheitskonzepts berücksichtigt werden müssen. In jedem Fall muss daher durch geeignete Auswahlkriterien die Zuverlässigkeit des eingesetzten Personals auch des beauftragten Dritten gewährleistet sein.

Besondere Sicherheitsmaßnahmen sind dann notwendig, wenn technologieabhängige Aufgaben an Dritte übertragen werden, die eine umfassende Anpassung oder Neukonzeption technischer und organisatorischer Abläufe erfordern. Die Übertragung technikneutraler Aufgaben stellt demgegenüber in der Regel ein geringeres Sicherheitsrisiko dar und erfordert einen geringeren technischen und organisatorischen Aufwand. Hierbei finden sich daher die größeren Synergiepotenziale.

2.2 Haftung

Als ein zentrales Mittel zur Gewährleistung des gesetzlich vorgeschriebenen Sicherheitsniveaus sieht § 11 SigG eine umfassende Verschuldenshaftung des Zertifizie-

[5] S. Roßnagel, NJW 2001, 1817.
[6] S. Schweitzer, Vertragstheorie, 1999.
[7] S. Fichert, Wettbewerbspolitik im digitalen Zeitalter, 2002.
[8] S. Scheuermann, in diesem Heft.
[9] S. ausf. Roßnagel, Einleitung ins SigG, in: ders. (Hrsg.), Recht der Multimediadienste, 6. EL, 2004, Rn. 24.
[10] S. Roßnagel, BB 2002, 261.
[11] S. Roßnagel/Hammer, in Roßnagel (Fn. 9), § 2 SigV, Rn. 19 ff.

rungsdiensteanbieters vor. Die Beweislast für die sorgfältige Erfüllung der gesetzlichen Sicherheitsanforderungen obliegt dem Zertifizierungsdiensteanbieter.[12]

Diese Haftung trifft den Zertifizierungsdiensteanbieter auch dann in vollem Umfang, wenn er einzelne Aufgaben nach § 4 Abs. 5 SigG anderen Unternehmen übertragen hat. Im Verhältnis zum Signaturschlüssel-Inhaber ergibt sich dies bereits aus § 278 BGB. Dritte, die der Zertifizierungsdiensteanbieter zur Erfüllung seiner Pflichtaufgaben heranzieht, sind seine Erfüllungsgehilfen, deren Verschulden ihm voll zugerechnet wird. Im Verhältnis zu jedem anderen, der auf die Sicherheit des verwendeten Signaturverfahrens vertraut, ergibt sich eine entsprechende Haftung aus § 11 Abs. 4 SigG. Für beauftragte Dritte muss der Zertifizierungsdiensteanbieter danach wie für eigenes Handeln einstehen, eine Möglichkeit zur Exkulpation nach § 831 BGB schließt § 11 Abs. 4 SigG ausdrücklich aus.

Im Schadensfall besteht für den Zertifizierungsdiensteanbieter jedoch die Möglichkeit zum Regress gegenüber dem beauftragten Dritten. Dieser muss dem Zertifizierungsdiensteanbieter für schuldhafte Verletzung des zugrunde liegenden Vertragsverhältnisses nach § 280 BGB einstehen. In Betracht kommt insbesondere die Verletzung von Sorgfaltspflichten, die der Einhaltung der Sicherheitsanforderungen des Signaturgesetzes dienen und unmittelbar oder mittelbar über das Sicherheitskonzept Vertragsbestandteil werden.

Das damit von der Ausweis ausstellenden Stelle übernommene zusätzliche Haftungsrisiko kann als beherrschbar angesehen werden. Werden gesetzliche Vorgaben und das geprüfte Sicherheitskonzept umgesetzt, ist ein Schadenseintritt unwahrscheinlich. Für den beauftragten Dritten ist das Bestehen der Regressmöglichkeit im Innenverhältnis ein weiterer Anreiz für die Einhaltung der vereinbarten Sicherheitsvorkehrungen.

3 Sicherung des Wettbewerbs

Die Einbindung von Signaturverfahren in bestehende Ausweisdokumente kann Auswirkungen auf den Markt für Zertifizierungsdienstleistungen bis hin zur Bildung monopolartiger Strukturen haben und damit einen Innovationswettbewerb zwischen Zertifizierungsdiensteanbietern gefährden.

Bei der Ausgestaltung der Rahmenbedingungen für elektronische Signaturen haben die Gesetzgeber auf europäischer und nationaler Ebene auf eine marktorientierte Regelung gesetzt. Dieser Ansatz lässt Kooperationsmodelle zur Förderung der Verbreitung sowohl unter privatwirtschaftlicher Form als auch unter staatlicher Beteiligung zu. Ein Innovationswettbewerb war bereits ausdrückliches Ziel des ersten deutschen Signaturgesetzes.[13] Ebenso stellt Erwägungsgrund 8 RLeS klar, dass die rasche technologische Entwicklung und der globale Charakter des Internets ein Konzept erfordern, das gegenüber unterschiedlichen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung prinzipiell offen steht.

Die Einflussnahme auf den Wettbewerb durch Kooperationen mit Zertifizierungsdiensteanbietern wird durch europäische Vorgaben zur Sicherung des freien Wettbewerbs im Binnenmarkt begrenzt. Im Falle staatlicher Maßnahmen zur Förderung von Signaturverfahren sind insbesondere die beihilferechtlichen Vorschriften der Art. 87 ff. EG zu beachten.

Allgemeine Infrastrukturmaßnahmen, die prinzipiell allen Unternehmen gleichermaßen zugute kommen, fallen jedoch nicht unter den Beihilfebegriff. Die Integration qualifizierter Signaturverfahren in Ausweisdokumente sollte daher grundsätzlich allen Zertifizierungsdiensteanbietern offen stehen. Beihilferechtlich irrelevant sind zudem wettbewerbsneutrale Begünstigungen, sofern für diese eine angemessene Gegenleistung erbracht wird. Für staatliche Infrastrukturleistungen, die einzelnen Zertifizierungsdiensteanbietern zugute kommen, muss daher eine angemessene Vergütung verlangt werden.

Aber auch wenn die speziellen beihilferechtlichen Bestimmungen nicht zur Anwendung kommen, sind die Vorgaben zur Gewährleistung der Dienstleistungsfreiheit nach Art. 50 EGV zu beachten. Diese verlangen nicht nur die Beseitigung aller Diskriminierungen im Wege der Inländergleichbehandlung, sondern auch die Aufhebung aller sonstigen Beschränkungen mit ähnlicher Wirkung für Anbieter aus anderen Mitgliedstaaten. Die Voraussetzungen für die Gewährleistung eines freien Dienstleistungsverkehrs für Zertifizierungsdiensteanbieter wurden mit der Harmonisierung der rechtlichen Rahmenbedingungen für elektronische Signaturen auf europäischer Ebene geschaffen. Sind die Voraussetzungen der Signaturrichtlinie erfüllt, so sind Produkte und Anwendungen im Geltungsbereich der Richtlinie anzuerkennen.

Für die Vergabe staatlicher Aufträge an einzelne Zertifizierungsdiensteanbieter stellen vergaberechtliche Vorschriften eine Sicherung des freien Wettbewerbs und Dienstleistungsverkehrs dar. Das Vergabeverfahren muss nach den einschlägigen europäischen Vergaberichtlinien transparent, fair und nach nicht diskriminierenden Kriterien durchgeführt werden. Insbesondere dürfen keine vergabefremden Kriterien angewendet werden. In diesem Rahmen ist die Begrenzung auf Anbieter qualifizierter Signaturverfahren zulässig, da nur diese umfassend im elektronischen Geschäftsverkehr eingesetzt werden können.

Eine Beschränkung auf ausschließlich inländische Anbieter oder Anbieter, die einer inländischen Aufsicht durch die Regulierungsbehörde unterliegen, ist nicht zulässig. Für die gegenseitige Anerkennung von Zertifizierungsdiensten trifft Art. 4 RLeS eine abschließende Regelung. Grundsätzlich müssen daher bei der Auswahl geeigneter Kooperationspartner alle Anbieter qualifizierter Zertifikate innerhalb des Geltungsbereichs der Richtlinie berücksichtigt werden.

Auch eine Beschränkung auf akkreditierte Zertifizierungsdiensteanbieter ist nur im Rahmen der engen Vorgaben des Art. 3 Abs. 7 RLeS möglich. Danach können die Mitgliedstaaten den Einsatz von elektronischen Signaturen nur eingeschränkt für spezifische Anwendungen im öffentlichen Bereich möglichen zusätzlichen Anforderungen unterwerfen. Im Zusammenhang mit der Förderung qualifizierter Signaturen sind jedoch keine solchen Gründe ersichtlich. Die Einbindung von Signaturfunktionalitäten in staatliche Trägermedien muss daher für alle Anbieter qualifizierter Zertifikate generell offen sein.

4 Integrationswege

Die Einbindung qualifizierter Signaturverfahren in staatliche Ausweisdokumente sollte den Ausweisinhabern als freiwillige Option angeboten werden. In diesem Fall ist zu erwarten, dass von den gegenwärtig ca. 65 Mio. Ausweisinhabern ca. 5 Mio. mittelfristig qualifizierte Signaturverfahren nut-

[12] S. Thomale, Haftung und Prävention nach dem Signaturgesetz, 2003, 123ff.; ders., MMR 2004, 80.

[13] BT-Drs. 13/7385, 16, 28.

zen werden. Eine generelle Ausstattung aller Ausweise mit Signaturfunktionalität ist daher schon aus Kostengründen nicht vertretbar.

Die Integration qualifizierter Signaturverfahren in staatliche Ausweisdokumente kann durch eine Aufteilung der Pflichtaufgaben zwischen Behörden und privatwirtschaftlichen Zertifizierungsdiensteanbietern sowie der gemeinsamen Nutzung der Chipkarte realisiert werden. Wird ausschließlich der Ausweis als Trägermedium für Signaturverfahren genutzt, ohne dass Ausweis ausgebende Stellen Aufgaben für Zertifizierungsdiensteanbieter übernehmen, können keine Synergien beim Registrierungs- und Produktionsprozess genutzt werden. Auch eine positive Wirkung auf die Verbreitung qualifizierter Signaturverfahren ist aufgrund der Freiwilligkeit der Signaturfunktion nicht zu erwarten. Übernehmen Behörden alle Aufgaben eines Zertifizierungsdiensteanbieters, können nennenswerte Synergieeffekte erzielt werden. Ein solcher staatlicher Zertifizierungsdiensteanbieter hätte aufgrund der weiten Verbreitung staatlicher Ausweisdokumente aber einen Wettbewerbsvorteil, der den Innovationswettbewerb gefährdet. Übernehmen die Behörden nur einen Teil der Aufgaben, als Dienstleistung für alle privaten Anbieter, verbleiben diese ohne staatliche Konkurrenz im Wettbewerb, gleichzeitig können Integrationsvorteile genutzt werden.[14]

4.1 Technikneutral

Übernehmen die Behörden die technikneutralen Aufgaben der Registrierung und Unterrichtung des Nutzers, wie auch die Übergabe der Signaturerstellungseinheit, entsteht ihnen dadurch kein nennenswerter zusätzlicher Aufwand und auch kein zusätzliches Haftungsrisiko.

Die Signaturfunktion wird in diesem Modell von verschiedenen Zertifizierungsdiensteanbietern als Option bei der Beantragung eines Ausweises mit angeboten. Die ausweisausgebenden Stellen haben insbesondere für eine ordnungsgemäße Identifizierung des Schlüsselinhabers bei der Registrierung und der Aushändigung des Ausweises als sicherer Signaturerstellungseinheit einzustehen. Da die Behörden einerseits diese schon im Eigeninteresse im Rahmen der Ausweisbeantragung vornimmt und andererseits auch die Registrierung durch private Anbieter aufgrund des Personalausweises oder eines „Dokuments von gleichwertiger Sicherheit“ erfolgen muss, kann durch die Übernahme von Identifizierungsaufgaben die Sicherheit qualifizierter Signaturverfahren erhöht werden. Die erforderliche gesonderte Übergabe des PIN-Briefs zur Aktivierung der Signaturfunktion kann in diesem Modell auch durch Dritte erfolgen, etwa durch die Post.

Die Zertifizierungsdiensteanbieter können sich auf die technologieabhängigen Aufgaben der Schlüsselgenerierung und dem Betreiben eines Verzeichnisdienstes konzentrieren, Investitionen und Unterhaltung einer Registrierungsinfrastruktur erübrigen sich. Ein Innovationswettbewerb bleibt für die technologieabhängigen Aufgaben erhalten. Als problematisch kann jedoch angesehen werden, dass der Ausweis im Produktionsprozess einem Zertifizierungsdiensteanbieter physikalisch zur Verfügung gestellt werden muss, um das Schlüsselpaar zu generieren und die Karte zu personalisieren. Die zusätzlichen Schnittstellen im Prozess erfordern insbesondere eine zusätzliche Koordination zwischen Ausweis ausgebenden Stellen und Zertifizierungsdiensteanbietern.

4.2 Vorpersonalisiert

Werden bei der Produktion des Personalausweises die Chipkarten bereits vorpersonalisiert, muss der Ausweis nicht mehr einem Zertifizierungsdiensteanbieter zur Verfügung gestellt werden, sondern lediglich elektronisch ein Zertifikatsantrag und Zertifikatsrequest übermittelt werden, worauf das zugehörige Zertifikat erstellt wird. Das Zertifikat selbst wird entweder auf elektronischem Wege in den Produktionsprozess eingebracht und auf den Ausweis geladen oder über eine Onlineanwendung dem Nutzer direkt zur Verfügung gestellt.

In diesem Integrationsmodell werden vom Staat neben den technikneutralen Aufgaben die Schlüsselgenerierung und eine Vorpersonalisierung der Signaturkarte übernommen und in den Produktionsprozess des Ausweises integriert. Dieser wird hierdurch geringfügiger beeinträchtigt und die Abläufe der Zertifizierungsdiensteanbieter werden weiter vereinfacht, aber der Innovationswettbewerb der kryptografischen Verfahren zur Schlüsselgenerierung verlagert sich. Die Auswahl der verwendeten Verfahren kann nicht mehr vom Nutzer getroffen werden, sondern wird in einem Zuliefererwettbewerb festgelegt. Es ist aber abzusehen, dass dadurch keine Beeinträchtigungen entstehen, da der Nutzer meist nicht in der Lage sein wird, die Qualität kryptografischer Verfahren zu beurteilen, um eine begründete Entscheidung zu treffen. Die Festlegung auf ein einheitliches Verfahren unterstützt darüber hinaus die Bemühungen um Interoperabilität.

Wird das Beschäftigungsfeld der Zertifizierungsdiensteanbieter auf einzelne Aufgaben konzentriert, können sich zudem veränderte Preismodelle etablieren. Eine Abkehr von den derzeitigen pauschalen Jahresbeiträgen hin zu einer Tarifierung der anfallenden Zertifikatsüberprüfungen wird für viele Anwendergruppen ihrem individuellen Nutzen besser entsprechen.

5 Fazit

Zur weiteren Verbreitung von qualifizierten Signaturkarten können mit der vorgestellten Integration Synergieeffekte genutzt werden. Durch simultane Prozessabläufe und einer erhöhten Stückzahl können insgesamt die Kosten für qualifizierte Zertifikate sinken. Die organisatorische Sicherheit wird für die elektronische Signatur zusätzlich erhöht, indem die Registrierung des Antragstellers für ein qualifiziertes Zertifikat durch die Ausweisbehörden bei Beantragung und Aushändigung eines neuen Ausweises übernommen werden.

Technische, rechtliche und wirtschaftliche Rahmenbedingungen können bei der Integration berücksichtigt werden. Verbleibende rechtliche und organisatorische Probleme lassen sich weiter minimieren, wenn die Kooperation zwischen Behörden und Zertifizierungsdiensteanbietern nicht als vertragliches Verhältnis ausgestaltet wird, sondern die Aufgaben der Behörden gesetzlich als Infrastrukturvorleistungen für den elektronischen Rechtsverkehr ausgestaltet werden.

Durch die Zusammenführung der Infrastrukturen für Signaturen und Ausweise können Kosten- und Akzeptanzhürden gesenkt werden. Erfolgt dies koordiniert mit zusätzlichen Anwendungsprojekten, kann die gegenwärtige ungünstige Ausgangslage überwunden werden. Im Ergebnis könnte die bisher selten genutzte Basistechnologie der qualifizierten Signatur zur alltäglichen Praxis des elektronischen Geschäftsverkehrs werden.

[14] S. ausf. Reichl/Roßnagel/Müller, Machbarkeitsstudie Digitaler Personalausweis, 2005, Teil II, 3.4.