Gerrit Hornung, Moritz Horsch, Detlef Hühnlein

Mobile Authentisierung und Signatur mit dem neuen Personalausweis

Innovative technische und rechtliche Lösungsansätze

Smartphones sind heute oftmals Dreh- und Angelpunkt unserer Kommunikation und ebenso wie der Personalausweis ein stetiger Begleiter. Ausgestattet mit NFC wird ein Smartphone zum Kartenleser und ermöglicht dadurch grundsätzlich die mobile Authentisierung mit dem neuen Personalausweis. Durch die innovative Kombination mit zusätzlichen Infrastrukturdiensten können hierdurch auch qualifizierte elektronische Signaturen erzeugt und dadurch Schriftformerfordernisse erfüllt werden.

Einleitung

Das Mobiltelefon entwickelt sich immer stärker zum fundamentalen Kommunikationsmedium unserer Gesellschaft und zählt heute zu unseren alltäglichen Begleitern. Deshalb liegt es nahe, ein Mobiltelefon als Grundlage einer ubiquitär und ergonomisch nutzbaren persönlichen Sicherheitsumgebung zu begreifen.

Vor dem Hintergrund der zunehmenden Verfügbarkeit von leistungsfähigen und mit der *Near Field Communication* (NFC) Technologie ausgestatteten Mobiltelefonen [1] bietet es sich an, den mit einer kontaktlosen Schnittstelle gemäß ISO/IEC 14443 [2] ausgestatteten *neuen Personalausweis* (nPA) [3] für die mobile Authentisierung und Signatur zu nutzen.

Der vorliegende Beitrag trägt in Abschnitt 1 die wichtigsten technischen und rechtlichen Grundlagen zusammen. Abschnitt 2 beleuchtet die Herausforderungen der mobilen Authentisierung und Signatur mit dem nPA. Abschnitt 3 stellt verschiedene innovative technische und rechtliche Lösungsansätze vor. In Abschnitt 4 werden die Vor- und Nachteile der verschiedenen Ansätze diskutiert. Darüber hinaus enthält der Beitrag eine kompakte Zusammenfassung der wesentlichen Erkenntnisse und schließt mit einem Ausblick auf zukünftige Entwicklungen ab.

Prof. Dr. Gerrit Hornung

ist Inhaber des Lehrstuhls für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik der Universität Passau.

E-Mail: gerrit.hornung@uni-passau.de

Moritz Horsch

ist Student an der Technischen Universität Darmstadt sowie Berater bei der ecsec GmbH und forscht seit 2009 an der mobilen Nutzung des nPA.

E-Mail: moritz.horsch@ecsec.de

Dr. Detlef Hühnlein

ist Geschäftsführer der ecsec GmbH und seit mehr als fünfzehn Jahren im Umfeld der elektronischen Signatur und Identität tätig.

E-Mail: detlef.huehnlein@ecsec.de

1 Grundlagen

Zu Beginn erläutern wir die rechtlichen und technischen Grundlagen zum nPA.

1.1 Recht

Der nPA enthält neben biometrischen Daten (vgl. [4]) die Möglichkeit zum Einsatz zweier Basisfunktionalitäten des elektronischen Rechtsverkehrs: den *elektronischen Identitätsnachweis* (eID-Funktion) als Authentisierungslösung und die Möglichkeit zum Erstellen *qualifizierter elektronischer Signaturen* (eSign-Funktion). Letztere ersetzt im Rechtsverkehr regelmäßig die Schriftform (v.a. gemäß § 126a Abs. 1 BGB und § 3a Abs. 2 VwVfG) und genießt den gesetzlichen Anscheinsbeweis des § 371a ZPO.

Gemäß § 18 Abs. 1 Satz 1 PAuswG kann der Personalausweisinhaber, der mindestens 16 Jahre alt ist, seinen Personalausweis dazu verwenden, seine Identität gegenüber öffentlichen und

nichtöffentlichen Stellen elektronisch nachzuweisen (vgl. [5, 6, 7]). Die besondere Qualität des elektronischen Identitätsnachweises liegt darin, dass seine Nutzung gemäß § 18 Abs. 4 PAuswG an die vorherige Übermittlung eines gültigen Berechtigungszertifikats durch den Dienstanbieter gekoppelt wird. Dieses erhalten nur Diensteanbieter, die in einem Prüfverfahren der *Vergabestelle für Berechtigungszertifikate* (VfB) nachweisen können, dass sie die Daten tatsächlich benötigen (vgl. [7, § 18 Rn. 19 ff.]). Während des eigentlichen Identifizierungsvorgangs werden die Daten aus dem Ausweis erst übertragen, nachdem sich der Diensteanbieter mittels des Zertifikats selbst authentisiert und der Ausweisinhaber mittels Eingabe der PIN seine Einwilligung erklärt hat.

Anders als bei den sehr detaillierten Regelungen zum elektronischen Identitätsnachweis hat sich der Gesetzgeber hinsichtlich der *qualifizierten elektronischen Signatur* (QES) sehr zurückgehalten. Als einzige Norm regelt § 22 PAuswG hierzu relativ lapidar: „Der Personalausweis wird als sichere Signaturerstellungseinheit im Sinne des § 2 Nr. 10 des Signaturgesetzes ausgestaltet. Die Vorschriften des Signaturgesetzes bleiben unberührt." (vgl. [7, § 22]). Damit wird rechtlich angeordnet, dass die technischen und organisatorischen Sicherheitsmechanismen, Ausgabeprozesse und Zertifikatsverwaltungen beim nPA denselben Anforderungen unterliegen wie bei anderen Signaturkarten. Das gilt auch für den Einsatz des elektronischen Identitätsnachweises im Rahmen der Beantragung des qualifizierten Zertifikats nach § 3 Abs. 1 Satz 2 SigV: Dies kann sowohl hinsichtlich eines Zertifikats für eine separate Signaturkarte als auch für ein auf den nPA nachzuladendes Zertifikat erfolgen.

Bei der Regelung des § 22 PAuswG hatte der Gesetzgeber die Hoffnung, dass durch die Bereitstellung einer sicheren Signaturerstellungseinheit für jeden Personalausweisinhaber ein Verbreitungshindernis der qualifizierten elektronischen Signatur behoben oder abgemildert werden würde. Neben den im Folgenden erörterten Problemen der Verfügbarkeit der entsprechenden Technik muss sich allerdings noch zeigen, ob allein die Verbreitung der Chipkarten das Problem beseitigen wird, dass Nutzer sich ein kostenpflichtiges Zertifikat zulegen müssen, ohne dass entsprechend attraktive Anwendungen bereitstehen.

Vor diesem Hintergrund ist es von Bedeutung, dass *Willenserklärungen* im Rechtsverkehr gemäß §§ 164 ff. BGB *auch durch Vertreter* abgegeben werden können. Sie wirken dann nach § 164 Abs. 1 Satz 1 BGB unmittelbar für und gegen den Vertretenen. Besitzt jemand also kein qualifiziertes Zertifikat, möchte aber dennoch eine elektronische Willenserklärung abgeben, die die Rechtsfolgen der qualifizierten elektronischen Signatur hinsichtlich Formerfüllung und Beweiswert erzeugt, so besteht die Möglichkeit, einen Vertreter, der über diese technische Möglichkeit verfügt, hierzu zu ermächtigen.

Im Allgemeinen ist eine solche Ermächtigung unproblematisch und formfrei möglich. Das Vertretungsrecht eröffnet sogar bei formbedürftigen Erklärungen die Möglichkeit einer formlosen Vollmachtserteilung: Diese bedarf gemäß § 167 Abs. 2 BGB nicht der Form, welche für das Rechtsgeschäft bestimmt ist, auf das sich die Vollmacht bezieht.

Selbst für formgebundene Erklärungen kann im Regelfall formfrei eine Vollmacht erteilt werden.

Auch wenn die Rechtsprechung angesichts der Risiken für den Vertretenen hiervon Ausnahmen macht (vgl. Abschnitt 4), wird doch die Möglichkeit der Autorisierung eines Dritten zur Erzeugung qualifizierter elektronischer Signaturen eröffnet.

Allerdings verlagert sich das Beweis- und Haftungsrisiko damit zumindest potentiell auf den Vertreter. Tritt er nach außen als solcher auf, kann im Streitfall die Vollmachtserteilung aber nicht beweisen, so haftet er *als Vertreter ohne Vertretungsmacht* („falsus procurator") dem Erklärungsempfänger nach dessen Wahl auf Vertragserfüllung oder Schadensersatz (§ 189 Abs. 1 BGB). Die Herausforderung für derartige Modelle ist deshalb, „unterhalb" der qualifizierten elektronischen Signatur für entsprechende technische Sicherheit zu sorgen, die dem Vertreter ein zumindest hinreichendes Sicherheitsniveau garantiert und so sein Haftungsrisiko beherrschbar werden lässt.

1.2 Technik

Der nPA ist mit einem Chip und einer kontaktlosen RFID-Schnittstelle gemäß ISO/IEC 14443 [2] ausgestattet. Neben der klassischen Anwendung als hoheitliches Ausweisdokument unterstützt der Ausweis den elektronischen Identitätsnachweis und ist als sichere Signaturerstellungseinheit ausgeprägt (vgl. [8, 9]). Damit kann der Ausweis nach dem Nachladen eines qualifizierten Zertifikats und in Verbindung mit einem Komfort-Chipkartenleser [10] zur Erstellung qualifizierter elektronischer Signaturen genutzt werden.

1.2.1 eID-Funktion

Der *elektronische Identitätsnachweis* (eID-Funktion) ermöglicht eine Registrierung und Anmeldung bei Dienstanbietern im Internet. So können beispielsweise die erforderlichen Daten (z.B. Name, Anschrift) bei einer Registrierung bei einem Online-Shop direkt vom Ausweis gelesen werden. Auch die Anmeldung im Internet, die heute vorwiegend mit Benutzername und Passwort erfolgt, kann mit der eID-Funktion zukünftig in einer sehr sicheren Art und Weise mit dem nPA erfolgen. Der technische Authentisierungsvorgang mit der eID-Funktion erfolgt jedoch in der Regel nicht direkt durch die Dienstanbieter, sondern wird von speziellen eID-Service-Providern in dessen Auftrag durchgeführt. Der eID-Service-Provider fungiert als „entferntes Authentisierungsterminal" (siehe [11, Abschnitt 3.2.2 und Annex C.4.2]). Dabei wird mit dem *Extended Access Control* (EAC) Protokoll, das über die in [12] definierten Schnittstellen mit einem eCard-API-konformen Client (vgl. [13, 14]) und einem eID-Server [15] abgewickelt wird, insbesondere die nach § 18 Abs. 4 PAuswG (vgl. Abschnitt 1.1) erforderliche Zugriffsberechtigung für die auf dem nPA gespeicherten Daten nachgewiesen.

Für das EAC-Protokoll und das für die PIN-basierte Absicherung der RFID-Schnittstelle eingesetzte *Password Authenticated Connection Establishment* (PACE) Protokoll existieren Sicherheitsbeweise (siehe [16, 17]). Im Rahmen dieser Protokolle werden dem Ausweisinhaber bei der eID-Funktion die im Berechtigungszertifikat enthaltenen Informationen gemäß § 18 Abs. 4 PAuswG, wie z.B. die Identität des Dienstanbieters und der Zweck der Datenübermittlung, angezeigt. Da das Berechtigungszertifikat gemäß [18] bzw. [11, Annex C] direkt durch den nPA ausgewertet und geprüft wird, ist technisch sichergestellt, dass nur ein rechtmäßiger Zugriff auf die im Ausweis gespeicherten Daten erfolgen kann. Außerdem kann der Ausweisinhaber bei Bedarf bestimmte Datengruppen im Einzelfall von der Übermittlung aus-

schließen, und er muss der Verarbeitung durch Eingabe der eID-PIN explizit zustimmen oder den Vorgang abbrechen. Vor diesem Hintergrund kann die technische Realisierung des elektronischen Identitätsnachweises auf Basis von EAC und PACE ohne Zweifel als datenschutz- und sicherheitstechnisch beispielgebend bezeichnet werden.

Der elektronische Identitätsnachweis auf Basis von EAC und PACE bietet ein Höchstmaß an Sicherheit und Datenschutz.

1.2.2 eSign-Funktion

Die *elektronische Signaturfunktion* (eSign-Funktion) des nPA ermöglicht das Erstellen von *qualifizierten elektronischen Signaturen* (QES) [9] und damit das digitale Unterschreiben von elektronischen Dokumenten.

Hierbei muss zwischen dem Vorgang des Nachladens des qualifizierten Zertifikates und der späteren Nutzung des Zertifikates für die Erstellung von qualifizierten elektronischen Signaturen unterschieden werden. Während beim Nachladen eines qualifizierten Zertifikates gemäß [9] eine entfernte EAC-Authentisierung gegenüber einem Zertifizierungsdiensteanbieter erfolgt (dies wird nunmehr durch § 3 Abs. 1 Satz 2 SigV rechtlich ausdrücklich zugelassen), wird im Regelfall bei der späteren Signaturerstellung eine lokale EAC-Authentisierung gegenüber dem als „Signaturterminal" (siehe [11, Abschnitt 3.2.3 und Annex C.4.3]) fungierenden Komfort-Chipkartenleser [10] durchgeführt. Wie in [10, Abschnitt B.7] bzw. [20] festgelegt, muss der private und zur Terminalauthentisierung genutzte Schlüssel des Komfort-Chipkartenlesers in der Regel in einem gemäß [21] nach *Common Criteria* mit *Assurance Level* EAL 4+ zertifizierten Sicherheitsmodul aufbewahrt und angewandt werden. Außerdem muss die auf dieses Sicherheitsmodul zugreifende Software bzw. Firmware gemäß Common Criteria mit Assurance Level EAL 3 zertifiziert sein, wobei in [10] empfohlen wird, das hierfür notwendige *Security Target* an das Schutzprofil [22] für hoheitliche Inspektionssysteme anzulehnen. Darüber hinaus ist in [10] klargestellt, dass für die Zertifizierung eines Komfort-Chipkartenlesers, der als Teil einer Signaturanwendungskomponente gemäß § 17 Abs. 2 SigG zu betrachten ist, eine Bestätigung gemäß Signaturgesetz notwendig ist. Die Anforderungen sind damit deutlich höher als hinsichtlich der eID-Funktion.

Im Hinblick auf den mobilen Einsatz des nPA spielt die *Near Field Communication* (NFC) Technologie gemäß ISO/IEC 18092 [23] und ISO/IEC 21481 [24] eine wesentliche Rolle. Hierbei handelt es sich um eine Funktechnologie zum Datenaustausch über wenige Zentimeter. Anders als die bereits etablierten Technologien wie WLAN oder Bluetooth erfordert NFC kein Einrichten einer Verbindung: Das einfache Zusammenführen der Geräte stellt eine Verbindung her. Des Weiteren erlaubt NFC eine Kommunikation mit passiven Komponenten, die selbst über keine Energieversorgung verfügen, wie RFID-Tags und kontaktlosen Chipkarten gemäß ISO/IEC 14443 [2] wie dem nPA. NFC weist jedoch noch Inkompatibilitäten zu ISO/IEC 14443 auf, so dass viele aktuell auf dem Markt verfügbare NFC-fähige Geräte noch Kommunikationsprobleme mit dem Ausweis haben. Die technische Machbarkeit wurde jedoch bereits mit einem älteren Gerät gezeigt [31].

2 Problemstellung

Damit der nPA für die mobile Authentisierung und Signatur genutzt werden kann müssen eine Reihe von Problemen gelöst werden:

- **Mobile eID-Applikation**
  Ein grundsätzliches Problem für die mobile Nutzung des nPA ist, dass die AusweisApp des Bundes [13] sowie vergleichbare eID-Clients [25, 26] bislang nur für PC-Plattformen verfügbar sind, während für die mobile Nutzung beispielsweise eine Unterstützung von Android [27] oder iOS [28] notwendig wäre.
- **Gestaltung des Nachladeprozesses**
  Während die technischen Abläufe für die Aktivierung der Signaturfunktionalität in [9] spezifiziert sind, scheinen bei der organisatorischen Ausgestaltung eines vollständig elektronischen Nachladevorgangs noch einige Detailfragen offen zu sein (siehe auch [29]).
- **Mobiler Komfort-Chipkartenleser**
  Selbst wenn mobile eID-Clients und Ausweise mit nachgeladenem qualifizierten Zertifikat zur Verfügung stehen sollten, kann damit im mobilen Umfeld noch keine qualifizierte elektronische Signatur erzeugt werden, da die eSign-Funktion des nPA erst nach der EAC-Authentisierung durch ein Signaturterminal – also beispielsweise in einem Komfort-Chipkartenleser – zugreifbar ist. Diese Funktionalität wird von heutigen Smartphones nicht bereitgestellt (vgl. Abschnitt 3.3).

3 Lösungsansätze

Im Folgenden werden Lösungsansätze beschrieben, die eine mobile Authentisierung und Signatur mit dem nPA ermöglichen. Ein NFC-fähiges Smartphone bildet die Grundlage für die mobile Nutzung des nPA.

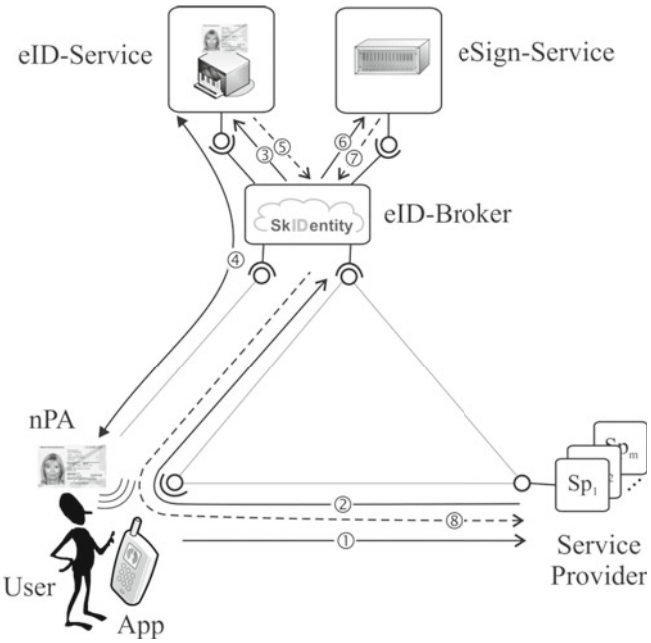
3.1 Mobiler Kartenleser

In der einfachsten Ausführung fungiert ein NFC-fähiges Smartphone nur als Kartenleser für den Ausweis. Die Aufgabe beschränkt sich auf das Weiterleiten der Datenübertragung. Das Smartphone, das als Basis-Chipkartenleser gemäß [10, Abschnitt 3.1] fungiert, lässt sich beispielsweise per USB oder Bluetooth mit dem Computer oder Notebook verbinden. Die Nutzung der Ausweisfunkionen erfolgt weiterhin über den Computer und die auf dem Computer installierte eID-Applikation.

Die Funktion des Smartphones lässt sich jedoch erweitern, so dass die Eingabe der PIN auf dem mobilen Gerät erfolgt und dieses daraufhin das PACE-Protokoll [30] ausführt. Damit kann ein Aufzeichnen der PIN durch Schadsoftware auf dem Computer verhindert werden. In diesem Fall fungiert das Smartphone als ein Standard-Chipkartenleser gemäß [10, Abschnitt 3.2].

Zum jetzigen Zeitpunkt besteht jedoch eine Diskrepanz zwischen den Anforderungen an Chipkartenleser für den nPA [10] und den Eigenschaften, Möglichkeiten und der technischen Realisierbarkeit eines mobilen Kartenlesers. Das heißt, dass beispielsweise gewisse Sicherheitsanforderungen auf mobilen Geräten nur durch zusätzliche Hardwaremodule realisierbar sind, die nicht in allen Geräten genutzt werden können. Allerdings erhöht die PIN-Eingabe auf dem mobilen Kartenleser bereits das Sicherheitsniveau im Vergleich zum Einsatz eines Basis-Chipkarten-

Abb. 1 | Mobile Authentisierung und Signatur mit dem nPA



lesers, so dass die Schaffung spezifischer Kriterien bzw. Klassen für mobile Kartenleser erwogen werden sollte.

3.2 Mobile eID-Applikation

Die Funktionen des Ausweises lassen sich aber auch direkt vom Smartphone aus nutzen, so dass beispielsweise die eID-Funktion für Anmeldungen auf Webseiten verwendet werden kann, die im Web-Browser des Smartphones geöffnet werden. In diesem „vollmobilen" Szenario vereint das Smartphone den Computer und den Kartenleser in einem Gerät. Dies erfordert jedoch eine mobile eID-Applikation wie beispielsweise MONA [31], die wie auf dem Computer die Interaktion mit den einzelnen Komponenten durchführt.

3.3 Mobiler und verteilter Komfort-Chipkartenleser

Die Nutzung der eSign-Funktion des nPA erfordert einen Komfort-Chipkartenleser gemäß [10, Abschnitt 3.3], dessen Anforderungen mit einem Smartphone nicht ohne weiteres realisierbar sind. Wie in Abschnitt 1.2.2 näher erläutert, müsste nämlich auch bei der Realisierung eines mobilen Komfort-Chipkartenlesers ein EAL 4+ zertifiziertes Sicherheitsmodul eingesetzt werden und die Software müsste gemäß EAL 3+ zertifiziert und gemäß SigG bestätigt sein. Da nicht in jedem Smartphone ein geeignetes EAL 4+ zertifiziertes Sicherheitsmodul genutzt werden kann, wurde in [19] ein Verfahren zur verteilten Signaturerzeugung (verteilter Komfort-Chipkartenleser) beschrieben, bei der das Smartphone und ein spezieller eID-Server mittels *Secret-Sharing Verfahren* [32] die erforderlichen Protokollschritte zum Ausführen der eSign-Funktion gemeinsam durchführen. Anstatt einer eSign-PIN werden verteilte PIN-Listen verwendet, so dass weder auf dem Smartphone noch beim eID-Server die signaturauslösende und deshalb besonders schützenswerte[1] eSign-PIN vorliegt.

3.4 Bevollmächtigte QES

Da sowohl beim Nachladevorgang für das qualifizierte Zertifikat als auch bei der möglichen Realisierung eines mobilen oder verteilten Komfort-Chipkartenlesers sehr hohe technische und regulatorische Hürden überwunden werden müssten, wäre es äußerst fraglich, ob ein System für die mobile Signatur mit dem nPA überhaupt wirtschaftlich[2] sinnvoll realisiert werden könnte.

Vor diesem Hintergrund erscheint der im Folgenden näher erläuterte „rechtliche Lösungsansatz" deutlich vielversprechender. Hierbei wird ein Signaturdienst vom Ausweisinhaber nach einer entsprechenden Authentisierung mit dem nPA formfrei bevollmächtigt, in seinem Auftrag eine qualifizierte elektronische Signatur zu erzeugen.

Wie in Abschnitt 1.1 und [33] erläutert, muss eine Vollmacht gemäß § 167 Abs. 2 BGB nicht der Form genügen, die für das Rechtsgeschäft bestimmt ist, auf das sich die Vollmacht bezieht. Deshalb kann in sehr vielen praxisrelevanten Anwendungsfällen die qualifizierte Signaturerzeugung ohne signifikante rechtliche Nachteile an einen bevollmächtigten Dritten delegiert werden.

Vollmacht und starke Authentisierung als Ersatz für eigenhändige qualifizierte elektronische Signatur.

Wie in Abbildung 1 angedeutet, besteht das System für die bevollmächtigte qualifizierte elektronische Signatur mit dem nPA aus dem

- *Benutzer* (User), der mit einem nPA und einer mobilen eID-Applikation (z.B. der „Open eCard App" [14]) ausgestattet ist, einem
- *Dienstanbieter* (Service Provider), mit dem der Benutzer ein formgebundenes Rechtsgeschäft durchführen will, einem
- *Authentisierungsdienst* (eID-Service), der die Authentisierung mit dem nPA durchführt, einem
- *Signaturdienst* (eSign-Service), der die qualifizierte elektronische Signatur im Auftrag des Benutzers erzeugt und schließlich dem
- *Vermittler* (eID-Broker, wie bereits im SkIDentity Projekt genutzt [38]) der den Ablauf steuert.

Nach der Initialisierung der Transaktion (1) erfolgt eine Umleitung zum eID-Broker (2), der die Authentisierung am eID-Service anstößt (3). Im Zuge der Authentisierung (4) bevollmächtigt der Benutzer den Signaturdienst in seinem Namen eine qualifizierte elektronische Signatur zu erzeugen (5-7), um das formgebundene Rechtsgeschäft zu tätigen, bevor schließlich die erstellte Signatur samt Informationen über die Vollmacht zum Dienstanbieter zurückgeliefert werden (8).

Das Verfahren läuft dabei vorwiegend automatisiert ab. Die Interaktion des Benutzers ist nur bei der Authentisierung (4) erforderlich.

1 Zu Sicherheitsanforderungen bzgl. PIN und PUK im Signatur-Umfeld siehe auch [34].

2 Wirtschaftliche Aspekte der mobilen Signatur werden z.B. in [35, 36, 37] diskutiert.

4 Diskussion

Ein NFC-fähiges Smartphone als reiner mobiler Kartenleser ermöglicht den Einsatz des Ausweises am stationären Rechner und im mobilen Umfeld verbunden mit einem Notebook. Die Nutzung des nPA mit dem Smartphone erfordert eine mobile eID-Applikation, deren technische Realisierbarkeit in [31] gezeigt werden konnte. Es verbleiben jedoch Herausforderungen in Bezug auf die NFC-Technologie, Sicherheitsanforderungen und aktuelle Geräteplattformen. Insbesondere in Bezug auf die Realisierung eines mobilen Komfort-Chipkartenlesers sind sehr hohe technische und regulatorische Hürden vorhanden, so dass die bevollmächtigte QES als deutlich vielversprechender erscheint.

Unter dem Gesichtspunkt der Vollmachtserteilung müssen drei Fragen unterschieden werden.

Erstens ist signaturrechtlich zu konstatieren, dass die qualifizierte elektronische Signatur als Funktionsäquivalent zur eigenhändigen Unterschrift die allgemeinen Vertretungsregeln zulässt. Es ist also möglich, dass der Vertreter mit einem eigenen qualifizierten Zertifikat agiert und seine Vertretungsmacht dabei offenlegt. Problematisch wäre es dagegen aus signaturrechtlicher Sicht, wenn die sichere Signaturerstellungseinheit des Vertretenen im Gewahrsam des Vertreters wäre, dieser die PIN eingeben würde und der Vorgang nach außen intransparent bleiben würde. Dies wäre mit der Grundkonzeption der qualifizierten elektronischen Signatur nicht vereinbar.

Zweitens stellt sich das erwähnte Problem der Haftung als Vertreter ohne Vertretungsmacht, sofern es dem Vertreter nicht gelingt, die Vollmachtserteilung im Einzelfall nachzuweisen. Da diese in den beschriebenen Modellen gerade nicht mittels qualifizierter elektronischer Signatur erfolgen soll, kommt der Vertreter nicht in den Genuss von § 371a ZPO, sondern ist im Einzelfall darauf angewiesen, die Vollmachtserteilung zur Überzeugung des Gerichts nachzuweisen. Dabei wird es wesentlich auf die technische Sicherheit der eingesetzten Verfahren ankommen, die über Zertifizierungen oder gerichtliche Sachverständige im Prozess thematisiert werden.

Drittens kann die Frage der Formerfüllung (v.a. nach §§ 126a ZPO, 3a VwVfG) auftreten – allerdings nur dann, wenn das Hauptgeschäft tatsächlich formbedürftig ist, was bei den allermeisten Rechtsgeschäften nicht der Fall ist. Liegt ein Formerfordernis vor, so ist zu berücksichtigen, dass die Regelung in § 167 Abs. 2 BGB nach Meinung von Rechtsprechung und Literatur in mehrfacher Hinsicht zu weit geraten ist (vgl. [39, 40, 41]). Um den Vertretenen vor Übereilung und Umgehung der gesetzlichen Formerfordernisse zu schützen, nimmt die Rechtsprechung – der Sache nach zur Erfüllung der Warnfunktion der jeweiligen Formerfordernisse – entgegen dem Wortlaut der Norm eine Formbedürftigkeit der Vollmachtserteilung insbesondere an, wenn

- die Vollmacht unwiderruflich erteilt worden ist[3] oder bei Grundstücksgeschäften den Interessen des Bevollmächtigten dient und von diesem sofort verwertet werden kann,[4]
- die Nichtvornahme des Geschäfts eine Vertragsstrafe oder sonstige Nachteile für den Vertretenen zur Folge hätte,[5]
- bei Grundstücksgeschäften der Bevollmächtigte ausschließlich den Anweisungen des Vertragspartners unterliegt,[6]
- es sich um eine Bürgschaft handelt, und der Vollmachtgeber kein Kaufmann ist[7] oder
- der Bevollmächtigte vom Verbot des Selbstkontrahierens (§ 181 BGB) befreit wird, falls sich daraus bereits eine rechtliche oder tatsächliche Bindung des Vollmachtgebers ergibt.[8]

Darüber hinaus hat der Gesetzgeber bestimmte Ausnahmen geregelt: Formbedürftig sind die Vollmacht zum Abschluss eines Verbraucherdarlehens (§ 492 Abs. 4 Satz 1 BGB), die Vorsorgevollmacht (§§ 1904 Abs. 5 Satz 2 und 1906 Abs. 5 Satz 1 BGB), die Vollmacht zur Ausschlagung der Erbschaft (§ 1945 Abs. 3 BGB) und zur Ablehnung der fortgesetzten Gütergemeinschaft (§ 1484 Abs. 2 BGB); weitere Ausnahmen finden sich im Gesellschaftsrecht (§§ 2 Abs. 2, § 47 Abs. 3 GmbHG, §§ 134 Abs. 3, 135 AktG). Daneben kann zwischen den Parteien auch rechtsgeschäftlich vereinbart werden, dass die Vollmachtserteilung formbedürftig ist.

In diesen Fällen ist das beschriebene Modell mithin gesetzlich oder rechtsgeschäftlich unzulässig. Im Übrigen kann man im Umkehrschluss davon ausgehen, dass eine formfreie Bevollmächtigung zumindest grundsätzlich zulässig ist; dies gilt allerdings nur vorbehaltlich der beschriebenen durch die Rechtsprechung entwickelten Ausnahmen. Diese sind für die qualifizierte elektronische Signatur allerdings weithin irrelevant, weil sie sich insbesondere auf Grundstücksgeschäfte und Bürgschaften beziehen. Erstere unterliegen jedoch nicht nur Schriftform, sondern gemäß § 331b Abs. 1 Satz 1 BGB der notariellen Form. Für letztere ist nach § 766 Satz 2 BGB die elektronische Form ohnehin vollständig ausgeschlossen.

Fazit

Hinsichtlich der Erfüllung der Form wird man im Ergebnis zwischen verschiedenen Formanforderungen zu unterscheiden haben, weil diese teilweise unterschiedliche Funktionen erfüllen (vgl. [39, 40]). Da allerdings nur die wenigsten Rechtsgeschäfte für die hier beschriebenen Anwendungen formbedürftig sind und die in der Rechtsprechung problematisierten Fallgruppen für die qualifizierte elektronische Signatur überwiegend nicht relevant sind, führt dies nicht zu wesentlichen Umsetzungshindernissen. Letztlich entscheidet sich die Umsetzbarkeit des Modells deshalb an der Frage der Beweisbarkeit der Vollmachterteilung, die auch über eine etwaige Haftung des Bevollmächtigten als Vertreter ohne Vertretungsmacht bestimmt (vgl. Abschnitt 1.1). Angesichts der hohen Sicherheitseigenschaften der eID-Funktion des nPA erscheinen die Risiken als beherrschbar. Erforderlich sind allerdings effektive Sicherungsmittel hinsichtlich des Inhalts der Erklärung, die vom Inhaber des nPA zum Signieren an den eSign-Service übermittelt wird. Eine direkte Weiterleitung durch diesen würde das Risiko bergen, dass auf dem Übermittlungsweg Fehler oder Manipulationen erfolgen. Deshalb wird im oben beschriebenen Modell die Erklärung zunächst an den Inhaber des nPA zurück übermittelt, welcher diese weiterleitet. So ist ihm eine Kontrolle des Inhalts möglich, bevor eine Weiterleitung an den

3 S. für Grundstücksgeschäfte BGH, NJW 1952, 1210; s.a. BGH, NJW 1979, 2306, NJW 1998, 1857.
4 BGH, WM 1965, 1006; BGHZ 132, 119, 124 f.
5 BGH, NJW 1971, 93; NJW 1971, 557.
6 RGZ 97, 334; 104, 236; KG, DNotZ 1986, 290.
7 BGHZ 132, 119.
8 RGZ 104, 237; 108, 125; BGH, NJW 1952, 1210;

Service Provider erfolgt. Damit werden auch die Beweisprobleme hinsichtlich Inhalt und Urheberschaft [42] deutlich vermindert.

In Ergebnis eröffnet die bevollmächtigte qualifizierte elektronische Signatur deshalb eine zusätzliche und bereits heute nutzbare Realisierungsoption, durch die der nPA ähnlich wie andere Europäische Bürgerkarten [43] für die mobile qualifizierte elektronische Signatur genutzt werden kann.

Literatur

[1] SJB Research: *NFC-world homepage*, http://www.nfcworld.com/nfc-phones-list

[2] ISO/IEC: *Identification cards – Contactless integrated circuit cards – Proximity cards*, ISO/IEC 14443, International Standard, Part 1 – 4, 2008 – 2011.

[3] BSI: *Architektur Elektronischer Personalausweis*, BSI-TR-03127, Version 1.14, 2011

[4] G. Hornung, *Die digitale Identität*, 2005, 146 ff., 178 ff., 346 ff. et passim.

[5] A. Roßnagel, G. Hornung, *Ein Ausweis für das Internet. Der neue Personalausweis erhält einen „elektronischen Identitätsnachweis"*, DÖV 2009, SS 301-306.

[6] A. Roßnagel, G. Hornung, C. Schnabel, *Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht*, DuD 2008, SS 168-172.

[7] G. Hornung, J. Möller, *Passgesetz und Personalausweisgesetz. Kommentar*, 2011.

[8] A. Roßnagel: *Der elektronische Personalausweis als sichere Signaturerstellungseinheit*, DuD, 07/2009, SS. 403-408.

[9] BSI: *eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit*, BSI-TR-03117, Version 1.0, 2011

[10] BSI: *Anforderungen an Chipkartenleser mit nPA Unterstützung*, BSI-TR-03119, Version 1.2, 2011

[11] BSI: *Advanced Security Mechanisms for Machine Readable Travel Documents*, BSI-TR-03110, Version 2.05, 2011

[12] BSI: *eCard-API-Framework*, BSI-TR-03112, Teil 1-7, Version 1.1.1, 2011

[13] BSI: Offizielles Portal für die AusweisApp, https://www.ausweisapp.bund.de

[14] D. Hühnlein, M. Horsch & al.: *On the design and implementation of the Open eCard App*, Sicherheit 2012.

[15] BSI: *eID-Server*, BSI-TR-03130, Version 1.5, 2011

[16] O. Dagdelen, M. Fischlin: *Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents*, ISC 2010, SS. 54-68

[17] J. Bender, M. Fischlin, D. Kuegler: *Security Analysis of the PACE Key-Agreement Protocol*, 2009

[18] ISO/IEC: *Identification cards Integrated circuit cards Part 8: Commands for security operations*, 2004

[19] J. Braun, M. Horsch, A. Wiesmaier, D. Hühnlein: *Mobile Authentisierung und Signatur*, D-A-CH Security 2011, September 2011

[20] BSI: *Certificate Policy* **für die** *eSign-Anwendung des ePA*, Version 1.0.1, 2010

[21] CEN: *prEN 14169-1 Protection Profile for Secure signature creation device Part 2: Device with key generation*, BSI-CC-PP-0059

[22] BSI: *Common Criteria Protection Profile for Inspection Systems*, BSI-CC-PP-0064

[23] ISO/IEC: *Information technology Telecommunications and information exchange between systems Near Field Communication Interface and Protocol (NFCIP-1)*, ISO/IEC 18092, International Standard, 2004.

[24] ISO/IEC: *Information technology Telecommunications and information exchange between systems Near Field Communication Interface and Protocol-2 (NFCIP-2)*, ISO/IEC 21481, International Standard, 2005

[25] bos GmbH & Co. KG: *Governikus Autent*, 2011

[26] Ageto Innovation GmbH: *AGETO AusweisApp*, 2011

[27] Google Inc.: *Android*, http://www.android.com

[28] Apple Inc.: *iOS* 5, http://www.apple.com/de/ios/

[29] BNetzA: *Hinweis zur Signatur-Funktion des neuen Personalausweise*, http://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Hinweise/Signaturfunktion_nPA.html

[30] A. Wiesmaier, M. Horsch, J. Braun, F. Kiefer, D. Hühnlein, F. Strenzke, J. Buchmann: *An efficient mobile PACE implementation*, In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS '11, SS. 176-185

[31] M. Horsch: *Mobile Authentisierung mit dem neuen Personalausweis (MONA)*, Master Thesis, TU Darmstadt, Juli 2011

[32] A. Shamir: *How to share a secret*, Communications of the ACM 22, 612-613, 1979

[33] D. Hühnlein: *How to Qualify Electronic Signatures and Time Stamps*, EuroPKI 2004, SS. 314-321

[34] BNetzA: *Beschlüsse der 37. Sitzung der Arbeitsgemeinschaft anerkannter Bestätigungsstellen (AGAB) vom 04.03.2009 – PIN-/PUK-Techniken bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 SigG*, 2009

[35] L. Fritsch, H. Roßnagel: *Die Krise des Signaturmarktes: Lösungsansätze aus betriebswirtschaftlicher Sicht*, Sicherheit 2005, SS. 315-326

[36] H. Roßnagel, D. Royer: *Wirtschaftlichkeit mobiler qualifizierter Signaturen im E-Government*, GI Jahrestagung 2006, SS. 451-458

[37] H. Roßnagel: *On Diffusion and Confusion – Why Electronic Signatures Have Failed*, TrustBus 2006, SS. 71-80

[38] D. Hühnlein, G. Hornung, H. Roßnagel, J. Schmölz, T. Wich, J. Zibuschka: *SkIDentity – Vertrauenswürdige Identitäten für die Cloud*, D-A-CH Security 2011, SS. 296-304

[39] K.-H. Schramm: *Kommentierung zu § 167*, in: Münchener Kommentar zum BGB, 6. Auflage 2012.

[40] P. Rösler: *Formbedürftigkeit der Vollmacht – Eine Darstellung nach Fallgruppen*, NJW 1999, SS. 1150-1153.

[41] E. Schilken, *Kommentierung zu § 167*, in: Staudinger, BGB, Neubearbeitung 2009.

[42] G. Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, 2011, 226 ff.

[43] T. Zefferer, P. Teufl, H. Leitold: *Mobile qualifizierte Signaturen in Europa*, DuD 11/2011, SS. 768-774