Wirtschaftlicher Nutzen des neuen Personalausweises

Diplomarbeit

Enrico Popall | 1140545
Wirtschaftsinformatik

TECHNISCHE UNIVERSITÄT DARMSTADT

Enrico Popall
Matrikelnummer: 1140545
Studiengang: Diplom Wirtschaftsinformatik

Diplomarbeit
Thema: "Wirtschaftlicher Nutzen des neuen Personalausweises"

Eingereicht: 26. Februar 2010

Betreuer: Dr. Alexander Wiesmaier

Prof. J. Buchmann
Technische Universität Darmstadt
Fachbereich Informatik
Kryptographie und Computeralgebra
Hochschulstraße 10
64289 Darmstadt

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und noch nicht veröffentlicht.

Darmstadt, den 26. Februar 2010

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface
BGB	Bürgerliches Gesetzbuch
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
EAC	Extended Access Control
eID	elektronische Identität
EU	Europäische Union
FH	Fachhochschule
HBCI	Homebanking Computer Interface
ICAO	International Civil Aviation Organization
nPA	neuer Personalausweis
MRZ	Maschinenlesbare Zone
PersAuswG	Personalausweisgesetz
PACE	Password Authenticated Connection Establishment
PIN	Persönliche Identifikationsnummer
QES	Qualifizierte elektronische Signatur
SigG	Signaturgesetz
SigV	Signaturverordnung
SSEE	Sichere Signaturerstellungseinheit
TAN	Transaktionsnummer
VwVfG	Verwaltungsverfahrensgesetz

1 Einleitung und Aufbau der Arbeit

Zum 1.November 2010 wird die Bundesrepublik Deutschland einen neuen Personalausweis (nPA) einführen. Damit reagiert sie auf die immer größer werdende Bedeutung von Computern und dem Internet in unserer Zeit. Mit dem nPA soll ein Instrument geschaffen werden, dass den alltäglichen Bedarf des Nachweises der eigenen Identität auch im Internet befriedigen kann. Die Einführung eines neuen Ausweises ist ein großes Projekt, das den überwiegenden Teil der Bevölkerung betreffen wird. Dazu verursacht ein solches Projekt natürlich auch große Kosten, die vom Steuerzahler getragen werden müssen. Daher erwartet der Bürger von einem solchen Projekt berechtigterweise auch einen Nutzen, Der Nutzen dieses neuen Ausweises für die Wirtschaft soll in dieser Arbeit untersucht werden. Da der Ausweis noch nicht eingeführt ist, kann es sich dabei nur um eine Prognose handeln, deren Richtigkeit in einigen Jahren überprüft werden kann.

Abbildung 1 Der neue Personalausweis

Im ersten Kapitel werden dazu zunächst einmal der aktuelle Personalausweis und seine Funktionen betrachtet. Des Weiteren wird der neue Personalausweis vorgestellt und ein Blick in andere europäische Länder gewagt, die bereits ähnliche Projekte durchgeführt haben.

Kapitel zwei führt in einige grundsätzliche Begriffe technischer und wirtschaftlicher Natur ein, die für das Verständnis der Arbeit von Bedeutung sind. Um den Nutzen des nPA beurteilen zu können, ist es wichtig, diese Begriffe zu kennen und sie grob einordnen zu können.

Danach folgt in Kapitel drei eine Analyse der möglichen Anwendungsgebiete des nPA. Es werden die drei größten Gebiete, nämlich eCommerce, Online-Banking und eGovernment vorgestellt und die Nutzungspotentiale des nPA in diesen Gebieten beschrieben. Neben den drei großen Anwendungsgebieten wird auch versucht, andere Branchen ausfindig zu machen, in den der nPA von Bedeutung sein und einen Mehrwert bringen könnte.

Das vierte Kapitel untersucht den Nutzen, den alle Beteiligten aus der Verwendung des nPA ziehen und stellt die anfallenden Kosten dem gegenüber. Dazu werden Kosten und Nutzen für privatwirtschaftliche Unternehmen genauso betrachtet wie die Kosten und Nutzen für den Verbraucher. Eine Analyse der volkswirtschaftlichen Effekte schließt das Kapitel ab.

Schließlich wird im Fazit das zuvor behandelte noch einmal abschließend gewertet.

2 Der Personalausweis

2.1 Die aktuelle Situation

Um den Nutzen des neuen Personalausweises beurteilen zu können, ist es nötig, sich die aktuelle Situation vor Augen zu führen.

Derzeit ist jeder Bundesbürger nach der Vollendung des 16. Lebensjahres verpflichtet, einen Personalausweis zu besitzen. Dieser Ausweis enthält nach §1 PersAuswG folgende Angaben:

- Familienname und ggf. Geburtsname
- Vornamen
- Doktorgrad
- Tag und Ort der Geburt
- Größe
- Farbe der Augen
- gegenwärtige Anschrift
- Staatsangehörigkeit
- Lichtbild

Im hoheitlichen Bereich dient der Ausweis zur Identifizierung und als Reisedokument. Im für diese Arbeit interessanten Bereich der Privatwirtschaft ist der Personalausweis ein anerkanntes Dokument zur Identifizierung, zur Meldebescheinigung und zum Altersnachweis.

Der Personalausweis gilt in seiner heutigen Form als fälschungssicher[1]. Betrugsfälle ergeben sich hauptsächlich aus der Verwendung von gestohlenen oder gefundenen Ausweisen durch andere Personen als den eigentlichen Inhaber. Da die Prüfung der Identität durch einen Vergleich der Angaben auf dem Ausweis, insbesondere einem Vergleich des Lichtbilds mit der zu identifizierenden Person, erfolgt, kann bei genügender Ähnlichkeit ein nicht gefälschter Ausweis zur fehlerhaften Identifizierung einer Person genutzt werden. Derzeit sind nach Angaben des BMI 2,26 Millionen

1 Quelle: [Bun101]

Personalausweise als verloren oder gestohlen gemeldet. Verglichen mit den im Umlauf befindlichen 62 Millionen Ausweisen ergibt sich somit ein Anteil von rund 3,6%.

Der Ausweis verfügt auch über eine maschinenlesbare Zone (MRZ[2]). Diese stammt aus der Luftfahrtbranche und ist durch die ICAO standardisiert[3]. Sie ermöglicht, wie es der Name schon erahnen lässt, ein Auslesen der Daten des Ausweises durch standardisierte Lesegeräte. Typischerweise wird diese Funktion beim Check-In für Flüge verwendet. Da die ICAO die den Standard erstellende Behörde ist, gilt dieser Standard international.

Ausweichpflichtig sind alle deutschen Staatsbürger, die das 16. Lebensjahr vollendet haben. Der Ausweis ist normalerweise 10 Jahre gültig, wodurch sich ein jährlicher Umschlag von über 6 Millionen Ausweisen ergäbe. Tatsächlich gibt der Bund pro rund 8 Millionen Ausweise aus[4]. Die Differenz ergibt sich aus der kürzeren Laufzeit der Ausweise bei jüngeren Personen, Ersatzausweisen bei Verlust und Diebstahl sowie sonstigem Austausch

2.2 Der neue Personalausweis

Der neue, elektronische Personalausweis erweitert die Funktionalitäten des bisherigen Ausweises um elektronische Funktionen. Er ist weiterhin ein Dokument, mit dem eine Person per Sichtvergleich identifiziert werden kann. Der neue Personalausweis besitzt das Format einer Bank- oder Kreditkarte. Er wird über einen Chip verfügen, der per kontaktlosem Kartenleser auszulesen ist.

Neben den Möglichkeiten des aktuellen Personalausweises soll der neue Personalausweis um mehrere Funktionen erweitert werden. Diese sind nach Reichl[5]:

- Legitimationsfunktion
- Signatur- und Verschlüsselungsfunktion
- Authentifikationsfunktion
- Investitionsfunktion

2 MRZ steht für machine readable zone. Es befindet sich auch eine VIZ (visual inspection zone) auf ICAO-konformen Ausweisen.

3 Quelle: [ICA08]

4 Quelle: [Sch09]

5 Quelle: [Rei05]

- Nutzung des Innovationspotentials

Die Nutzung der Legitimationsfunktion spielt sich sowohl im hoheitlichen als auch im privatwirtschaftlichen Bereich ab. Bei der hoheitlichen Nutzung erhofft man sich durch Nutzung biometrischer Daten eine Verbesserung der Zuverlässigkeit der Identitätsfeststellung. Dies spielt zum Beispiel bei Grenzübertritten oder Personenkontrollen eine Rolle. Die Abwicklung dieser Prozesse kann durch den neuen Personalausweis sowohl in Zuverlässigkeit als auch in der Geschwindigkeit verbessert werden. So gibt es dafür beispielsweise am Flughafen Frankfurt schon ein Pilotprojekt, das allerdings den ePass benutzt[6]. Das Prinzip ist allerdings dasselbe, so dass eine Ausweitung dieser Art der Grenzkontrolle auch auf den neuen Personalausweis als realistisch erscheint.

Für den privatwirtschaftlichen Bereich ist die Legitimationsfunktion wohl der wichtigste Bestandteil am neuen Personalausweis. Es ermöglicht dem Inhaber sich auf elektronischem Weg, also insbesondere auch online, gegenüber einer anderen Instanz zu identifizieren. Dem Inhaber ist also theoretisch möglich, das Vorzeigen des Personalausweises für bestimmte Transaktionen in Zukunft auch online durchzuführen. Die daraus zu erwartenden Nutzenvorteile werden in Kapitel 5 näher erläutert.

Die zweite durchaus wichtige Funktion des nPA besteht in der Möglichkeit, Signaturen zu leisten und Verschlüsselungen von Daten durchzuführen. Zumindest, und dies ist eine Einschränkung gegenüber der Legitimationsfunktion, hat der Inhaber die Option, diese Funktion zu wählen. Da die Bereitstellung der Infrastruktur für diese Funktion Geld kostet und dies nicht über die normale Gebühr des Personalausweises abgedeckt ist, muss der Inhaber mit Zusatzkosten rechnen.

Die Authentifizierungsfunktion erweitert die zuvor angesprochene Identifikation um die Verifikation der angegebenen Identität. Es ist denkbar, dass bestehende Zugriffssysteme durch Systeme zu ersetzen, die den nPA benutzen. Möglich wäre dies

6 zB http://www.welt.de/reise/article4869536/Jetzt-kontrollieren-Automaten-schon-die-Reisepaesse.html

beispielsweise bei Rechnern oder Türen. Allerdings wäre zu prüfen, inwieweit solche Anwendungen wirklich praktikabel sind und einen Mehrwert gegenüber den bestehenden Systemen bieten, der über den der allgemein verfügbaren Karte hinausgeht.

Die Investitionsfunktion beschreibt die Wirkung des nPA als Maßnahme zur Förderung der Infrastruktur. Zum einen kommt die Einführung natürlich direkt den Unternehmen zu Gute, die Chipkarten und Leser produzieren. Zum anderen kann die Einführung des nPA aber auch als Investition in eine sichere Geschäftsumgebung im Internet gesehen werden.

Das Grobkonzept des BMI nennt zwei bedeutende Ziele bei der Entwicklung des nPA[7]:

- die Verbesserung der Zuverlässigkeit der Identifizierung in hoheitlichen Verfahren
- die Erhöhung der Transaktionssicherheit im elektronischen Geschäfts- bzw. Rechtsverkehr

Das erste Ziel spielt auf die schon besprochene Schwäche des aktuellen Personalausweises in hoheitlichen Verfahren an. Der Besitzer kann nur anhand des Lichtbildes identifiziert werden. Biometrische Daten sollen die Zuverlässigkeit der Identifizierung erhöhen und Betrug auf dem Wege der fälschlichen Nutzung eines gestohlenen oder verlorenen Ausweises verhindern. Dieses Ziel spielt für die Privatwirtschaft keine Rolle, da die biometrischen Daten nur von staatlichen Stellen ausgelesen werden können.

Das zweite Ziel der Erhöhung der Transaktionssicherheit betrifft sowohl die Privatwirtschaft als auch sämtliche Bemühungen, die unter dem Begriff eGovernment gefasst werden. Der neue Personalausweis soll es dem Bürger ermöglichen, seine Daten auf dem elektronischen Weg sicher, den Erfordernissen des Datenschutzes entsprechend zu verwenden und dabei die volle Kontrolle über diese Daten zu behalten.

[7] Siehe [Bun08]

2.3 Internationale Projekte

Zur Beurteilung des neuen Personalausweises ist es auch hilfreich, über die Landesgrenzen hinaus auf die entsprechenden Projekte anderer Länder zu schauen. Es existieren in Europa eine Reihe von vergleichbaren Projekten in den der bestehende Personalausweis um elektronische Funktionen erweitert wurde. Erfahrungen aus diesen Projekten lassen sich nutzen, um die Potentiale des deutschen Projektes zu untersuchen.

2.3.1 Belgien

2002 begann Belgien in einem Pilotprojekt, einen elektronischen Personalausweis einzuführen. Die auf dem Ausweis enthaltenen Daten können mit jedem Kartenleser ohne Einschränkung gelesen werden. Eine Sicherung über eine PIN erfolgt nicht. Der Ausweis enthält eine für jeden Inhaber eindeutige Identifikationsnummer. Biometrische Daten werden nicht auf dem Ausweis gespeichert. Die flächendeckende Einführung des Ausweises begann 2005, so dass bei einer üblichen Gültigkeitsdauer von 5 Jahren mit einer nahezu vollständigen Verbreitung des Ausweises in diesem Jahr gerechnet werden kann. Neben den Identitätsdaten können auch Zertifikate zum Signieren und Authentisieren auf der Karte gespeichert werden. Diese sind nur per PIN über die vom belgischen Staat zur Verfügung gestellte Middleware abrufbar.

Problematisch beim belgischen Modell ist, dass die Daten zur Identifizierung einer Person von jeder Anwendung gelesen werden können. Es ist daher auch möglich, diese auf andere Karten zu kopieren und damit Identitätsdiebstahl zu begehen[8]. Anwendungen, die auf die einfache Nutzung der Daten ohne Eingabe der PIN setzen, laufen somit Gefahr, Opfer von falschen Daten zu werden.

2.3.2 Niederlande

Der niederländische Personalausweis besitzt seit 2006 einen kontaktlosen Chip auf dem die nötigen Daten zur Nutzung im eGovernment gespeichert werden. Er ist trotz

8 Quelle: [Ver09]

der (im Moment) wenigen Nutzungsmöglichkeiten mit 31 Euro im europäischen Vergleich relativ teuer.

2.3.3 Estland

Auch in Estland gibt es seit 2002 elektronische Funktionen im Personalausweis[9]. Estland ist als Untersuchungsobjekt wohl am interessantesten, da der Staat jedem Bürger Zugang zum Internet garantiert. Dadurch lassen sich Aussagen über die Nutzung treffen, die sich nicht nur auf den Teil der Bevölkerung beschränken, die Zugang zum Internet haben. Es gilt eine Personalausweispflicht, was sich in einer hohen Verbreitung des Ausweises widerspiegelt[10]. Der Ausweis wird in Estland in vielen Bereichen des eGovernments genutzt. Daneben finden sich zahlreiche Banken und andere privatwirtschaftliche Unternehmen, die den Ausweis akzeptieren[11]. Es können auch Tickets im Nahverkehr gekauft werden[12]. Der Betreiber gibt die regelmäßige Nutzung mit 120.000 Personen an. Dies ist im Vergleich zur Einwohnerzahl ein als hoch einzuschätzender Wert von knapp 10%. Da sich dies natürlich nicht 1:1 auf Deutschland hochrechnen lässt, sind solche Zahlen als Vergleich nur bedingt geeignet. Sie geben dennoch einen Eindruck darüber, was mit der richtigen Strategie in punkto Nutzung erreicht werden kann.

Die Personendaten sind, wie auch beim belgischen Ausweis auf dem Chip nicht gesondert geschützt. Es wird aber auch hier eine Signatur- und Authentisierungsfunktion angeboten, die nur per PIN nutzbar ist. Bei Transaktionen im Bereich eGovernment ist die Nutzung der Signatur Pflicht. Esten können den Ausweis auch nutzen, um bei Wahlen ihre Stimme abzugeben.

Für in Estland lebende Personen, die nicht estnische Staatsbürger sind, besteht auch die Möglichkeit einen Ausweisersatz zu bekommen, der ähnliche Funktionen bietet.

9 Quelle: [IDA05]
10 Aktuelle Nutzungszahlen nach id.ee: rund 1,01 Millionen gültige Ausweise bei rund 1,3 Millionen Einwohnern.
11 Quelle: [ide10]
12 Quelle: [Uni10]

2.3.4 Italien

Der elektronische Personalausweis wird in Italien seit 2001 ausgegeben, seit 2006 ist bei der Neuausstellung die elektronische Variante Pflicht. Es werden neben den Personendaten auch biometrische Daten (Fingerabdrücke und Bild) gespeichert. Die Personendaten können wie auch beim belgischen Ausweis ohne weitere Beschränkung ausgelesen werden. Der Ausweis ermöglicht auch eine Speicherung von Zertifikaten zur Signierung und Authentisierung.

2.3.5 Schweden

Auch Schweden hat einen elektronischen Ausweis eingeführt. Der Ausweis hat sowohl einen kontaktbehafteten als auch einen kontaktftreien Chip. Die Funktionen werden zurzeit noch nicht benutzt. Der Ausweis ist im Vergleich mit 400 schwedischen Kronen, ca. 41 €, für fünf Jahre recht teuer.

2.4 Sicherheit und Technik des neuen Personalausweises

Grundlage für jegliche Art von Erfolg des neuen Personalausweises ist dessen Sicherheit. Das betrifft sowohl die Sicherheit auf Ebene der Fälschungssicherheit, wie sie schon aus dem alten Ausweis bekannt ist als auch die Sicherheit aller neuen Funktionen. Die Fälschungssicherheit des Ausweises stellt die Bundesdruckerei mit den bekannten Verfahren sicher. Es ist nicht zu erwarten, dass sich hier eine signifikante Änderung des Sicherheitsniveaus feststellen lässt. Es kann also davon ausgegangen werden, dass weiterhin nur eine sehr geringe Anzahl von gefälschten Ausweisen im Umlauf ist.

Für die Nutzung in der elektronischen Kommunikation ist allerdings die Fälschungssicherheit der optischen Eigenschaften der Karte nicht von Bedeutung. Hier ist sicherzustellen, dass sich der kontaktlose Chip, der auf dem neuen Ausweis zu finden sein wird, nicht kopieren lässt oder auf eine andere Art und Weise der Besitz eines gültigen Ausweises vorgetäuscht werden kann. Es muss sichergestellt sein, dass…

- …keine Daten während eines berechtigten Auslesevorgangs abgehört werden.
- …keine Daten während eines berechtigten Auslesevorgangs verändert werden.

- …keine Daten unberechtigt ausgelesen werden.
- …die Authentizität des Chips und der gespeicherten Daten jederzeit gegeben ist.
- …die Integrität des Chips und der gespeicherten Daten jederzeit gegeben ist.
- …nur die Daten ausgelesen, die den im Berechtigungszertifikat freigegeben sind.
- …der Aufenthaltsort des Inhabers nicht nachzuvollziehen ist.
- …das unbemerkte Wiedererkennen eines Ausweises verhindert wird.

Zum Erreichen der genannten Sicherheitsziele muss der Chip auf dem Ausweis und die Verbindung mit einem Dienstanbieter geschützt werden. Dazu wird auf die Verfahren Extended Access Control (EAC)[13], passive Authentisierung[14] sowie Password Authenticated Connection Establishment (PACE)[15] zurückgegriffen.

EAC stellt im Zusammenspiel mit PACE sicher, dass nur berechtigte Zugriffe auf die Daten auf dem Chip des Ausweises zugelassen werden. Es wird auch im ePass benutzt. Die passive Authentisierung ist im Allgemeinen eine Signierung der Daten auf dem Chip. Ein Kopieren lässt sich damit zwar nicht verhindern, aber es lässt sich feststellen, wenn Daten unberechtigt verändert wurden, da veränderte Daten die Signatur ungültig werden lassen. Beim neuen Personalausweis werden aber nicht die Daten selbst, sondern die Echtheit des Chips signiert. Signierte man die Daten, so hätte jeder Dienstanbieter vom Staat signierte Personendaten. Dies ist aus Datenschutzgründen und mit Blick auf den Adresshandel nicht wünschenswert. Zusätzlich gäbe es das Problem, dass man geänderte Daten wieder neu signieren müsste. Da der dazu notwendige Schlüssel allerdings ein zentrales Element in der Sicherheitsarchitektur des Ausweises ist, haben Meldestellen keinen Zugriff auf diesen Schlüssel und könnten somit die Daten auch nicht signieren. Durch die Authentisierung des Chips werden beide Probleme umgegangen und die Integrität und Authentizität der Daten implizit garantiert.

13 Quelle: [BSI10]
14 Quelle: [BSI101]
15 Quelle: [BSI102]

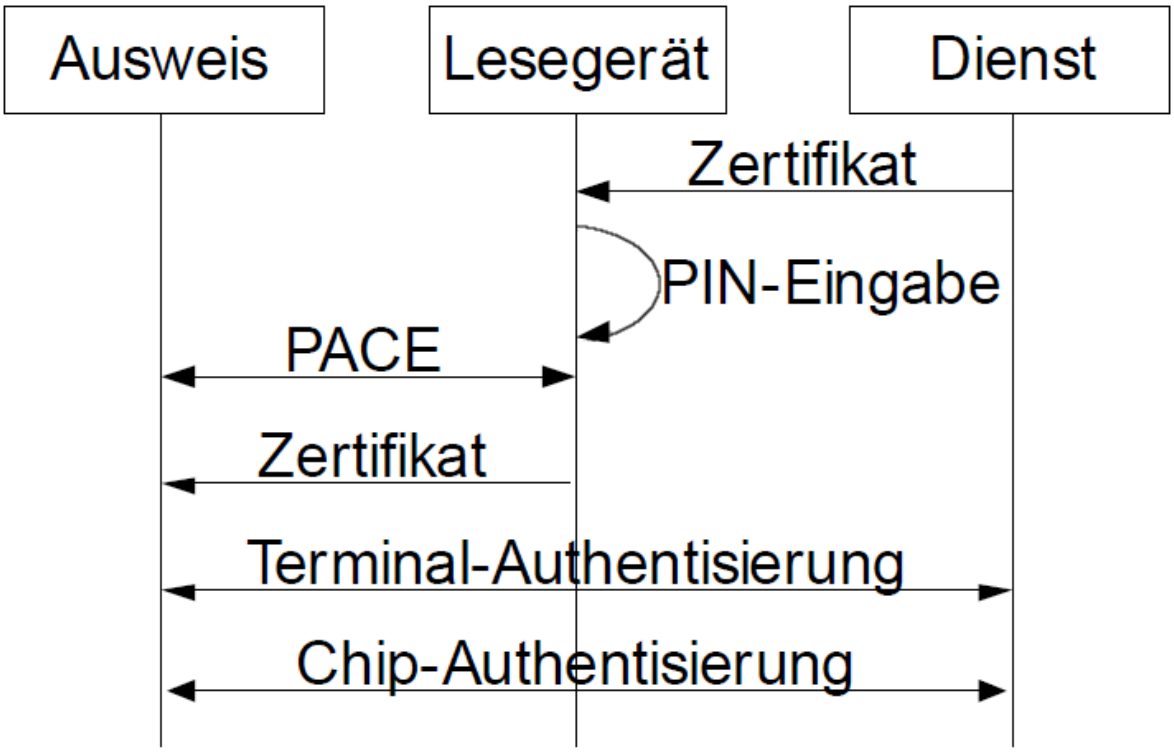

Abbildung 2 Zugriffskontrolle beim neuen Personalausweis, Quelle: [Ben08]

PACE ist ein neues Verfahren, in dem mittels der Eingabe einer PIN sowie der Authentisierung von Terminal und Chip sichergestellt wird, dass der Zugriff nur durch berechtigte Dienste erfolgen kann. Hoheitliche Lesegeräte erhalten einen PIN-freien Zugriff über ein anderes Verfahren, müssen sich dabei aber immer als hoheitliches Gerät identifizieren. Dem Missbrauch soll hier durch eine sehr kurze Gültigkeitsdauer der Zertifikate (wenige Tage) vorgebeugt werden.

Alle benutzten Verfahren basieren auf elliptischen Kurven und können daher zum heutigen Zeitpunkt als sicher angesehen werden.

Das Verhindern einer Rückverfolgung oder eines Wiedererkennens eines Ausweises wird durch eine variable Chip-UID erreicht, mit der der Chip mit einem Terminal kommuniziert.

Die Sicherheit der PIN ergibt sich aus ihren sechs Stellen in Verbindung mit der Limitation der Eingabe auf drei Versuche. Im Allgemeinen wird das System der vierstelligen PIN bei Bankkarten als sicher angesehen, daher kann auch hier von einem ausreichend sicheren Verfahren ausgegangen werden. Durch die PIN wird die missbräuchliche Benutzung eines gestohlenen oder verlorenen Ausweises verhindert.

Um die Inhaber des Ausweises vor dem unbefugten dreimaligen Eingeben der PIN über die kontaktlose Schnittstelle zu schützen, sieht PACE nachdem zweiten Fehlversuch die unbegrenzt mögliche Eingabe der auf dem Ausweis aufgedruckten Karten-PIN vor. Da ein Angreifer diese in der Regel bei einem Angriff über die kontaktlose Schnittstelle nicht sieht, kann dieser denial-of-service-Angriff mit ausreichender Wahrscheinlichkeit verhindert werden.

Es ist beim neuen Personalausweis auch möglich neben den Personendaten auch eine Altersverifikation durchzuführen. In Szenarien, in denen der Dienst nur die Berechtigung hat, zu prüfen ob ein Nutzer älter ist als ein vorgegebenes Alter, ist derselbe Dienst unter Umständen nicht berechtigt, das Geburtsdatum des Nutzers abzufragen. Hier bietet der Ausweis die Möglichkeit, eine Antwort in Form von ja oder nein auf die Frage zu geben, ob der Inhaber ein bestimmtes Alter überschritten hat. Dies ist nur einmal pro Authentisierungsvorgang möglich, so dass ein Dienst nicht durch mehrmaliges Abfragen des Überschreitens einer Altersgrenze das Geburtsdatum ermitteln kann. Das Gleiche Verfahren wird zur Überprüfung des Ablaufdatums des Ausweises verwendet.

Für den Fall, dass Nutzer wiedererkannt werden sollen und dem auch zustimmen, bietet der Ausweis die Möglichkeit der Nutzung von Pseudonymen. Da der Name alleine in vielen Fällen keine eindeutige Identifizierung des Nutzers ermöglicht, mehr Daten für den abfragenden Dienst aber nicht freigegeben werden, muss dieses Anwendungsszenario anders gelöst werden. Hierzu werden eine eindeutige Kennung des Chips und ein eindeutiges Kennzeichen des Dienstes zu einer Kennung zusammengeführt. Die Kennung des Anbieters kann von diesem nicht frei gewählt werden sondern wird von der ausstellenden Stelle festgelegt. Dadurch wird verhindert, dass Dienste untereinander ihre gespeicherten Pseudonyme vergleichen können und somit Bewegungsprofile erstellen.

3 Begriffsklärung

Zum besseren Verständnis der Terminologie in dieser Arbeit, werden im Folgenden einige Begriffe noch einmal kurz erläutert, die für das weitere Verständnis von Bedeutung sind.

3.1 Signatur

Es gibt zwei Arten von Signaturbegriffen, die in diesem Kontext unterschieden werden müssen: die digitale Signatur, ein Begriff aus der Kryptografie, und die elektronische Signatur, ein Begriff aus dem Rechtswesen.

Eine digitale Signatur ist ein kryptografisches Verfahren, mit dem die Integrität (Daten sind vollständig und unverändert) und Authentizität (Daten stammen aus der vorgegebenen Quelle) von Daten überprüft werden kann. Grundlage einer digitalen Signatur ist ein asymmetrisches Kryptosystem. In der Regel wird zum Berechnen der Signatur der Hashwert der zu signierenden Daten berechnet und dieser mit dem privaten Schlüssel des genutzten Kryptosystems verschlüsselt. Mit dem öffentlichen Schlüssel lässt sich die Signatur dann verifizieren.

Die elektronische Signatur erfüllt denselben Zweck auf einem elektronischen Dokument wie eine eigenhändige Unterschrift auf einem Papierdokument. Es existieren diverse Rechtsnormen, die die elektronische Signatur regeln:

- im europäischen Recht die Signaturrichtlinie (EG-Richtlinie 1999/93/EG)
- im deutschen Recht
    - die Signaturverordnung (SigV)
    - das Signaturgesetz (SigG)
    - Teile des Bürgerlichen Gesetzbuches (BGB)
    - Teile des Verwaltungsverfahrensgesetzes (VwVfG)

Das Signaturgesetz unterscheidet zwischen drei Formen der elektronischen Signatur:

- allgemeine elektronische Signatur
- fortgeschrittene elektronische Signatur

- qualifizierte elektronische Signatur

An die allgemeine elektronische Signatur werden keine besonderen Anforderungen gestellt. So ist die unverschlüsselte Angabe eines Absenders schon eine elektronische Signatur nach dem SigG. Dass sie nicht fälschungssicher ist, liegt auf der Hand. Eine fortgeschrittene elektronische Signatur erfordert einen geheimen Signaturschlüssel und der Signaturersteller muss identifizierbar sein. Ein Zertifikat ist nicht erforderlich. Vor einem Gericht wird die fortgeschrittene elektronische Signatur ähnlich behandelt wie die allgemeine elektronische Signatur. Dem Gericht unterliegt es, die Beweiskraft zu würdigen. Implizite Beweiskraft hat nur die qualifizierte elektronische Signatur (QES). Eine solche Signatur ist eine fortgeschrittene elektronische Signatur, die mit einem zum Zeitpunkt der Erstellung gültigen Zertifikat und mit einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde. Eine SSEE wird von einer anerkannten Stelle auf ihre Konformität mit dem SigG geprüft. Das nötige Zertifikat muss auf vertrauenswürdige Wurzelinstanz zurückgehen. Der neue Personalausweis wird die Möglichkeit haben, vom Staat ausgestellte Zertifikate zu speichern und somit mit Hilfe des Ausweises qualifizierte elektronische Signaturen ausstellen zu können.

3.2 Verschlüsselung

Unter eine Verschlüsselung von Information versteht man die Veränderung von Klartext mittels eines geheimen Schlüssels in nicht mehr lesbare Daten. Im Kontext des neuen Personalausweises sind vor allem die asymmetrischen Verschlüsselungsverfahren von Bedeutung. Hier wird, analog zum Verfahren beim Signieren, die Information mittels eines öffentlichen Schlüssels verschlüsselt. Der Empfänger der verschlüsselten Information kann dann mittels des nur ihm bekannten geheimen Schlüssels die Information wieder entschlüsseln.

3.3 Zertifikate

Ein Zertifikat ist eine digital signierte Sammlung von Daten, die benutzt wird um die Inhaber des jeweiligen Zertifikats zu identifizieren. Der Aussteller des Zertifikats ist entweder eine Stelle, der vertraut wird oder der Aussteller besitzt selbst ein Zertifikat

von einem vertrauenswürdigen Aussteller. In diesem Fall wird von einer Zertifikatskette gesprochen, da die Vertrauenswürdigkeit des Zertifikats über mehrere Schritte geprüft wird.

3.4 Identifizierung, Authentifizierung, Authentisierung

Die drei Begriffe Identifizierung, Authentifizierung und Authentisierung werden oft in einem Zusammenhang gebraucht und aufgrund ihrer ähnlichen Bedeutung oftmals verwechselt.

Identifizierung ist der Vorgang der Erkennung einer Person. Dies kann beispielsweise geschehen indem die Person ihren Namen sagt, indem man ihr Gesicht erkennt oder indem der Fingerabdruck mit einem bekannten Abdruck verglichen wird. Der Vorgang der Identifizierung sagt selbst noch nichts über die Richtigkeit der behaupteten Identität aus.

Unter einer Authentisierung versteht man den Vorgang, der die behauptete Identität glaubhaft machen will. Beispielsweise sendet ein Benutzer eine Kombination aus Name und Passwort an einen Server um sich zu authentisieren.

Authentifizierung versteht die Verifikation der behaupteten Identität. Beim vorher genannten Beispiel wäre der Vorgang der Authentifizierung also das Prüfen des angegebenen Namens und des Passworts mit den gespeicherten Informationen. Stimmt beides überein, so wird der Benutzer authentifiziert. Methoden um die Identität einer Person zu verifizieren sind der Nachweis von Wissen (also zum Beispiel ein Passwort), Besitz (zum Beispiel eine Zugangskarte) oder ein biometrisches Merkmal (zum Beispiel ein Fingerabdruck). Im Allgemeinen lässt sich sagen, dass die Zuverlässigkeit der Authentifizierung erhöht wird, wenn zwei oder alle drei Methoden kombiniert werden.

3.5 Wirtschaftlicher Nutzen

Die zentrale Frage dieser Arbeit ist, welchen Nutzen der neue Personalausweis hat. Diese Frage lässt sich aber nur beantworten, wenn überhaupt klar ist, was dieser Nutzen eigentlich ist und wie er sich messen lässt. Allgemein gesprochen spiegelt der

Nutzen die Befriedigung eines oder mehrerer Bedürfnisse wieder. Demgegenüber stehen in vielen Fällen auch Kosten, die mit dieser Befriedigung einhergehen. Die Differenz aus Nutzen und Kosten lässt sich somit als Nettonutzen charakterisieren. Wie und ob dieser Nutzen messbar ist, hängt immer von der Art und Weise der zu Grunde liegenden Entscheidung zusammen. Am einfachsten ist ein Vergleich offensichtlich, wenn er in Geldeinheiten ausgedrückt werden kann. So ist es leicht nachzuvollziehen, dass eine Entscheidung für eine Alternative immer dann getroffen wird, wenn der Betrag des Nettonutzens, ausgedrückt beispielsweise in Euro, höher ist als der einer anderen Alternative.

Leider lässt sich in den meisten Fällen keine derart simple Metrik finden. Oftmals muss sich die Bewertung des Nutzens auf eine Beschreibung desselben beschränken. Daher ist auch die Würdigung dieses Nutzens in diesen Fällen sehr subjektiv. Als ganz einfaches Beispiel lässt sich das eines Buchkäufers aufführen, der 10 Euro zur Verfügung hat und sich zwischen zwei Büchern für jeweils 10 Euro entscheiden muss. Er wird immer das nehmen, das ihm aufgrund seiner subjektiven Bewertung, den größeren Nutzen verspricht. Dieser lässt sich kaum in Zahlen fassen, dennoch lässt sich allein aus der Entscheidung für ein Buch auf eine subjektive Rangfolge der Bücher des Käufers schließen. Ein anderer Käufer kann eine völlig andere Rangfolge festlegen. Dies ist eine wichtige Erkenntnis, die auch für die Bewertung des Nutzens des neuen Personalausweises von Bedeutung ist. Stiftet der nPA für ein Individuum oder eine Organisation einen bestimmten Nutzen so impliziert das nicht zwingend, dass dieser Nutzen auch für andere Individuen oder Organisationen gestiftet wird. Ist eine Nutzenfunktion nicht quantifizierbar, so wird von einer ordinalen Nutzenfunktion gesprochen. Das Gegenteil, als eine quantifizierbare Nutzenfunktion, wird als kardinal bezeichnet.

Der Nutzen und die Kosten eines Gutes können direkt, indirekt oder intangibel sein. Direkter Nutzen ergibt sich aus den Eigenschaften eines Gutes selbst. Im Falle des nPA also unter anderem die Möglichkeit, sich auszuweisen. Direkte Kosten fallen bei der Beantragung des Ausweises an. Indirekter Nutzen ist beispielsweise die Möglichkeit, bei Reisen innerhalb der EU auf einen Reisepass verzichten zu können. Indirekte Kosten ergeben sich aus der Zeit, die für die Beantragung des Ausweises gebraucht

wird. Ein intangibler Nutzen des nPA kann die frühe Nutzung einer Innovation sein. Intagible Kosten des Ausweises sind beispielsweise Datenschutzbedenken bei den Inhabern. Diese Aufzählung soll nur Beispiele für die verschiedenen Kostenarten liefern und ist keinesfalls als vollständig zu verstehen.

Ein nur schwer lösbares Problem bleibt die Ermittlung eines Nettonutzens bei vielen unterschiedlichen Einflussfaktoren. Lässt sich der Nettonutzen noch relativ leicht bestimmen, wenn Kosten und Nutzen in Euro ausgedrückt werden können, so ist dies schon nicht mehr möglich, wenn einer der Faktoren nur beschrieben, nicht aber quantifiziert werden kann. Ein Nettonutzen lässt sich dann nur noch unter subjektiven Kriterien ermitteln. Es liegt in der Natur der subjektiven Einschätzung, dass dann äußerst unterschiedliche Bewertungen des Nettonutzens das Ergebnis sein können. Gerade beim nPA lässt sich in der öffentlichen Meinung ein breites Spektrum an Bewertungen feststellen. Von generell positiven Meinungen bis zu solchen, die die Gefahr der Verletzung des Datenschutzes und die Angst vor einem Überwachungsstaat übermäßig stark gewichten.

Betriebswirtschaftlicher Nutzen eines bestimmten Gutes kann auf allen Ebenen einer Organisation zu finden sein, sowohl im Bereich der eigentlichen Wertschöpfung, also dem Kern des Unternehmens, als auch in Bereichen, die nicht zum Kern gehören, wie zum Beispiel der Verwaltung. Auch hier sind selbstverständlich alle zuvor genannten Arten von Nutzen und Kosten zu finden. Für die Betrachtung des nPA erscheinen vor allem Kategorien wie Produktivität, Kosteneinsparungen in der Kommunikation und in der Logistik, Kundenbeziehungen und Service sowie Marketing interessant. Bereiche wie beispielsweise das Personalwesen oder das Controlling werden durch den nPA höchstwahrscheinlich nicht beeinflusst.

Mit dem volkswirtschaftlichen Nutzen verhält es sich ganz ähnlich, nur dass hier der Blick nicht mehr auf einzelne Unternehmen gerichtet ist, sondern versucht wird, Nutzen makroökonomisch zu analysieren. Das heißt, dass diese Perspektive die jeweilige Volkswirtschaft und den Nutzen von Gütern oder auch politischen Entscheidungen auf diese Volkswirtschaft als Ganzes im Blick hat. Ein ganz einfaches Beispiel hierfür ist die Erhebung von Steuern. Diese wird wohl von keinem

Unternehmen mit einem direkten Nutzen verbunden, volkswirtschaftlich gesehen sind sie allerdings, im richtigen Maß, durchaus sinnvoll.

3.6 Netzeffekte

Wird von Netzeffekten gesprochen, so ist damit der positive Effekt auf den Nutzen eines Gutes gemeint, den eine erhöhte Gesamtzahl der Nutzer auf den Nutzen eines einzelnen Nutzers hat. Dieses Phänomen hat zur Folge, dass für bestimmte Güter eine spezifische kritische Masse an Nutzern erreicht werden muss, damit der einzelne Nutzen die Kosten überwiegt. Das beliebteste Beispiel für einen Netzeffekt ist wohl das Telefon. Ein Telefon allein hat für den einzigen Nutzer gar keinen Nutzen, schließlich kann er es so nicht benutzen. Ein weiterer Nutzer erhöht den Nutzen schon, immerhin kann jetzt schon untereinander kommuniziert werden. Jeder weitere Anschluss erhöht den Nutzen für alle Beteiligten, da sie immer mehr Möglichkeiten der Nutzung bekommen. Für den nPA sind Netzeffekte insofern interessant, da für die Nutzung der neuen Funktionen Entwicklungsarbeit geleistet werden muss. Diese zahlt sich jedoch nur oder schneller aus, wenn eine möglichst große Masse an Ausweisen schnell in Umlauf gebracht wird. Ein weiteres Anwendungsfeld, die elektronische Signatur, hat seit ihrer legalen Einführung durch das Signaturgesetz genau das Problem, dass eine kritische Masse an Nutzern bisher nicht erreicht wurde[16]. Es ist zu vermuten, dass beispielsweise eine flächendeckende Signierung und Verschlüsselung von E-Mails Standard wäre, gäbe es genug Nutzer mit Zertifikaten zum Signieren. Eine kritische Masse scheint auf diesem Markt noch nicht erreicht.

[16] Quelle: [Fri]

4 Anwendungsbereiche

Um den Nutzen des nPA überprüfen zu können, muss zunächst untersucht werden, welche Anwendungsbereiche es überhaupt gibt. Grundsätzlich lässt sich hier zwischen den Bereichen unterscheiden, in denen heute schon der herkömmliche Personalausweis zum Einsatz kommt und solchen Bereichen, in denen zwar eine Authentifizierung und/oder Identifizierung erforderlich ist, dies aber nicht über den Personalausweis geschieht, typischerweise weil kein persönlicher Kontakt besteht.

Gebraucht wird der herkömmliche Personalausweis beispielsweise bei der Überprüfung des Alters beim Kauf von altersbeschränkten Artikeln im Einzelhandel. Einen Mehrwert bringt der nPA hier in einer ersten Überlegung wohl nicht. Die Informationen werden anhand der Sichtmerkmale des Personalausweises verifiziert. Der Einsatz der zusätzlichen Merkmale des nPA würde in solchen Situationen oft nur Mehraufwand bedeuten. Dieser Mehraufwand käme aus der zusätzlich benötigten Infrastruktur. Ist diese bereits vorhanden, so würde sie wohl auch genutzt. Dennoch erscheinen Vorteile hier nur marginal, so dass auf eine weitere Betrachtung verzichtet wird.

Daneben steht der nPA auch in Konkurrenz mit anderen Methoden zur Identifizierung. So ist beispielsweise an Zigarettenautomaten eine Verifikation des Alters auch mit einer Geldkarte möglich. Es ist fraglich, ob die Betreiber eine erneute Umrüstung der Automaten ohne wirklichen Mehrwert durchführen würden.

Einen Vorteil hat der nPA in Anwendungen, bei denen Information aus dem Personalausweis übertragen werden müssen. Als Beispiel sei die Eröffnung eines Bankkontos genannt, bei der ein Medienbruch und somit eine Fehlerquelle vermieden werden kann. Es stellt sich allerdings die Frage, ob es Anwendungen gibt, bei deren Ausführung der nPA einen Vorteil bietet, die nicht auch in den nächsten Abschnitt des eCommerce fallen. Um bei dem Beispiel des Bankkontos zu bleiben sei hier angemerkt, dass die Eröffnung nichts ist, was aus Prozesssicht mit Hilfe des nPA nicht auch am heimischen Computer durchgeführt werden könnte. Für die Eröffnung eines Kontos ist

neben dem beiderseitigen Willen der Parteien, ein Konto zu führen, eine Identifizierung des Kunden nötig.

Die Bundesregierung hat als ausgegebene Stelle des nPA die folgenden Anwendungsbereiche mit Partnern in der Wirtschaft getestet:

Name der Einrichtung	Test-Szenario
Air Berlin	Fluggastabfertigung
Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)	E Government Services
Allianz Deutschland AG	Kundenserviceprozesse im Versicherungsportal
ARGE eKFZ (Fraunhofer FOKUS; Christoph Kroschke AG; subreport; BDR; versch. Verwaltungen)	Teilprojekte eKFZ, Metaportal eVergabe und Premium EA (EU-DLR)
Bayerisches Landesamt für Steuern	Registrierungsverfahren für ELSTER (elektronische Steuererklärung)
bird.i ag & co. kg	Zutrittskontrolle, Zeiterfassung, Besucherverwaltung, Check-In in Hotels
CosmosDirekt	authentisierte Willenserklärungen und Mitteilungen
Datenzentrale Baden-Würtemberg	Online Gewerbeanzeige des Kommunalen Gewerbemanagements
Deutsche Emissionshandelsstelle (DEHSt) im Umweltbundesamt	Antrag auf Zuteilung von Emissionszertifikaten und Emissionsberichterstattung
Deutsche Kreditbank	Online Banking
Deutsche Rentenversicherung	eService der Deutschen Rentenversicherung
d-hosting GmbH	E Government Services
FRITZ & MACZIOL GmbH	elektronische Verwaltung von Entsorgungsnachweisen und Begleitscheinen
Fujitsu Technology Solutions	Fujitsu Online Shop Deutschland

Gothaer Allgemeine Versicherung	Antragstellung
Hagener E-Governmentkonsortium (Stadt Hagen; HABIT; Fernuniversität Hagen; IKS GmbH der FU Hagen, IFG CC, SAP)	Kommunale Verwaltungsdienstleistungen aus dem E Government Framework des virtuellen Rathaus 21
HSH Soft- und Hardware Vertriebs GmbH	E Bürgerservice
HUK24	Online-Versicherung
init AG in Zusammenarbeit mit der Arbeitsgruppe Extrapol	Unterstützung der länderübergreifenden Zusammenarbeit der Polizeien Rahmen der gemeinsamen Plattform "Extrapol"
InterCard AG	Kundenkarte mit Zahlfunktion
Lotterie-Treuhandgesellschaft	Registrierung und Altersverifikation für Glücksspiele
LVM-Versicherungen	Authentifizierung, Portalzugang, Adressübernahme
Schufa	Verbraucher-Onlineportal meineschufa.de und Online-Beantragung von Eigenauskünften
SIZ – Informatikzentrum der Sparkassenorganisation	Online-Beantragung von qualifizierten elektronischen Signaturen
Tönjes Holding AG	Identitätsnachweis bei Online-Zulassungen von Kfz
T-Systems Enterprise Services in Kooperation mit Innenministerium Baden-Württemberg:	"mein service-bw" im Verwaltungsdiensteportal Baden-Württemberg
Verkehrsverbund Rhein-Ruhr	eTicket-System
Willi Weber GmbH & Co. KG	Altersverifikation an Zigarettenautomaten
Wincor Nixdorf International	Authentifizierung an Geldautomaten oder Transaktionsterminals in Banken, Behörden und Industrie

Tabelle 1 Teilnehmer des Praxistest des BMI,Quelle: [ITB10]

Es lässt sich auf den ersten Blick eine recht große Vielfalt an Einsatzgebieten erkennen. Schwerpunkte lassen sich in den Bereichen eGovernment und Versicherungen

feststellen. eCommerce ist hingegen kaum ein Thema. Diese Tatsache überrascht sicher. Interessante Spezialfälle stellen das eTicket beim Verkehrsverbund Rhein-Ruhr sowie das Thema der Fluggastabfertigung bei airBerlin dar und werden später in diesem Kapitel noch näher besprochen.

Neben der Bundesregierung hat auch der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) einige Anwendungsszenarien in Workshops mit Partnern entwickelt[17]. Schwerpunkt dieser Betrachtung lag auf den Branchen

- Online-Handel,
- Luftverkehr,
- Banken und Versicherungen,
- regulierte Dienstleister und
- Logistik

Die Erkenntnisse aus beiden Workshops der BITKOM fließen in die folgenden Abschnitte ein.

4.1 eCommerce

Die nachfolgende Betrachtung konzentriert sich auf die Anwendungsmöglichkeiten des nPA im Bereich eCommerce. Dieser Bereich umfasst Transaktionen in der Privatwirtschaft die auf elektronischem Weg durchgeführt werden. Nicht betrachtet werden so genannte Business-to-business (B2B) Geschäfte. Der Grund hierfür liegt in der Natur dieser Geschäfte. Sie sind in der Regel nicht spontan und setzen eine nähere Bekanntschaft der Geschäftspartner voraus. Demzufolge kommen hier die Möglichkeiten des nPA nicht zum Tragen. Darüber hinaus ist der nPA in seiner Natur personengebunden und repräsentiert kein Unternehmen.

[17] Quellen: [BIT08] und [BIT07]

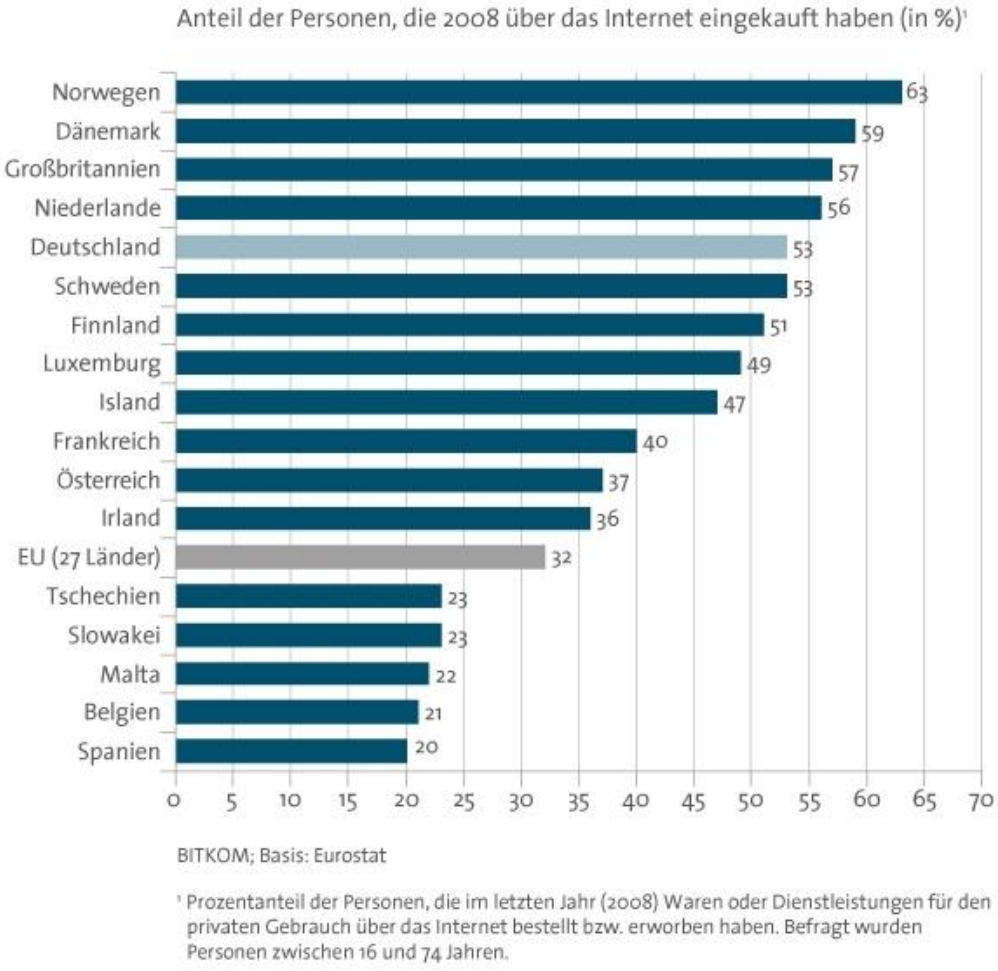

Abbildung 3 Nutzung von Online-Versandhandel im europäischen Vergleich, Quelle: [BIT093]

Geschäfte mit Verbrauchern kommen im Internet auf vielfältigen Wegen zu Stande.

Der augenscheinlichste ist wohl der Online-Handel. Beim Online-Handel tritt ein Unternehmen im Internet mit einem Webshop auf und verkauft seine Waren und Dienstleistungen an die Verbraucher.

Unterschieden werden kann dabei zwischen Händlern, die ausschließlich auf das Internet als Vertriebskanal setzen und solchen Händlern, die ihre Waren über mehrere Kanäle verkaufen, von denen das Internet einer ist (Multi-Channel-Versender). Das Volumen dieses Handels betrug 2009 laut Angaben des Bundesverbands des Deutschen Versandhandels bereits 15,5 Milliarden Euro in Deutschland[18]. Den größten Anteil am Gesamtumsatz hatten die Multi-Channel-Versender mit 5,8 Mrd. € gefolgt von den Versandhändlern, die nur im Internet aktiv sind, mit 4,5 Mrd. €. Der Anteil online durchgeführter Geschäfte im Versandhandel beträgt 53,3% am Gesamtumsatz des Versandhandels in Deutschland. Abbildung 3 zeigt die Bedeutung das eCommerce im europäischen Vergleich anhand des Anteils der Bevölkerung, die ihn nutzt. Es lässt sich erkennen, dass in Deutschland bereits heute relativ viele Geschäfte online durchgeführt werden. Jedoch ist nicht zu vermuten, dass sich daraus eine Sättigung des Marktes schließen lässt. Dieser Anteil von 42% in 2008 wird tendenziell aufgrund weiterer Verbreitung von breitbandigen Internetanschlüssen eher noch steigen.

Zusätzlich zum Versandhandel fallen auch online durchgeführte Dienstleistungen unter den Begriff eCommerce. Diese hatten 2008 ein Volumen von 6,2 Mrd. €.

Eine weitere sehr beliebte Art des eCommerce sind Online-Auktionen. Marktführer ist das Auktionshaus eBay mit 14,5 Millionen registrierten Nutzern und 3,1 Milliarden Euro Handelsvolumen[19].

Online-Versandhandel sowie Online-Auktionen sind Anwendungsfelder für den nPA, weil beide Geschäftsmodelle sicherstellen müssen, dass sich der Kunde korrekt identifiziert.

18 Quelle: [Bun10]
19 Quelle [eBa10]

4.2 eGovernment

Unter dem Begriff eGovernment verbirgt sich die Interaktion des Bürgers mit staatlichen oder kommunalen Organen auf dem elektronischen Weg. Oder genauer:

„Electronic Government ist eine Organisationsform des Staates, welche die Interaktionen und Wechselbeziehungen zwischen dem Staat und den Bürgern, privaten Unternehmungen, Kunden und öffentlichen Institutionen durch den Einsatz von modernen Informations- und Kommunikationstechnologien (IKT) integriert.“[20]

Folglich sind die Einsatzmöglichkeiten auch ähnlich vielfältig, wie die Leistungen, die ein Bürger in Anspruch nehmen kann oder muss. Schedler [Sch00] unterscheidet eGovernment in drei Felder:

- Electronic Democracy and Participation (eDP)
- Electronic Production Networks (ePN)
- Electronic Public Services (ePS)

Unter eDP umfasst die „elektronische Abwicklung demokratisch legitimierender Entscheidungsverfahren“, insbesondere also Wahlen, die auf dem elektronischen Weg durchgeführt werden. Es ist leicht nachvollziehbar, dass der nPA hier zum Einsatz kommen kann. Politische Wahlen bauen unter anderem darauf auf, dass jede Stimme das gleiche Gewicht hat. Mit dem nPA kann bei Wahlen über das Internet analog zum Register in jedem Wahllokal sichergestellt werden, dass jeder nur eine Stimme hat und auch nur seine Stimme und nicht die anderer abgegeben kann.

In den Bereich ePN fallen Formen der Zusammenarbeit zwischen öffentlichen Stellen untereinander oder mit privatwirtschaftlichen Einrichtungen. Dies ist unter dem Gesichtspunkt der Anwendungsbereiche des nPA weniger relevant.

Unter ePS fallen alle Leistungen, die eine öffentliche Stelle schließlich erbringt. Die Vielzahl von Möglichkeiten lässt sich schon aus Tabelle XX erahnen. So gut wie alle Leistungen, die von öffentlichen Stellen erbracht werden, lassen sich online zumindest

20 Quelle: [Sch00]

vorbereiten. Beantragt man beispielsweise einen Pass, so wird die Kontrolle des benötigten Lichtbilds immer noch vor Ort vorgenommen werden, aber andere Formalitäten wie das Ausfüllen von Formularen können schon vorher online passieren. Andere Verwaltungsakte wie zum Beispiel eine Gewerbeanmeldung könnten gänzlich online durchgeführt werden.

Die Bundesregierung teilt das Thema eGovernment in ihrem Umsetzungsplan in vier Handlungsfelder auf[21]:

- Portfolio
- Prozessketten
- Identifikation
- Kommunikation

Unter Identifikation fällt der nPA selbst als zentrales Element der gesamten eGovernment-Strategie. Das Feld Portfolio umfasst die meisten bürgernahen Dienstleistungen staatlicher Stellen, die für den nPA relevant sind. Als Beispiele sind genannt:

- Kommunikation mit der Arbeitsagentur
- Kommunikation mit der Deutschen Rentenversicherung
- Steuererklärungen auf dem elektronischen Weg
- Meldewesen
- Personenstandswesen
- Kfz-Wesen

[21] Quelle: [Bun091]

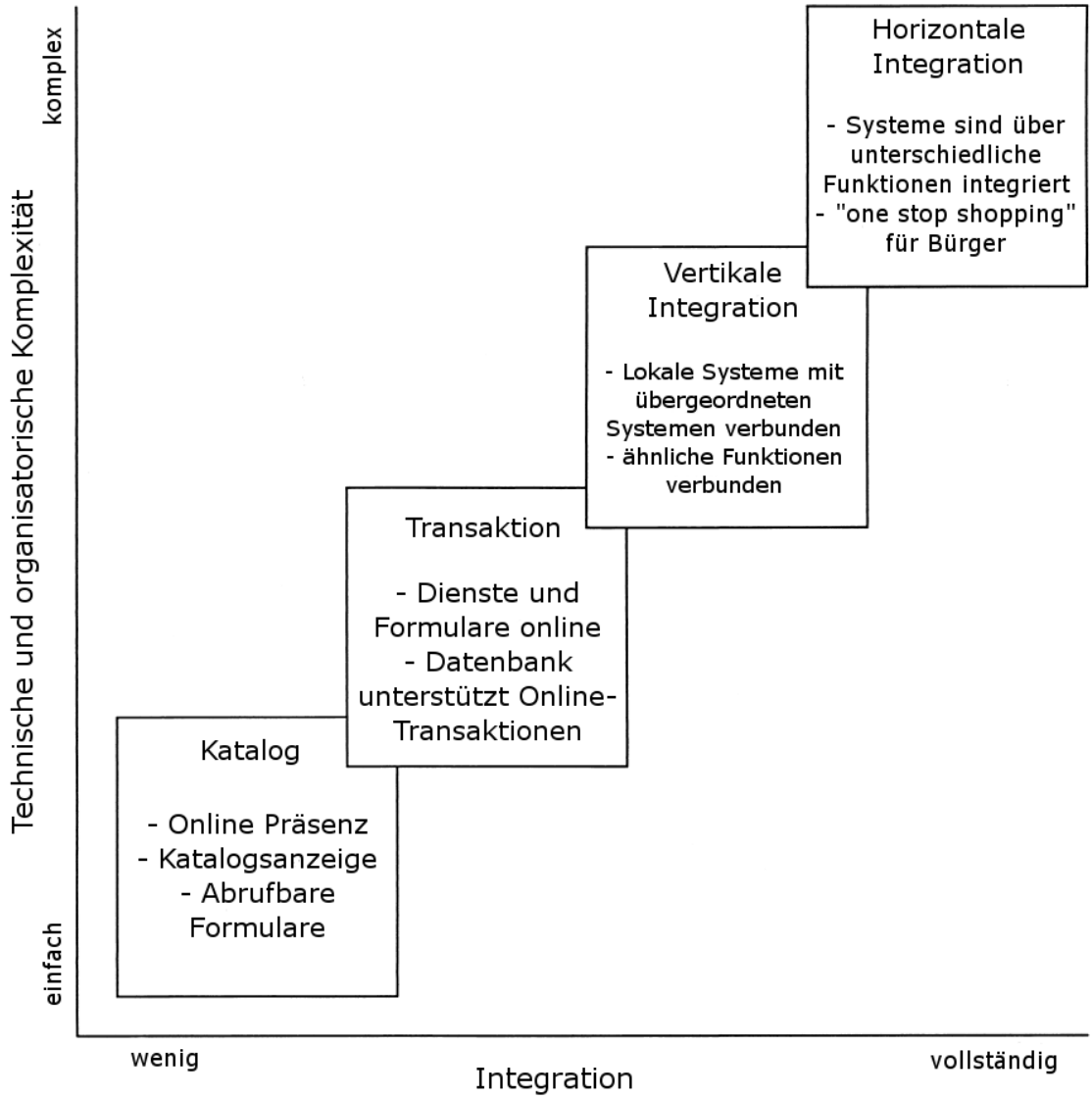

Abbildung 4 Entwicklung einer eGovernment-Architektur, übersetzt aus [Lay01]

In Abbildung 4 lässt sich erkennen, welche Evolutionsstufen eine eGovernment-Architektur im Zuge technischer Entwicklung entläuft. Das Ziel ist eine voll integrierte Systemlandschaft mit dem größtmöglichen Umfang an Dienstleistungen für den Bürger. Ohne eine ausreichende Verifizierung der Identität der Nutzer ist allerdings schon der zweite Schritt, die Einführung der Online-Transaktionen, nicht oder nur schwer möglich. Deutschland befindet sich in diesem gerade auf dem Schritt von der ersten auf die zweite Stufe. Erste Erfolge, wie die Möglichkeit die Steuererklärung online abzugeben, gibt es schon.

Abbildung 5 zeigt, dass Deutschland im Bereich eGovernment nur ein wenig über dem EU-Schnitt liegt was die Verfügbarkeit von Dienstleistungen angeht. Dabei sind es nicht nur kleine Länder, die ihre Verwaltung umfangreicher auf das Internetzeitalter umgestellt haben. Auch Länder vergleichbarer Größe wie Frankreich, Großbritannien oder Spanien bieten mehr Dienstleistungen online an.

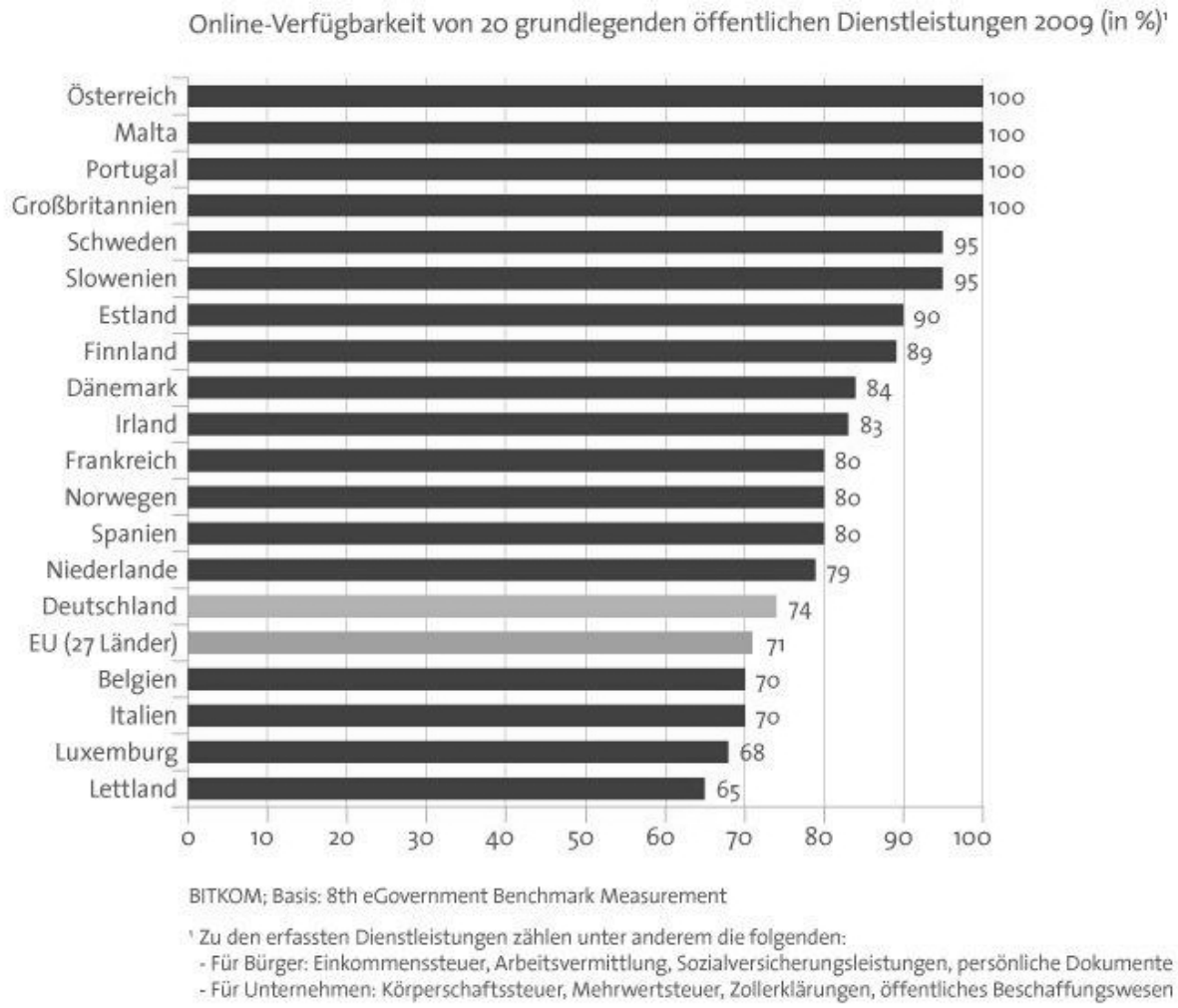

Abbildung 5 Verfügbarkeit von eGovernmentdiensten, Quelle: [BIT092]

Betrachtet man die Nutzung des eGovernment aufgeteilt nach Unternehmen und Privatpersonen, so ist dort ein großer Unterschied festzustellen. Unternehmen nutzen Dienstleistungen des eGovernment deutlich häufiger. EU-weit ist die Nutzung von eGovernment durch Unternehmen mehr als doppelt so stark wie durch Privatpersonen. Nur ein Drittel der Deutschen zwischen 16 und 74 nutzen zurzeit Angebote im eGovernment. Unter Nutzung versteht die zugrunde liegende Studie auch das Herunterladen von Formularen, sie fasst den Begriff der Nutzung also relativ weit.

Es ist unschwer zu Erkennen, dass es in diesem Bereich noch eine Menge Nutzungspotential gibt.

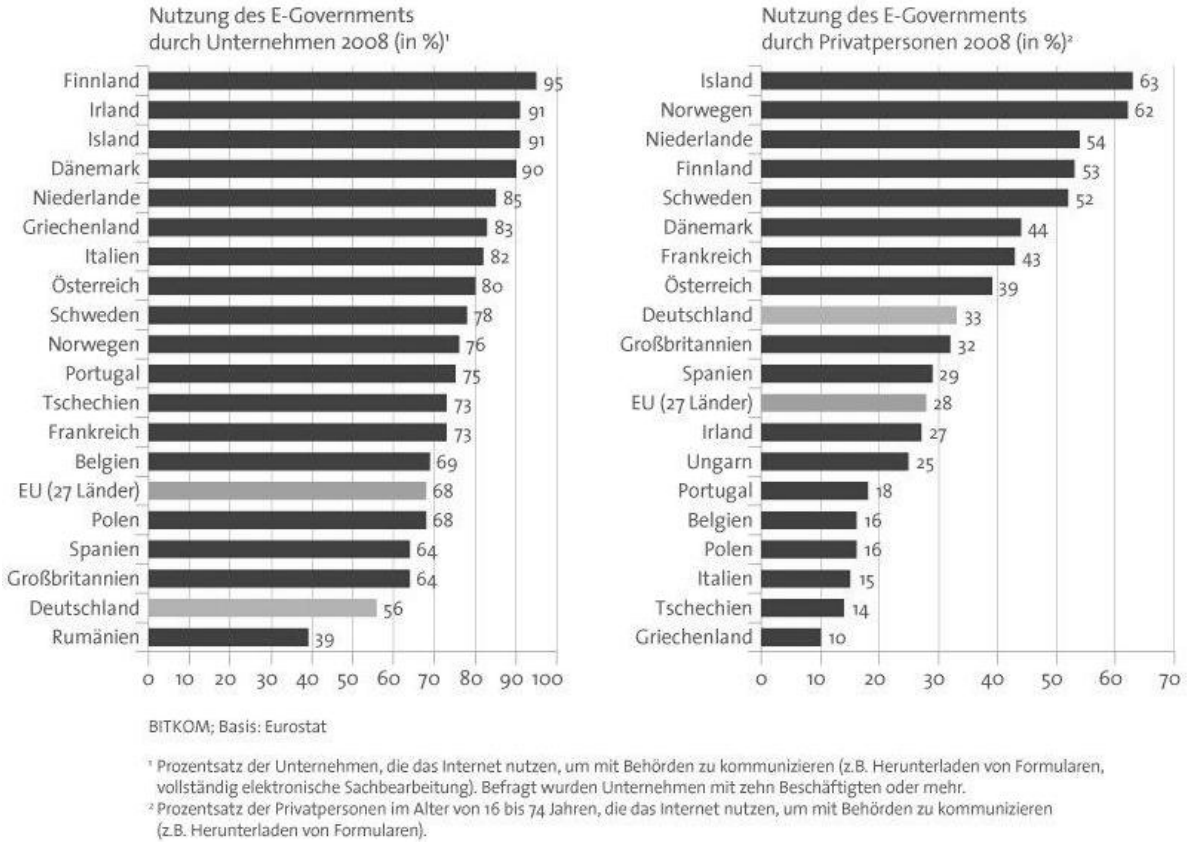

Abbildung 6 Nutzung des eGovernments in Europa, Quelle: [BIT091]

Der Anwendungsbereich eGovernment ist vor allem für die Betrachtung der Wirtschaftlichkeit des nPA aus Sicht des Verbrauchers interessant. Sind Kosteneinsparungen in diesem Bereich groß genug so kann schnell eine kritische Masse an Nutzern erschlossen werden. In seinem Umsetzungsplan gibt das BMI die möglichen Kosteneinsparungen bei Verwaltungsakten im Durchschnitt mit 15% an. Natürlich bleibt abzuwarten, wie viel von diesen 15% in reduzierten Gebühren beim Bürger ankommen, eine gewisse Kostensenkung für elektronisch durchgeführte Verwaltungsakte ist allerdings auch für den Bürger zu erwarten. Die aus den Netzeffekten[22] bekannte kritische Masse bezieht sich hier auf die Verbreitung der Kartenleser.

[22] Siehe Kapitel 3.6

4.3 Banken

4.3.1 Traditionelle Banken

Der dritte große Anwendungsbereich ist der Bankensektor. Lassen sich Bankgeschäfte in der Filiale noch problemlos mit bestehenden Methoden, also der Nutzung des klassischen Personalausweises und der händischen Unterschrift, abwickeln, so ist das Online-Banking ohne eine ausreichende Identifizierung der Kunden nicht möglich. Dabei wird Online-Banking von einem großen Teil der Bevölkerung bereits genutzt. An Abbildung 7 lässt sich aber auch erkennen, dass noch unausgeschöpfte Potentiale vorhanden sind. Die Nutzung von Online-Banking ist demnach beispielsweise in Finnland nahezu doppelt so hoch. Ohne näher auf die Gründe für diese Differenz einzugehen bleibt dennoch festzuhalten, dass die Nutzung in Deutschland ausbaufähig ist. Letztendlich ist sie auch im Sinne der Banken, da so Kosten reduziert werden können.

Für den Bankensektor ist neben der eID-Funktion auch die Signaturfunktion des nPA von großem Interesse, da für Bankgeschäfte die alleinige Authentifizierung der Kunden für die Geschäftsabwicklung nicht reicht. Solche Geschäfte müssen beweissicher durchgeführt werden. Das bedeutet, dass entweder ganz klassisch eine Unterschrift geleistet wird, die mit einer bestehenden Probe im Streitfall abgeglichen werden kann, oder dass auf das online gebräuchliche Verfahren von PIN und TAN zurückgegriffen wird. Mit der PIN authentisiert sich der Kunde bei der Bank und mit jeweils einer TAN wird eine Transaktion durchgeführt. Eine TAN kann dabei immer nur einmal verwendet werden. Die Sicherheit dieses Verfahrens beruht darauf, dass zur Durchführung etwas gewusst werden muss, nämlich die PIN, und dass etwas im Besitz sein muss, nämlich die TAN-Liste.

Daneben gibt es bereits heute das Homebanking Computer Interface (HBCI), mit dem einige Banken ihre Geschäfte online abwickeln. Bei diesem Verfahren wird auch auf Chipkarten zurückgegriffen, der PIN wird über einen Kartenleser eingegeben. Auch hier beruht die Sicherheit auf Wissen und Besitz, da ohne den Besitz der Bankkarte keine Abwicklung der Aufträge möglich ist.

Im Alltagsgeschäft könnte der nPA die Funktion der Bankkarten übernehmen. Er könnte einen Kunden identifizieren und die nötigen Signaturen leisten. Allerdings gibt es durch den nPA hier keinen Mehrwert. Im Gegenteil, er hat zwei Nachteile: Zum einen kann er Personen nur aufgrund ihrer nicht zwingend eindeutigen Personendaten identifizieren. Eine Bankkarte kann einfach die Kontonummer angeben und die Bank weiß zweifelsfrei, um welchen Kunden es sich handelt. Zum anderen sind die nötigen Signaturen beim nPA nicht kostenfrei.

Schritte	klassische Kontoeröffnung	Kontoeröffnung online
1. Schritt = Identitätsnachweis (eID-Funktion)		
Die Bank weist ihre Identität nach	Der Kunde betritt die Geschäftsräume einer Bank.	Bank legt Berechtigungszertifikat vor, das vom elektronischen Personalausweis überprüft wird.
Der Kunde weist seine Identität nach	Der vom Kunden vorgelegte Personalausweis wird vom Bankangestellten geprüft.	Der elektronische Personalausweis übersendet verschlüsselt ausgewählte eID-Daten.
2. Schritt = Unterschrift (QES-Funktion)		
Vertragsvorbereitung	Bankangestellte und Kunde handeln die Vertragsbedingungen aus und nehmen alle erforderlichen Daten in den Vertragstext auf.	Der Kunde wählt im geführten Dialog die gewünschten Vertragsinhalte, liest die AGB und ergänzt in den Browsermasken weitere erforderliche Sachdaten.
Abschluss eines Vertrages zur Kontoführung	Der Kunde und der Bankangestellte unterschreiben einen Kontoführungsvertrag.	Unter Verwendung der QES-Funktion des Personalausweises und der QES eines Angestellten der Bank wird ein Vertrag über die Kontoführung signiert.

Tabelle 2 Vergleich der Schritte bei der klassischen Kontoeröffnung und bei der Kontoeröffnung online, Quelle: [Mar10]

Vorteile bietet der nPA bei der Eröffnung von Konten. Tabelle 2 zeigt den Vorgang einer Kontoeröffnung und vergleich die notwendigen Schritte für eine Eröffnung in einer Filiale und eine Eröffnung online.

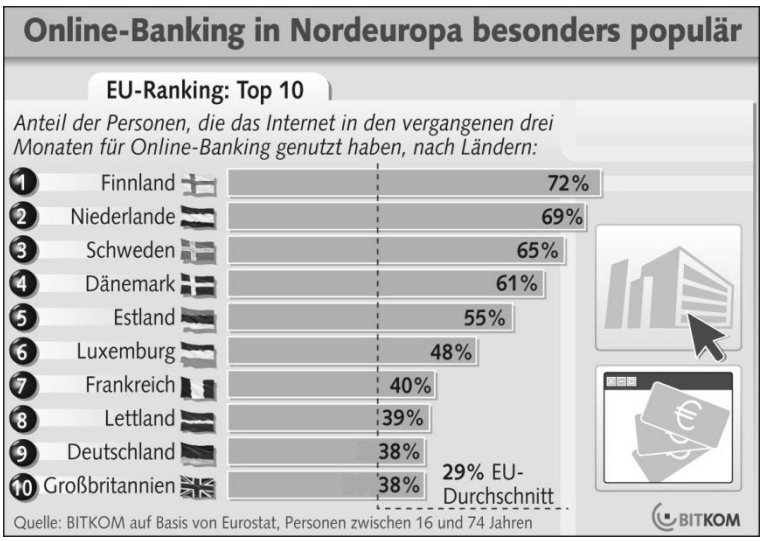

Abbildung 7 Popularität von Online-Banking im europäischen Vergleich, Quelle: [BIT09]

Anwendungsbereich für den nPA im Bankensektor ist also weniger die Abwicklung alltäglicher Geschäfte, dort scheinen die Speziallösungen besser geeignet. Vielmehr hilft der nPA zu einem Zeitpunkt, zu dem eine Speziallösung der jeweiligen Bank dem Kunden noch nicht zur Verfügung steht, insbesondere also bei der Kontoeröffnung. Dennoch könnte die Einführung des nPA für Banken noch einen anderen Nutzen haben: Es ist zu erwarten, dass mehr Kartenleser zur Verfügung stehen werden, was sich positiv auf die Nachfrage nach und die Nutzung von HBCI-Lösungen auswirken wird. HBCI hat zurzeit noch den Nachteil, dass sich Kunden einen Kartenleser anschaffen müssen und dass dies mit Kosten verbunden ist.

Abbildung 7 zeigt, dass Online-Banking noch nicht den Stellenwert hat, den es bereits in anderen europäischen Ländern genießt. Zwar bewegt sich die Nutzung über dem EU-Schnitt, allerdings nutzt beispielsweise in Finnland ein fast doppelt so großer Anteil der Bevölkerung die Online-Angebote der Banken.

4.3.2 P2P Banking

P2P Banking oder auch social lending bezeichnet die Kreditvergabe zwischen Verbrauchern ohne das Einschalten einer Bank als Mittler zwischen beiden Parteien[23]. Beim P2P Banking geht es zwar hauptsächlich um Kleinkredite, dennoch sehen die

[23] [Fre08]

Analysten von Gartner für 2013 einen Markt von 5 Mrd Dollar in den USA voraus[24]. Auch in Deutschland befinden sich heute schon einige Anbieter von Plattformen am Markt. Diese Plattformen führen die Kreditgeber und Kreditnehmer zusammen, unterscheiden sich von klassischen Banken allerdings darin, dass sie selbst die Kredite nicht vergeben. Das System ist vergleichbar dem von Internetauktionshäusern wie eBay, die Waren auch nicht selbst verkaufen sondern nur eine Plattform bieten um Angebot und Nachfrage zusammenzuführen. Die klassischen Funktionen der Banken wie Losgrößentransformation, Fristentransformation und Risikotransformation übernehmen diese Anbieter nicht.

Ein großes Problem dieser Anbieter ist die Verifizierung der Identität der Kunden. Da die Anbieter keine Filialen besitzen, trotzdem aber ähnlichen Regularien wie klassische Banken unterworfen sind, müssen sie über einen anderen Weg die Identität ihrer Kunden sicher verifizieren können. Es bleibt ihnen in der Regel nur das teure PostIdent-Verfahren. Dadurch sind die Anbieter auch gezwungen, eine Anmeldegebühr zu verlangen, was eine spontane Anmeldung, ein Ausprobieren des Dienstes, erschwert, wenn nicht sogar unmöglich macht. Anbieter von P2P-Banking-Plattformen könnten sehr vom Gebrauch des nPA profitieren, da sie so den Einstieg in ihr Angebot, billiger, wenn nicht sogar kostenfrei, gestalten können und so eine größere Zahl von Nutzern anlocken.

4.4 Versicherungen

Auch bei Versicherungen zeichnet sich ein Trend hin zur Vermittlung des Versicherungsvertrages über das Internet ab. Der Anteil der Kunden, die das Internet zumindest zum Teil bei der Suche nach einer Versicherung nutzen nimmt dabei immer weiter zu. So betrug dieser Anteil 2005 bereits rund 50%[25]. Gerade für weniger beratungsintensive Versicherungen wie beispielsweise Kfz-Versicherungen, ist das Internet als Vertriebskanal sehr gut geeignet.

Die Formerfordernisse eines Versicherungsabschluss über das Internet sind dabei nicht so streng, wie bei den vorher betrachteten Banken. Der Vertragsabschluss selbst

[24] Quelle: [Gar10]
[25] Quelle: [Kas09]

unterliegt dem Textformerfordernis nach §126b BGB. Dies bedeutet insbesondere, dass eine Unterschrift nicht nötig ist. Hier ergeben sich große Potentiale für den nPA, der den Abschluss für beide Seiten sicherer machen kann. Denn dass nur die Textform verlangt wird, bedeutet nicht, dass die Versicherer Interesse an mit falschen Daten abgeschlossen Verträgen haben, deren Abwicklung danach unnötig Geld kostet. Lediglich einzelne Bestandteile des Vertrags wie Datenschutzklauseln können dem Schriftformerfordernis nach §126 BGB unterliegen, das heißt sie benötigen eine Unterschrift der Vertragspartner. Diese Unterschrift kann durch eine QES geleistet werden, somit gibt es auch hier Potential beim Einsatz des nPA, so er von seinem Besitzer mit dieser Funktion ausgestattet wurde.

4.5 Weitere Branchen

Neben den drei genannten Bereichen, die vermutlich den Löwenanteil bei der Nutzung des nPA ausmachen werden, gibt es auch noch andere Branchen, die sich Funktionen des nPA zu Nutze machen können.

BITKOM zählt regulierte Dienstleister und die Logistik als solche Branchen auf. Unter den Begriff der regulierten Dienstleister fallen Firmen wie Lottogesellschaften und die Schufa. Für die Schufa wäre es interessant, Auskünfte aus ihrem Datenbestand online geben zu können. Da es sich um äußerst sensible Daten handelt, muss allerdings gewährleistet sein, dass der Zugriff sicher und befugt erfolgt. Diese wäre mit dem nPA machbar. Für die Schufa wäre es natürlich auch interessant aus Imagegründen, die persönlichen Auskünfte leichter erteilen zu können.

Regulierten Dienstleistern ist es gemein, und das sagt der Name ja schon, dass sie einem gewissen Maß an Regulierungen unterliegen. Daraus erfolgt zu jeder Zeit die Pflicht, die Geschäfte so abzuwickeln, dass diese Regeln eingehalten werden. Gerade wenn es um sensible Daten oder um Jugendschutz geht, so sind Dienstleistungen in diesem Bereich nur schwer online durchzuführen. Dass beispielsweise bis zum heutigen Tag keine staatliche Lottogesellschaft ihr Spiel auch online angeboten hat, ist sicher auch auf solche Schwierigkeiten zurückzuführen. In diesem konkreten Fall existiert sogar ein gesetzliches Verbot. Dieses resultiert aus einem Urteil des Bundesverfassungsgrichtes, welches bemängelte, dass die Spielsucht mit online

vertriebenen Lottoscheinen nicht eingegrenzt werden kann und somit das staatliche Monopol hinfällig sei. Mit dem nPA ließe sich diesem Einwand effektiv begegnen und somit mittelfristig Lotto auch wieder online anbieten[26].

Lotto sei hier nur ein Beispiel. Allgemein lässt sich sagen, dass der nPA bei regulierten Dienstleistern dort eingesetzt werden kann, wo er bisher nicht vorhandene Rechtssicherheit herstellt.

Im (recht grob definierten) Feld der Logistik lassen sich ebenfalls mehrere Anwendungsbereiche identifizieren. Denkt man an Logistik so fällt vielen wohl zunächst die Deutsche Post ein. Einige Dienstleistungen wie zum Beispiel Einschreiben erfordern dort eine Identifizierung des Abholers. Dazu wird die Ausweisnummer notiert. Problematisch dabei ist, dass dazu immer ein Mitarbeiter gebraucht wird, der dann die Nummer per Hand überträgt. Einschreiben lassen sich auch nicht in einer der Packstationen zur Abholung hinterlegen. Probleme durch den Medienbruch und die Möglichkeit der Ausweitung des Services auf automatisierte Systeme wie die Packstation legen nahe, dass der nPA auch hier einen möglichen Einsatzbereich hat.

Eine weitere Branche, die grob dem Bereich Logistik zugerechnet werden kann, ist der Luftverkehr. Die Entwicklung der letzten Jahre dort lässt ein Bestreben erkennen, möglichst viele Prozesse zu automatisieren. So wurde beispielsweise das Papierticket für Flüge weitestgehend abgeschafft und durch elektronische Tickets (eTix) ersetzt. Bisher wird das eTix meist an eine Kreditkarte gekoppelt und kann so abgerufen werden. Da diese Kreditkarte in diesem Fall als Identifikationsmittel dient, könnte sie auch durch den nPA ersetzt werden. Es wäre so auch sichergestellt, dass der Name des tatsächlich fliegenden Passagiers auch mit dem Namen des Ticketeigentümers überein stimmt. Dem in den letzten Jahren durch die weiter bestehende Terrorgefahr zunehmendem Sicherheitsdenken wäre mit der Nutzung des nPA an Stelle einer Kreditkarte sicher genüge getan. Eine Hürde bei der Verwendung im Luftverkehr ist aber die Frage der internationalen Interoperabilität. Ist der nPA eine rein deutsche Insellösung, so wären seine Vorteile im Luftverkehr sicher beschränkt. Ist eine Interoperabilität mit anderen EU-Staaten sowie idealerweise mit den Staaten der

26 Es sei angemerkt, dass es zwar Onlineangebote für Lotto gibt, diese aber nicht von deutschen Firmen angeboten werden.

großen Wirtschaftsräume in Nordamerika und Asien gewährleistet, so hat der nPA mehr Potential in dieser Branchen.

Für den Luftverkehr könnte neben der eID-Funktion auch eine Verbesserung der Effizienz der hoheitlichen Funktionen des nPA von Vorteil sein. Die Aus- oder Einreise liegt bei Flügen, die von außerhalb des Schengenraums kommen oder diesen verlassen, mitten im Abfertigungsprozess der Fluggesellschaft. Verbessert sich dieser Teil in Schnelligkeit und Zuverlässigkeit, so kann die Fluggesellschaft ein insgesamt besseres Produkt anbieten.

Das Testprojekt der Bundesregierung mit dem Verkehrsverbund Rhein-Ruhr zeigt, dass auch eine Nutzung des nPA im Nahverkehr als Ticket möglich ist. Bedenkt man, dass heutzutage sogar schon Mobiltelefone als Ticket verwendet werden können, so erscheint diese Einsatzmöglichkeit rein vom Innovationswillen der Beteiligten her gesehen durchaus realistisch. Die größte Hürde bei dieser Anwendung wäre die Möglichkeit der Kontrolle. Diese muss im Fahrzeug stattfinden können und darf nicht zu lange dauern. Dazu müsste der Kunde, ohne technische Erweiterungen des nPA, immer auch seine PIN eingeben. Für den Ablauf einer Fahrscheinkontrolle kann die Eingabe des PIN nur hinderlich sein. In Estland wird die dortige Version des elektronischen Personalausweises schon als Fahrausweis gebraucht, allerdings besteht dort die Problematik der PIN-Eingabe nicht. Eine Nutzung des nPA mittels eID-Funktion als Fahrschein erscheint nicht praktikabel.

5 Wirtschaftlicher Nutzen

In diesem Abschnitt soll analysiert werden, welchen konkreten Nutzen der nPA für die Verkäufer und Käufer auf dem Markt bietet. Dazu werden auch volkswirtschaftliche Effekte untersucht. Dabei kann sich der Nutzen sowohl für den Anbieter als auch für den Kunden entweder in der Vermeidung von Kosten oder Generierung eines zusätzlichen Produktnutzens zeigen. Auf diese Aspekte soll eingegangen und die Potentiale analysiert werden.

5.1 Betriebswirtschaftliche Effekte

5.1.1 Altersverifikation

Betrachtet man Anbieter im eCommerce-Bereich, so ist der Wirkungsbereich des nPA, die Schnittstelle zwischen Kunden und Anbieter auf den Bereich der Authentifizierung und der Bestell- und Zahlungsabwicklung beschränkt. Ein weiterer Kontakt, zum Beispiel persönlich, besteht in der Regel nicht.

Eine Altersverifikation ist dort nötig, wo angebotene Ware oder andere Inhalte einer Altersbeschränkung unterliegen. Beispiele für solche Angebote finden sich im Bereich Glückspiel. Eine Altersverifizierung wird dort auf verschiedene Art und Weise vorgenommen. Einzelne Anbieter verlangen Kopien des klassischen Personalausweises, die per Post oder Fax zugesandt werden. Andere beschränken sich auf eine Erklärung des Kunden, was offensichtlich keine besonders sichere Maßnahme ist. Gerade für Anbieter von Inhalten, deren Produkte einer Altersbeschränkung unterliegen, kann ein sicherer Weg der Altersverifikation der Kunden für die Aufrechterhaltung des Geschäftsmodells hilfreich sein. Aus der Tatsache, dass gewisse Güter einer Altersbeschränkung unterliegen, lässt sich schließen, dass das Vertreiben solcher Güter über das Internet aufgrund der bisher fehlenden Möglichkeit der Altersverifikation in der öffentlichen Meinung kritisch gesehen wird. Die gesellschaftliche Akzeptanz von derartigen Angeboten, hängt auch davon ab, wie einfach und effektiv der Jugendschutz dort umgesetzt werden kann. Die gesellschaftliche Akzeptanz ist deshalb von Bedeutung, da sie letztendlich auch Druck auf die Legislative ausübt. So sieht man

beispielsweise am Werbeverbot für Anbieter von Sportwetten, dass Gesellschaft und Politik durchaus bereit sind, in diesen Branchen regulativ in einem hohen Maße einzugreifen und die Handlungsfähigkeit der Unternehmen einzuschränken. Der Einsatz des nPA in diesem Umfeld könnte daher zu deutlichen Erleichterungen führen, da eine sichere und verlässliche Altersverifikation eingeführt werden kann. Zumindest jedoch werden die Anbieter den Vorgang der Altersverifikation automatisieren können. Der manuelle Abgleich von Ausweiskopien kann komplett entfallen, der administrative Aufwand sinkt. Es muss bei Kunden, die den nPA nutzen nur noch die Verifikation über den Ausweis erfolgen. Das ist sowohl für den Kunden relativ einfach, gerade für Erstkunden solcher Angebote. Aber auch für die Unternehmen ist es von Nutzen eine rechtssichere Altersverifikation nutzen zu können.

5.1.2 Gesetzliche Legitimationspflicht

Eine gesetzliche Legitimationspflicht besteht für Unternehmen, insbesondere Banken, die Konten oder andere Werte für ihre Kunden verwalten. Geregelt ist dies in der Abgabenordnung, einem Teil des Steuerrechts, und im Geldwäschegesetz. Die betroffenen Unternehmen müssen die Identität ihrer Kunden prüfen. Besteht persönlicher Kontakt, so reicht in der Regel die Vorlage eines Personalausweises aus. Eine Kostenersparnis durch die Nutzung des nPA bestünde nur darin, den Vorgang der manuellen Erfassung mittels einer elektronischen Übertragung abzukürzen. Allerdings sind Personalausweise auch schon heute maschinenlesbar, weshalb diese Ersparnis wohl nur theoretischer Natur ist. Gäbe es einen Vorteil bei maschineller Erfassung, so würde man ihn heute schon nutzen.

Besteht kein persönlicher Kontakt mit dem Kunden, etwa bei der Eröffnung eines Kontos bei einer Direktbank[27], so muss die Legitimation anders durchgeführt werden und dabei immer noch den gesetzlichen Vorschriften genügen. Ein gängiges Verfahren ist hierfür die Identitätsprüfung der Deutschen Post, das so genannte Postident. Hierbei stellt die Deutsche Post die Identitätsprüfung als Dienstleistung zur Verfügung. Den Vorschriften des Geldwäschegesetzes wird dabei folge geleistet. Die Kosten für

27 Eine Bank ohne Filialgeschäft.

dieses Verfahren liegen bei bis zu 7,16€ pro Vorgang[28]. Verfügt der Kunde über die nötige technische Infrastruktur, so lassen sich hier Kosten in größerem Umfang einsparen. Es sei auch erwähnt, dass die Deutsche Post die Fehlerquote des Verfahrens mit 1,1% angibt[29]. Erreicht man mit der eID-Funktion des nPA bessere Quoten, was durchaus zu erwarten ist, so ergäben sich dadurch weitere Ersparnisse.

5.1.3 Schutz von Nutzerkonten

eCommerce-Angebote führen in der Regel alle eine Form von Nutzerkonto für ihre Kunden, auf das dieser zugreifen kann. Diese bestehenden Login-Verfahren von eCommerce-Angeboten ließen sich auf eine Nutzung des nPA umstellen. Diese herkömmlichen Verfahren, in der Regel eine Kombination aus Nutzername und Passwort, haben den Nachteil, dass ihre Sicherheit darauf beruht, wie stark das Passwort des Nutzers und dessen Geheimhaltung sind. Angreifer bei solchen Verfahren brauchen nur die Kombination aus Nutzernamen und Passwort kennen, um im Namen des eigentlichen Kunden tätig zu werden. Da oft auch Kreditkartendaten hinterlegt werden, kann so erheblicher Schaden entstehen. Bei einer Authentifizierung der Nutzer mittels nPA ließe sich die Sicherheit signifikant erhöhen. Angriffe wären bei der unterstellten Sicherheit des nPA nur möglich, wenn der nPA auch physisch im Besitz der Angreifer wäre.

Es ist also zu prüfen, welche Form der Kostenersparnis sich bei der Verwendung solcher Konten in Verbindung mit dem nPA realisieren lassen. Zunächst muss dazu betrachtet werden, welche Kosten mit einem herkömmlichen System entstehen, um danach nach den Kostenanteilen zu suchen, die durch den nPA reduziert werden oder gar entfallen können.

Der erste Teil der Kosten entsteht aus der Installation und dem Betrieb der Software, die für die Verwaltung der Konten eingesetzt wird. Fixe Kosten fallen bei der Entwicklung des Systems an, laufende Kosten ergeben sich aus Wartung und

28 Postident Comfort. Siehe [Deu08]

29 1,1% erscheint dem Autor als relativ hoch, wird so jedoch vom TÜV angegeben. Es ist davon auszugehen, dass mit dem nPA verlässlichere Ergebnisse erzielt werden können. Der Faktor Mensch entfiele bei der Erfassung der Daten. Legt man die unterstellte Sicherheit des nPA zu Grunde, so blieben nur noch Missbrauch und Fehler bei der Bedienung als Fehlerquellen. Da diese jedoch auch beim Postident vorhanden sind, dürfte die Fehlerquote insgesamt kleiner ausfallen.

Betriebskosten wie Strom. Der zweite Teil der Gesamtkosten sind die Wagniskosten[30]. Für diese Betrachtung sind die Risiken von Belang, die sich über eine Versicherung abdecken lassen und solche, die im Rahmen der kalkulatorischen Wagnisse abgedeckt werden. Durch den Missbrauch der zur Verfügung gestellten Nutzerkonten entsteht jedem Anbieter im eCommerce-Bereich ein Ausfallrisiko. Dieses Risiko muss in die Kostenrechnung mit aufgenommen werden. Dies geht zum einen über den Abschluss von Versicherungen und der Kalkulation mit der der Prämie dieser Versicherung, zum anderen lässt sich dies aber auch die kalkulatorischen Wagnisse erfassen. Dabei wird ein erwarteter Ausfall angenommen und als Kostenpunkt in die Kalkulation mit aufgenommen. Über Vor- und Nachteile beider Verfahren lässt sich streiten, beiden ist jedoch gemein, dass die Kosten mit einem höheren Risiko für den Ausfall steigen. Entweder erhöht der Versicherer seine Prämie oder es entstehen real höhere Kosten als kalkuliert, was sich dann in der Folgeperiode auf die Kalkulation auswirken muss. Eine allgemeine Quantifizierung dieser Kosten ist kaum möglich. Sie hängt von den individuellen Gegebenheiten eines jeden Unternehmens ab. Einflussgrößen sind unter anderem die Sicherheitsarchitektur des jeweiligen Kundenportals und der Wert der angebotenen Güter. So ist beispielsweise die Komplexität eines Logins auf der Webseite einer Bank um einiges höher als der in einem relativ kleinen Webshop. Es ist anzunehmen, dass eine höhere Komplexität auch höhere Kosten in der Entwicklung und Wartung verursacht, als ein einfaches System. Gründe hierfür sind das benötigte Wissen für die Entwicklung und die Notwendigkeit, das System immer auf dem aktuellsten stand zu halten.

Es ist nun die Frage zu klären, inwieweit der nPA zur Reduktion dieser Kosten beitragen kann. Im Falle der kalkulatorischen Wagnisse erscheint die Antwort einfach. Aus der zu Grunde gelegten Unterstellung einer erhöhten Sicherheit folgt, dass die erwarteten Kosten durch Missbrauch geringer ausfallen. Daraus folgt, dass der zu kalkulierende Kostenanteil kleiner ausfällt. Ist diese Annahme der erhöhten Sicherheit richtig, so werden die Kosten in diesem Bereich sinken.

30 Quelle: [Sch03]

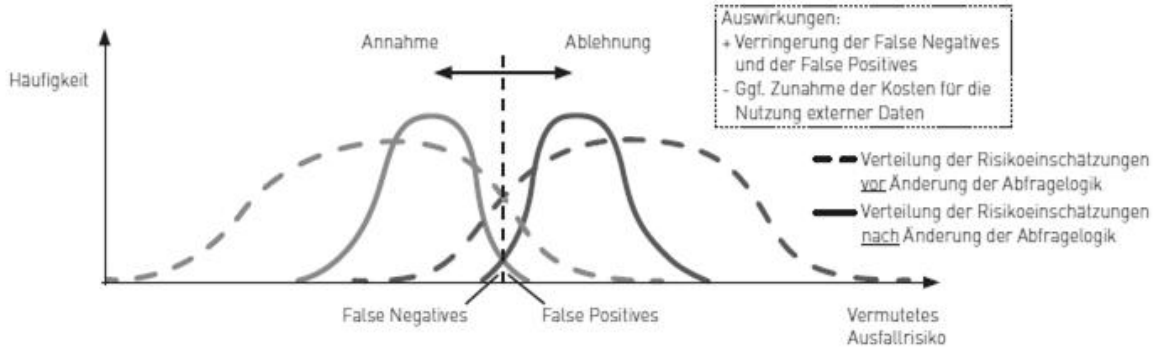

Abbildung 8 Änderung der Risikobetrachtung bei Verbesserung der zu Grunde liegenden Logik, Quelle: [ibi09]

Analog dazu lässt sich der kostensenkende Effekt auf Ausgaben für Versicherungen feststellen. Die Prämie einer Versicherung errechnet sich aus der erwarteten Schadenshöhe und der Wahrscheinlichkeit des Eintritts zuzüglich der Provision des Versicherers. Lässt sich also entweder an der Schadenshöhe oder der Wahrscheinlichkeit etwas verbessern, so sinken die Kosten. Die Schadenshöhe wird im Einzelfall nicht unterschiedlich sein, dafür ist der nPA das falsche Instrument[31]. Aber die Wahrscheinlichkeit des Eintritts lässt sich reduzieren. So sinken auch hier die Kosten, da der Versicherer die Prämien senken kann und zu erwarten ist, dass er dies im Zuge des Wettbewerbs mit anderen Versicherern auch machen wird. Hinzu kommt, dass mit der Einführung einer Sicherheitsarchitektur, die den nPA beinhaltet, Standards definiert werden können und diese eine Beurteilung der Sicherheit einfacher machen.

In Abbildung 8 ist abgebildet, wie sich die Risikobetrachtung einer Transaktion ändern kann, wenn die dahinterstehende Logik verbessert wird. Eine Verbesserung des Verfahrens unter anderem dann festzustellen, wenn die Datenbasis verbessert wird. Der nPA kann für eine solche Verbesserung sorgen. Es kann also sicherer gesagt werden, ob es sich um einen Betrugsversuch handelt und entsprechend kann die Transaktion dann abgebrochen werden. Zusätzlich kann auch die fälschliche Ablehnung („false negatives“) von Transaktionen reduziert werden, was zu einem höheren Umsatz führt.

31 Ein geeignetes Mittel wäre beispielsweise ein strengeres Sicherheitskonzept ab einem bestimmten Bestellwert.

5.1.4 Verbesserung des Angebots und die Einführung von Zahlungsverfahren

Dieser Abschnitt soll untersuchen, inwieweit der nPA neben einer möglichen Kostenreduktion auch zu einer Verbesserung des Produktangebots eines Unternehmens beitragen kann. Dass es diese Möglichkeit überhaupt gibt, mag auf den ersten Blick nicht sofort sichtbar zu sein. Die wenigsten Unternehmen werden den nPA selbst als Produktkern haben. Der Produktkern ist jedoch nicht alles, was ein Produkt ausmacht[32]. Neben ihm gibt es noch die Zusatzeigenschaften eines Produkts, die Verpackung, verknüpfte Basis- und Zusatzdienstleistungen sowie die Marke. Abbildung 9 verdeutlicht dies noch einmal bildlich. Während der nPA für die Marke und die Verpackung keine Rolle spielt, so kann er doch bei den verschiedenen Dienstleistungen und den Zusatzeigenschaften zum Tragen kommen.

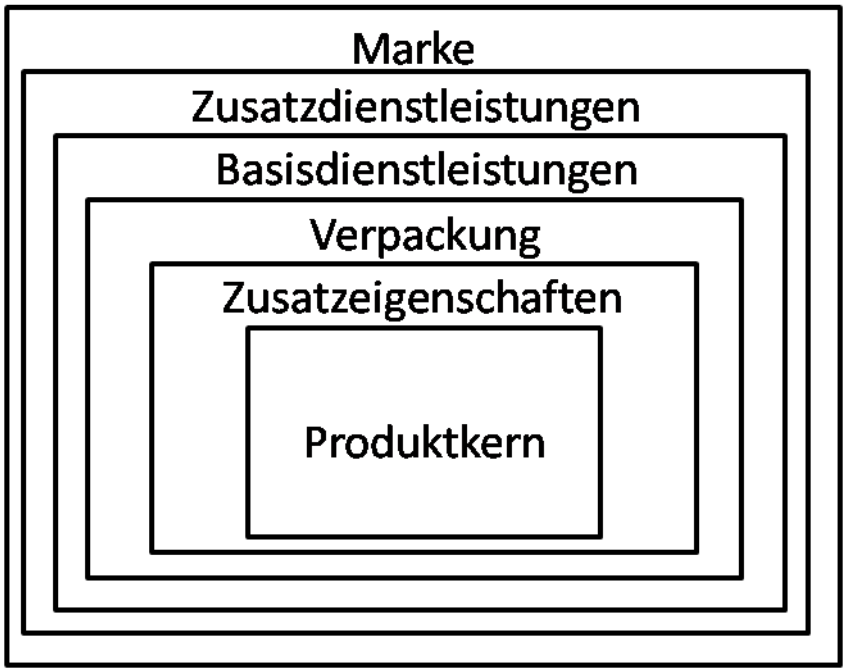

Abbildung 9 Komponenten eines Produkts, Quelle: [Hom06]

Am Beispiel eCommerce lässt sich dies gut darstellen. Betrachtet man das Angebot und den Verkauf bestimmter Waren als eine Dienstleistung, so ist die Auswahl an Zahlungsmethoden ein Teil dieser Dienstleistung. Werden beispielsweise nur Vorkasse oder Nachnahme als Zahlungsmethoden angeboten, so ist das Angebot weniger

32 Quelle: [Hom06]

attraktiv, als wenn auch eine Zahlung auf Rechnung oder per Kreditkarte angeboten wird. Das Anbieten dieser Zahlungsarten hängt, wie zuvor beschrieben, auch von dem damit verbundenem Risiko ab. Da dieses mit Hilfe des nPA gesenkt werden kann, können Unternehmen so im Einzelfall den Schritt hin zur Einführung einer oder mehrerer zusätzlicher Zahlungsmöglichkeiten gehen. Dem Kunden mehr Auswahl zu bieten, erhöht die Attraktivität des eigenen Angebots. Durch den nPA kann Kunden einfacher eine weitere Möglichkeit der Bezahlung zur Verfügung gestellt werden. Es wäre denkbar, ec-Karten in Kombination mit dem nPA zu nutzen oder einfache Lastschriftverfahren unter Zuhilfenahme des nPA zu ermöglichen.

Die Auswahl an angebotenen Zahlungsverfahren hängt direkt mit dem wirtschaftlichen Erfolg eines Webshops zusammen. So führt die Einführung neuer Zahlungsverfahren zum Rückgang der Kaufabbruchsquote, also dem Anteil der potentiellen Kunden, die zwar die Seite mit Kaufinteresse besuchen, allerdings keine Bestellung durchführen. Abbildung 10 zeigt den Rückgang dieser Quote für ausgewählte Zahlungsverfahren. Bietet ein Konkurrent die gewünschte Zahlungsmethoden an, so ist die Gefahr gegeben, dass eine Kunde dann zu diesem Anbieter wechselt und für längere Zeit als

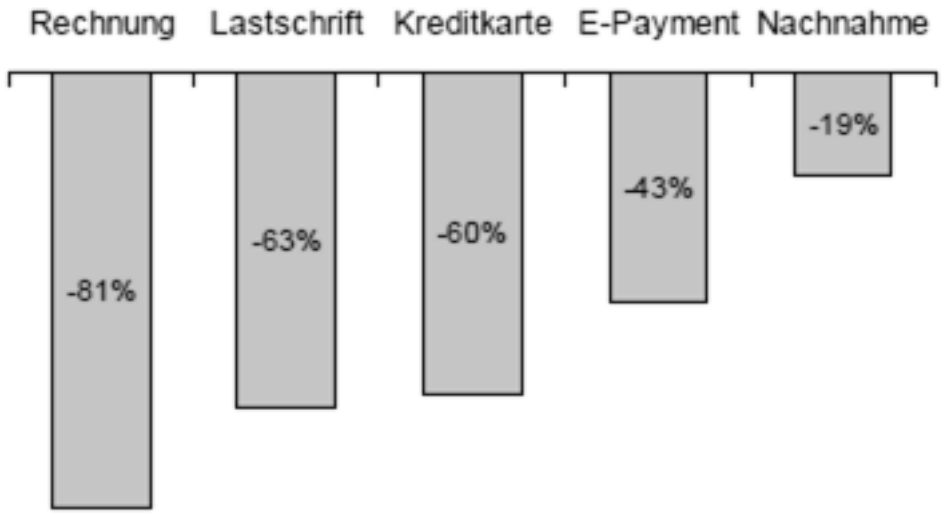

Abbildung 10 Durchschnittlicher Rückgang der Kaufabbruchsquote bei Einführung verschiedener Zahlungsmethoden, Quelle: [ibi091]

potentieller Kunde verloren ist. Am größten sind die Chancen, einen Kunden aufgrund der Zahlungsmethoden zu halten bei Zahlungen per Rechnung, per Lastschrift und per Kreditkarte. Dies sind Zahlungsmethoden, bei denen der Anbieter einem großem Betrugsrisiko ausgesetzt ist. Bei Rechnungen besteht die Gefahr, dass Sendungen abgefangen werden. Bei Lastschriften können Kosten durch nicht gedeckte, zurückgebuchte Lastschriften oder der missbräuchlichen Nutzung von gefälschten Kontodaten entstehen. Dasselbe gilt für Kreditkarten.

Anbieter haben verschiedene Möglichkeiten, sich vor dem Betrug bei diesen Zahlungsarten zu schützen. Den drei genannten Zahlungsmethoden ist gemein, dass die Adressverifizierung ein geeignetes Mittel der Betrugsprävention ist. Durch die Daten auf dem nPA lässt sich eine solche Verifizierung vornehmen, wenn das Berechtigungszertifikat des Anbieters eine Abfrage der Adresse zulässt. Es bliebe im

Bereich der Adresse des Kunden nur noch das Problem eines nicht gemeldeten Umzugs, dass auch der nPA nicht lösen kann. Andere Präventionsmaßnahmen wie eine Bonitätsprüfung oder im Fall der Kreditkarte eine Autorisierung kann der nPA jedoch nicht bieten. Er ist somit nur ein Teil der Sicherheitsarchitektur.

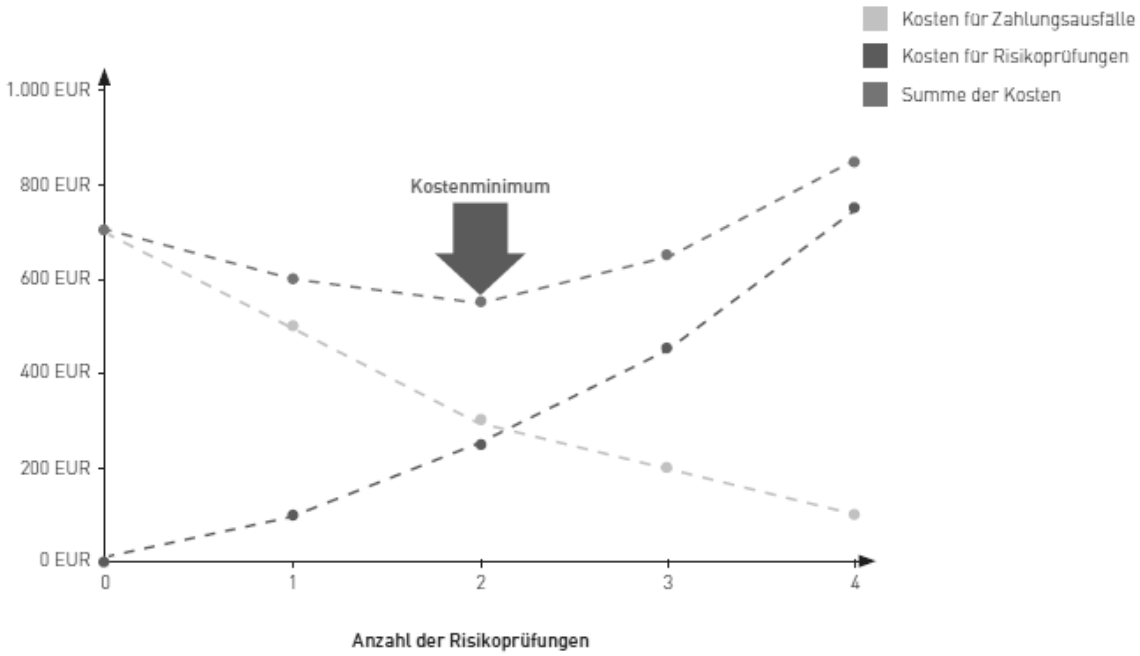

Abbildung 11 Kostenverlauf von Risikoprüfung und Zahlungsausfällen, Quelle: [ibi09]

Abbildung 11 zeigt beispielhaft den Verlauf der Kosten für Betrugsprävention und Zahlungsausfälle. Der Anbieter wird sich mittelfristig für eine kostenminimale Strategie entscheiden. Der Einsatz des nPA kann die Kurve, die den Verlauf der Kosten für Risikoprüfungen anzeigt nach rechts unten verschieben. Der kostenminimale Punkt verschiebt sich dadurch auch in diese Richtung. Dies bedeutet weniger Gesamtkosten und setzt sich aus zwei Effekten zusammen: Zum einen werden die Kosten für Zahlungsausfälle durch das höhere Sicherheitsniveau gemindert und zum anderen sinken die Kosten für die Risikoprüfungen, da beispielsweise keine Adressauskunfteien mehr in Anspruch genommen werden müssen.

Mit Hilfe des nPA kann es also möglich sein, dass die Entscheidung gegen eine Zahlungsmethode revidiert wird, weil der nPA das Risiko und die Kosten in einem Maße senkt, die eine Entscheidung für eine Zahlungsmethode wirtschaftlich macht. Kann die Entscheidung für eine weitere Zahlungsmethode getroffen werden, so hat dies einen positiven Effekt auf den Erfolg des Unternehmens.

5.1.5 Prozessinnovation

Auch ist es möglich, den ganzen Verkaufsprozess zu einfachen und damit die Dienstleistung für den Kunden attraktiver zu machen. Das bekannteste Beispiel für Prozessinnovation ist die Firma Dell[33]. Dell hat seine heutige Stellung im Markt nicht durch die Erfindung des Computers erreicht. Auch sind die Computer, die Dell verkauft nicht außerordentlich hochwertig oder preiswert im Vergleich zu Konkurrenten. Dell hat es aber geschafft, durch Innovation im Herstellungs- und Verkaufsprozess Marktanteile zu gewinnen. Dell eliminierte Zwischenhändler in ihre Wertschöpfungskette und bot Kunden an, den Computer individuell zu konfigurieren. Zwar stand man weiter mit dem „klassischen" Händler in Konkurrenz, konnte sich mit dieser Änderung des Prozesses aber am Markt differenzieren. Ähnliches lässt sich für Amazon sagen. Amazon ist in einen Markt eingetreten, auf dem schon einige Anbieter vertreten waren. Trotzdem haben sie es geschafft durch einfache Prozesse und den damit verbundenen Vorteil für die Kunden ihre Stellung im Markt immer weiter auszubauen.

Möglich ist Prozessinnovation dort, wo relativ komplizierte und kostentreibende Prozesse die Regel sind. Das kann beispielsweise für die Bezahlung im Online-Handel gesagt werden. Vergleicht man beispielsweise den Prozess, der bei der Bezahlung per Nachnahme durchlaufen werden muss mit einem unter Hilfe des nPA durchgeführten Lastschriftverfahren. Der Kunde bestellt eine Ware, die der Versender dann mitsamt Zahlschein der Post übergibt. Die muss an der Haustür den Betrag einziehen oder der Kunde muss zu ungünstigen Geschäftszeiten in eine der immer weniger werdenden Filialen gehen und dort seine Sendung gegen Zahlung abholen. Die Post muss dieses Geld dann an den Versender schicken. Zu guter letzt kostet dieses Verfahren im Vergleich mit anderen Zahlungsmethoden wohl am meisten. Kann ein Unternehmen dank der Nutzung des nPA die Zahlungsmethode Nachnahme durch eine gleichwertige aber günstigere Zahlungsmethode, beispielsweise ein Lastschriftverfahren, ersetzen,

33 Quelle: [Kir08]

so bietet es seinen Kunden einen Mehrwert allein durch die Innovation im Prozess. An der Ware selbst oder dem Preis wird dabei nichts geändert.

Für den Online-Handel mag diese Möglichkeit kritisch gesehen werden, da auch heute schon andere, relativ sichere und einfache Zahlungsmethoden existieren. Denkt man beim Thema Prozessinnovation aber an das Online-Banking, so wird schnell ersichtlich, dass auch hier erhebliche Potentiale existieren, Prozesse zu vereinfachen. Allein die Nutzung von Transaktionsnummern, eine gängige Praxis im Online-Banking, könnte reduziert werden, würde jede Transaktion mit Hilfe des nPA signiert werden.

5.1.6 Verbesserung der Kundenbeziehungen

Die (möglichst positive) Beziehung zum Kunden ist für jedes Unternehmen von höchster Bedeutung. Für Unternehmen im eCommerce ist die Kundenbeziehung vor allem durch Vertrauen in das Unternehmen und die Sicherheit des Onlineangebots, durch Benutzbarkeit des Onlineangebots und durch die Zuverlässigkeit des Service geprägt. Fühlt sich ein potentieller Kunde auf der Seite nicht wohl, so wird sich die Wahrscheinlichkeit eines Einkaufs wohl nicht erhöhen. Ging bei einer Bestellung etwas schief, so schmälert das die Chancen eines weiteren Einkaufs. Als Betreiber hat man auch nicht die Chance, das Verhältnis zum Kunden durch ein sympathisches Auftreten zu verbessern. Es bleibt in der Regel nur der unpersönliche Kontakt. Mit dem nPA bietet sich ein Instrument, das helfen kann die Beziehung zum Kunde zu verbessern. Allein durch die Tatsache, dass ein Medienbruch vermieden wird, nämlich bei der Eingabe der Kundendaten durch den Kunden selbst, können Fehler bei der Abwicklung des Bestellvorgangs vermieden werden. Ist die Abfrage der Daten aus dem nPA dazu noch geschickt in das Onlineangebot eingebaut, kann die Nutzbarkeit der ganzen Seite erhöht werden.

5.1.7 Möglichkeiten für die Unternehmenskommunikation

Die Funktionen des nPA lassen sich auch in der Unternehmenskommunikation einsetzen. Insbesondere in der Kommunikation mit dem Kunden, der das Onlineangebot besucht, lässt sich gut auf die Möglichkeit der Verwendung des nPA

hinweisen. Solange die Nutzung des nPA noch kein De-facto-Standard ist, kann das Unternehmen so seine Innovationsfähigkeit nach außen kommunizieren.

Es ist zu bezweifeln, dass die Einsatzmöglichkeit des nPA im eigenen Angebot signifikanten Niederschlag in der geschalteten Werbung eines Unternehmens findet. Wäre die Bestellabwicklung wichtig für die eigene Werbung, so würde sich auch heute schon etwas zu dieser Thematik in der Werbung finden. Dies kann aber nicht festgestellt werden. Zwar zielt beispielsweise der Slogan von ebay („3, 2, 1, meins…“) auf die einfach gehaltene Oberfläche beim Ersteigern von Artikeln ab, die eigentliche Abwicklung des Geschäfts nach der Auktion ist aber nicht das Thema dieser Kampagne.

5.2 Kosten des nPA für Anbieter

Um die Möglichkeiten des nPA zu nutzen, muss ein Unternehmen einige Investitionen tätigen. Zunächst muss nach der Entscheidung, nPA-bezogene Funktionen in das Angebot aufzunehmen, die nötige Berechtigung bei der Vergabestelle für Berechtigungszertifikate beantragt werden. Dazu muss dargelegt werden, welche Daten zu welchem Zweck gebraucht werden. Diese Berechtigungen werden für drei Jahre ausgesprochen[34]. Es ist jedoch davon auszugehen, dass der anfängliche Aufwand für das Erlangen einer Berechtigung größer ist, als der Aufwand bei der Erneuerung der Berechtigung nach Ablauf der drei Jahre. Der nötige Aufwand ist schwer zu schätzen und hängt sowohl vom beantragenden Unternehmen als auch von den Abläufen innerhalb der Vergabestelle ab. Es ist in der ersten Zeit nach der Einführung des nPA mit weniger effizienten Abläufen auf beiden Seiten zu rechnen. Die genauen Kosten lassen sich daher zu diesem Zeitpunkt noch nicht bestimmen. Es ist jedoch davon auszugehen, dass es sich um einmalige Kosten handelt. Daher ist die genaue Höhe zwar wichtig, wenn ein Zeitpunkt der Amortisation dieser Investition berechnet werden soll, für die generelle Beurteilung der Wirtschaftlichkeit sind diese Kosten allerdings zweitrangig.

Ein weiterer Kostenblock ist bei der Weiterentwicklung des Onlineangebots zu erwarten. Die bestehenden Funktionalitäten müssen um die Funktionen des nPA

34 Quelle: [Mar10]

erweitert werden. In der Regel bedeutet dies also, dass eine Schnittstelle zu der eID-Funktion hergestellt werden muss. Im Laufe der Zeit ist damit zu rechnen, dass es für diese Schnittstelle standardisierte Lösungen gibt, die von den Herstellern dieser Webshops angeboten werden. Größere Unternehmen werden ihre individuellen Lösungen anpassen müssen. Auch hier hängt der Aufwand unmittelbar von der bestehenden Lösung ab. Das BMI spricht in seinen Veröffentlichungen von einer leicht zu integrierenden eCard-API. Über diese API sollen die möglichen Funktionen leicht auch in bestehende Systeme integrierbar sein. Es bleibt abzuwarten, inwieweit sich diese Ankündigung bestätigt. Erste Erfahrungen werden zurzeit innerhalb des Pilotprojektes des BMI gesammelt. Die Erfahrungen daraus, sowie die Erfahrungen in der ersten Zeit nach der Einführung werden dazu führen, dass die Kosten für die Erstellung einer Schnittstelle höchstwahrscheinlich im Laufe der Zeit sinken werden. Dies lässt sich ganz einfach mit Lerneffekten begründen, wie sie überall zu finden sind, wo neue Technologie eingeführt wird.

Indirekte Kosten können der Verlust von Kunden sein, die dem nPA generell kritisch gegenüber stehen. Dies ist insbesondere zu befürchten, sollte die Nutzung des nPA für eine Bestellung obligatorisch sein. Zu erwarten ist eine solch restriktive Politik jedoch nicht, bevor genug neue Personalausweise im Umlauf sind, da sich ein Unternehmen sonst unnötigerweise eines Teils seiner Kundenbasis beraubt. Ist der Umtausch der Ausweise jedoch weitgehend abgeschlossen, kann es passieren, dass Anbieter Kunden ohne nPA ausschließen oder über preisliche Maßnahmen schlechter stellen, wenn die real wahrgenommenen Vorteile der nPA-Funktionen eine solche Vorgehensweise zulassen. Ein ähnliches Verhalten lässt sich bereits heute beim Anbieten bestimmter Zahlungsmethoden beobachten. Unternehmen entscheiden sich für oder gegen die Aufnahme einer Zahlungsmethode aufgrund einer Kosten-Nutzen-Abwägung. Sind genug neue Ausweise im Umlauf wird zusätzlich abgewogenen werden, ob weiterhin die klassische Eingabe der Personendaten per Hand akzeptiert wird. Werden die bereits beschriebenen Nachteile dabei als zu groß bewertet, so ist es durchaus möglich, dass Unternehmen auf die klassische Methode verzichten und dadurch einige Kunden verlieren. Das ist als möglicher Kostenpunkt zu berücksichtigen.

5.3 Nutzen für Verbraucher

Neben den Nutzen für privatwirtschaftliche Organisationen muss auch untersucht werden, welchen Nutzen der Verbraucher vom neuen Personalausweis hat. Diese Notwendigkeit begründet sich darin, dass es Folgen für das Verhalten beider Seiten hat, welchen Nutzen der Verbraucher in den Funktionen des nPA sieht. Ist der Nutzen gering, so müssen von politischer oder privatwirtschaftlicher Seite Anreize geschaffen werden, den nPA zu nutzen. Ist der Nutzen für den Verbraucher hoch, so ist davon auszugehen, dass die Nutzung der Funktionen verstärkt nachgefragt wird. Anreize, wie beispielsweise Subventionen für Kartenleser, werden dann nicht oder in einem verringertem Maße benötigt.

5.3.1 Geschäftsabwicklung

Für den Verbraucher sind die Vorteile in der Geschäftsabwicklung ähnlich wie für die Anbieter. Auch er profitiert von automatisch ausgefüllten Formularen für Personaldaten. Kann eine Bestellung nicht oder nur verspätet geliefert werden, weil sich der Kunde beim Eingeben der Daten vertippt hat, so ist das nicht nur ein Schaden auf der Seite des Anbieters, auch der Kunde selbst hat einen Nachteil. Dieser Nachteil kann sich allein auf die Verspätung beschränken, es kann aber auch zu monetären Kosten kommen, wie zum Beispiel bei einer nicht erfolgreichen Lastschrift, deren Kosten der Anbieter dann weiterreicht.

Der Nutzen und damit der Erfolg der eID-Funktion hängen direkt mit der Benutzbarkeit der Schnittstelle zusammen. In einem Beispiel des Instituts für Internet-Sicherheit der FH Gelsenkirchen[35] lässt sich erkennen, dass der Vorgang der Eingabe der Daten womöglich sogar länger dauert, als das Eingeben per Hand gedauert hätte. Bedenkt man, dass die Eingabe über den nPA in der Frage der Benutzbarkeit auch mit der Auto-Vervollständigen-Funktion in modernen Browsern konkurriert, so ist ein Mehrwert an Nutzen für den Verbraucher nicht zwingend zu erkennen. Im Unterschied zu anderen eID-Modellen, wie beispielsweise dem belgischen, ist es bei der deutschen Version immer notwendig, die PIN einzugeben. Dadurch verlängert sich die Eingabeprozedur

35 Quelle: [Ins10]

für den Benutzer um einen weiteren Schritt. Tabelle 3 gibt einen Überblick über die Möglichkeiten für den Verbraucher, seine Daten einzugeben.

	Manuelle Eingabe	Auto-Vervollständigen	eID-Funktion
Vorgang	– Eintippen der Informationen per Hand – Springen durch die Eingabefelder per Mausklick oder Tab-Taste	– Lesen der im Browser hinterlegten Informationen – Eingabe durch Auswahl der hinterlegten Informationen – Springen durch die Felder per Mausklick oder Tab-Taste	– Eingabe durch Aufruf des eID-Applets – Zusätzlicher Schritt durch PIN-Eingabe
Vorteile	– Schnelle Eingabe	– Schnelle Eingabe	– Garantiert richtige Personendaten – Sichere Kommunikation – Keine Möglichkeit, falsche Daten einzugeben
Risiken	– Falsche Eingaben durch einfaches Vertippen möglich	– Mehrere Nutzer an einem Computer können zu Problemen führen – Felder des Eingabeformulars sind nicht standardisiert und machen manuelle Eingabe notwendig	– Personendaten, für deren Zugriff keine Berechtigung besteht, müssen unter Umständen zusätzlich per Hand eingegeben werden

Tabelle 3 Vorteile und Risiken verschiedener Eingabearten von Personendaten in Formulare

Es lässt sich erkennen, dass der Vorteil des nPA hauptsächlich in der Datensicherheit liegt. Ein schnellerer Ablauf einer Bestellabwicklung ist zunächst nicht zu erwarten. Welchen Nutzen, Schnelligkeit oder Sicherheit, der Verbraucher höher bewertet,

unterliegt wohl einer subjektiven Bewertung und müsste empirisch untersucht werden.

5.3.2 Netzeffekte

Die schon zuvor beschriebenen Netzeffekte haben auch für den Verbraucher Einfluss auf seine Wahrnehmung des Nutzens des nPA. Am Anfang der Umstellungsphase wird es wohl nur wenige Unternehmen geben, die nPA-Schnittstellen anbieten. Der größte Mehrwert wird sich bei eGovernment-Anwendungen feststellen lassen, da davon auszugehen ist, dass der Staat als Triebfeder des Projektes auch entsprechende Anwendungen zur Verfügung stellen wird. Mit größerer Nutzerbasis wird es dann auch immer interessanter für privatwirtschaftliche Anbieter, Schnittstellen anzubieten. Der genaue Zeitpunkt lässt sich nur schwer vorhersagen. Es ist nicht davon auszugehen, dass bereits im ersten Jahr größere Anstrengungen unternommen werden und damit dann nur etwas mehr als 10% der potentiellen Kunden erreicht werden können. Allerdings ist auch zu erwarten, dass keine 100% Verbreitung des Ausweises erforderlich sein wird, um die Entwicklung von Anwendungen auszulösen.

Die Existenz von Netzeffekten ist sicherlich unbestritten, wann genau sie in diesem Kontext zum Tragen kommen, ist allerdings ungewiss. Es kann allerdings zu einem so genannten Pinguin-Effekt kommen, bei dem eine im Grunde sinnvolle Innovation keinen Erfolg hat, da die kritische Nutzerbasis nie erreicht wurde. Zwar wird sich, da der nPA per Gesetz eingeführt wird, niemand, der unter die Ausweichpflicht fällt, dem neuen Ausweis verweigern können. Dennoch besteht die Gefahr eines Pinguin-Effekts, wenn nicht genug Kartenleser in Umlauf gebracht werden können.

Fraglich bleibt, was die Netzeffekte für einen Einfluss auf Personen haben werden, die keinen Anspruch auf einen deutschen Personalausweis haben. Sie könnten dazu führen, dass ein relativ großer Bedarf an Karten mit einer eID-Funktion nach Vorbild des nPA entsteht, die aber keine Personalausweise sind. In Estland wurde für diesen Personenkreis eine eigene Version des Personalausweises eingeführt. Dies könnte bei Erfolg des nPA in Deutschland auch erforderlich werden, um dem betroffenen Personenkreis Zugang zur Technologie und dem verbundenen Nutzen zu geben.

Für die qualifizierte elektronische Signatur werden diese Angaben vermutlich nicht gelten, da sie optional sein wird und mit zusätzlichen Kosten verbunden ist. Wie schon vorher angesprochen, ist der Signaturmarkt sehr abhängig von den Netzeffekten. Zwar hat auch eine einzelne Signatur ihren Wert, ohne dass andere selbst Signaturen ausstellen, aber für einen möglichst großen Nutzen wird eine breite, auf Signaturen ausgelegte Infrastruktur gebraucht. Diese wird nicht entstehen, wenn nur wenige Ausweisinhaber auch die Signatur nutzen. Beispielsweise ist bei ausreichender Verbreitung und Nachfrage der Signatur zu erwarten, dass Anbieter von freien Emaildiensten in ihren Oberflächen auch Funktionen einbauen, die eine Signatur der Emails ermöglicht. Entschiede sich die Mehrheit der Ausweisinhaber nur für den einfachen nPA ohne die für die Signierung nötigen Zertifikate, dann ist es zu bezweifeln, dass sich an der aktuellen Situation des Signaturmarktes etwas ändert[36]. Es ist zu befürchten, dass der Teufelskreis aus mangelnder Infrastruktur aufgrund zu wenig Nachfrage nach Signaturen, die wiederum aus der mangelnden Infrastruktur resultiert, ohne weitere Anreize für die Nutzer nicht durchbrochen werden kann. Ein möglicher Anreiz wäre eine kostenlose Nutzung in den ersten Jahren oder eine Verrechnung der Gebühren bei der Nutzung im Bereich eGovernment.

5.3.3 Schutz vor Identitätsdiebstahl

Identitätsdiebstahl ist ein besonders in den USA und in Großbritannien stark verbreitetes Verbrechen. Darunter wird der Betrug unter Zuhilfenahme einer gestohlenen oder anders erlangten Identität verstanden. Ermöglicht wird der Betrug durch die mangelnde Kontrolle angegebener Daten auf Seiten von Unternehmen und durch einen vergleichsweise sorglosen Umgang mit den eigenen Daten auf Seiten des Verbrauchers. In Deutschland ist es noch kein wirklich stark verbreitetes Problem, dennoch tritt es auch hierzulande auf[37]. Dies liegt vor allem daran, dass es einen Personalausweis gibt, mit dem Transaktionen, die persönlichen Kontakt beinhalten, abgesichert werden können. In Ländern ohne Personalausweis ist eine Kontrolle der Daten ungleich schwerer und erleichtert den Betrug. Ein Ziel bei der Einführung des

36 Siehe [Fri]

37 Ein Beispiel liefert eine recht persönliche Darstellung hier: http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung

nPA ist es, ein gleichwertiges Pendant zum herkömmlichen Ausweis für das Internet zu schaffen. Daraus folgt aber auch, dass es dort momentan noch keine ausreichende Kontrolle gibt und geben kann. Dies haben die vorangegangen Kapitel auch schon gezeigt. Demzufolge steigt allerdings auch die Gefahr des Identitätsdiebstahls mit dem Anteil der Transaktionen, die vom offline- in den online-Bereich verlagert werden.

Der nPA schützt nicht direkt vor Identitätsdiebstahl. Er kann nicht verhindern, dass Daten bei Anbietern, die keine ausreichende Verifikation der Daten betreiben, missbräuchlich verwendet werden. Er kann aber dafür sorgen dass

- weniger Daten gestohlen werden
- weniger Anbieter mit unzureichender Verifikation auf dem Markt sind

Dass weniger Daten gestohlen werden können, ergibt sich aus der verschlüsselten Verbindung. Insbesondere das Phishing kann man mit dem nPA verringert werden. Er kann selbstverständlich nicht verhindern, dass Verbraucher ohne ausreichendes Problembewusstsein die eigenen Daten freiwillig herausgeben oder veröffentlichen. Sei es über die eigene Homepage oder über Angaben in sozialen Netzwerken. Der nPA kann auch nicht verhindern, dass Daten aus nicht fachgerecht entsorgten Dokumenten gestohlen werden[38].

Sollte sich der nPA mit seinen Funktionen im eCommerce etablieren, so ist zu erwarten, dass die Nutzung der eID-Funktion ein De-facto-Standard wird. Das heißt, dass die Nutzung durch beide Seiten der Transaktion gewollt ist. Es ist zu erwarten, dass vor allem die Unternehmen mit relativ großem Marktanteil dann schnell auf die eID-Funktion zurückgreifen. Dadurch sinken die Möglichkeiten des Betrugs, da es auf der einen Seite weniger Anbieter ohne eID-Funktion geben wird und bei der Mehrzahl der Anbieter wohl der Verzicht auf die eID-Funktion mit erhöhten Sicherheitsmaßnahmen einhergehen wird. Dies kann zum Beispiel der Verzicht auf eine oder mehrere Zahlungsmöglichkeiten oder eine aufwendigere Verifikation der Daten bedeuten.

38 Zum so genannten „bin raiding“: [Hec06]

Der nPA kann also sowohl direkt durch seine Sicherheitsmechanismen als indirekt durch die mit der Verbreitung verbundene Entwicklung der Sicherheit für den Verbraucher von Nutzen sein.

5.3.4 Kosten des nPA für den Verbraucher

Für den Verbraucher entstehen vor allem zwei Kostenblöcke. Zum einen ist das die Gebühr für die Ausstellung des Personalausweises, zum anderen ist das der Kauf eines oder mehrerer Lesegeräte.

Bei der Ausstellungsgebühr muss berücksichtigt werden, dass sicher jeder ausweispflichtige Bürger ohnehin Personalausweis zulegen muss. Diese Kosten liegen im Moment bei 8 Euro. Es ist davon auszugehen, dass dieser Betrag beim nPA höher ausfällt. Dies ergibt sich aus einer allgemeinen Preissteigerung sowie der erweiterten Funktionalität und den damit verbundenen Kosten des Ausweises. Zusätzlich können auch noch Kosten für die qualifizierte elektronische Signatur anfallen. Diese ist optional. Die Kosten für die Signatur werden vermutlich turnusgemäß, höchstwahrscheinlich jährlich, anfallen.

Neben den Kosten für die Karte selbst muss der Verbraucher auch mit Kosten für die Anschaffung der nötigen Hardware rechnen. Um die Karte am eigenen Computer lesen zu können, ist ein Kartenleser nötig. Diese Kartenleser müssen einer technischen Richtlinie (TR-03119) des BSI entsprechen. Es wird drei verschiedene Arten von Lesegeräten geben:

- Cat-B
- Cat-S
- Cat-K

Die Basisversion (Cat-B) besitzt lediglich eine kontaktlose Schnittstelle. Die Karte wird auf das Lesegerät gelegt, den Rest der Funktionalität übernimmt die eCard-API. Cat-B-Lesegeräte besitzen kein PIN-Eingabefeld und können auch keine QES ausstellen. Diese Leser sind ausdrücklich dazu gedacht, einer breiten Masse einen möglichst einfachen Einstieg in die Funktionen des nPA geben zu können (Zitat aus der Richtlinie: „Zu Beginn des Aufbaus der Infrastruktur wird das Angebot an Diensten und somit der

Nutzen für den Anwender noch begrenzt sein. Daher müssen die Anschaffungskosten in einer Größenordnung liegen, die aus Sicht des Bürgers ein „Ausprobieren“ zulässt oder alternativ für die Subventionierung geeignet ist.“[39]). Die Cat-B-Leser sollen durch ihren Verzicht auf eine kontaktbehaftete Schnittstelle, eine Tastatur oder ein Display Kostenvorteile gegenüber den Cat-S und Cat-K-Lesern bieten. Sie sind allerdings nicht mehr als eine einfache Möglichkeit, mit der Karte zu kommunizieren. Für die Sicherheit der Verwendung des nPA sorgen sie nicht.

Ein Cat-S-Leser muss nur eine kontaktlose Schnittstelle haben, eine kontaktbehaftete Schnittstelle ist optional. Dafür muss er aber eine Tastatur zur Eingabe des PINs besitzen. Hierdurch wird die Sicherheit erhöht, da alle Schlüssel innerhalb des Gerätes generiert werden und somit Angriffe erschwert werden. Bei Cat-B-Lesern wird dagegen der PIN über die Tastatur des angeschlossenen Computers eingegeben, was dieses Verfahren anfällig für Angriffe wie das Protokollieren von Tastaturanschlägen („keylogging“) macht. Die Nutzbarkeit der QES ist bei diesem Typ optional.

Cat-K-Leser sind die Leser mit dem größten Funktionsumfang. Sie besitzen eine kontaktlose und kontaktbehaftete Schnittstelle, ein Display und eine Tastatur. Daneben müssen sie die QES unterstützen. Es ist zu erwarten, dass diese Leser auch am teuersten sein werden.

Die Lesegeräte sind nicht auf den nPA beschränkt sondern können auch andere Karten lesen. Daher bieten Cat-K-Leser dem Benutzer nicht Nutzen in Bezug auf den nPA, sondern durch die verschiedenen Schnittstellen auch den größtmöglichen Nutzen mit anderen Kartensystemen, seien dies andere Kartenprojekte seitens des Staates wie zum Beispiel die Gesundheitskarte oder privatwirtschaftliche Karten, beispielsweise von Banken.

Die Aufteilung der Lesegeräte nach ihren Eigenschaften lässt sich grob mit der Aufteilung vergleichen, die die ZKA getroffen hat[40].

Die Kosten für die Geräte lassen sich im Moment nur abschätzen. Verbreitete Karten wie zum Beispiel die Geldkarte nutzen kontaktbehaftete Kartenleser. Kontaktfreie

39 Quelle: [Bun09] S.19
40 Quelle: [Ini08]

Leser sind bisher nur wenige auf dem Markt. Ein Modell der Firma SCM[41], SCL011, implementiert laut dem Hersteller dabei schon ausdrücklich die technische Richtlinie des BSI. Der Preis liegt momentan bei knapp unter der Marke von 100,-Euro. Das Vorgängermodell wird im Shop des Herstellers für 64,95Euro angeboten[42].

Anwendung	Cat-B	Cat-S	Cat-K
eID	+	+	+
QES	-	O	+

Tabelle 4 nPA-Anwendungen nach Leserklasse[43]

Ein Leser der höchsten Kategorie wird ein Modell der Firma Reiner SCT, „cyberJack e-com plus R“, wird in der Version ohne das nötige kontaktlose Schnittstelle ab knapp unter 100,-Euro gehandelt[44]. Der Richtlinien-konforme Leser mit der nötigen RFID-Technologie soll Mitte des Jahres 2010 auf den Markt kommen. Daher ist eine Abschätzung des Preises heute schwierig, von einem dreistelligen Betrag sollte allerdings ausgegangen werden.

Es lässt sich feststellen, dass vor allem die Kosten für die Lesegeräte der Karten eine relativ große Hürde für die Benutzung des nPA darstellen. Ohne einen deutlichen Preisverfall bei den einfachen Lesern, kann nicht davon ausgegangen werden, dass der nPA von einer breiten Masse der Bevölkerung im Internet genutzt wird. Hier ist entweder der Staat oder eine privatwirtschaftliche Initiative gefordert, für eine Verbreitung der nötigen Kartenleser zu sorgen. Möglich ist dies zum Beispiel über eine Subventionierung der Geräte oder eine Kooperation der ausstellenden Behörde des nPA mit den Herstellern der Lesegeräte.

Es wird zu beobachten sein, ob sich der Einbau von Kartenlesern in neue Computer zum Standard entwickelt. So ist es heutzutage nicht mehr unüblich, dass Computer über eingebaute Fingerabdruckleser verfügen. Eine ähnliche Entwicklung wäre bei

41 Quelle: [SCM10]
42 Preise lt. www.scm-pc-card.de, dem Shop des Anbieters
43 Bedeutung der Kürzel: + = vorhanden; - = nicht vorhanden, O = optional
44 Verkaufspreis bei amazon.de am 19.02.2010 97,40 Euro

entsprechender Nachfrage sicher auch mit Kartenlesern möglich. Zumindest für Cat-B-Geräte scheint es problemlos möglich, diese in Tastaturen oder Gehäusen von Laptops zu integrieren, da sie keine eigene Tastatur oder Display benötigen. Müssten Nutzer den Ausweis nur noch in einen bestimmten Bereich ihrer Tastatur legen und bräuchten nicht einmal mehr ein eigenes Gerät, wäre der Nutzung der eID-Funktion des nPA sicher sehr geholfen. Es muss das Ziel aller Beteiligten sein, die Hürde für eine Nutzung so flach wie möglich zu halten. Dazu zählt neben dem Preis der nötigen Geräte auch die Anwenderfreundlichkeit von Hardware und Software.

6 Volkwirtschaftliche Effekte

In diesem Abschnitt wird versucht, die volkswirtschaftlichen Effekte, die Kosten und den Nutzen, des nPA darzustellen. Eine einheitliche Definition von volkswirtschaftlichem Nutzen gibt es nicht. Allgemein kann gesagt werden, dass unter den Begriff des volkswirtschaftlichten Nutzens alle Vorteile fallen, die sich für die Gesellschaft als Ganzes ergeben. Beispielsweise ist ein volkswirtschaftlicher Nutzen von Kindertagesstätten, die Möglichkeit der betreuenden Elternteile, wieder einer Arbeit nachzugehen. Diese Art von Nutzen wurde bisher nicht betrachtet.

Der bedeutendste Effekt, den der nPA gesamtwirtschaftlich hat, ist die Vermeidung von Kosten durch Betrug. Zwar haben wir den Kostenpunkt Betrug schon vorher betrachtet, es lohnt sich allerdings, dies auch unter gesamtwirtschaftlichen Gesichtspunkt zu tun. Betrug sorgt dafür, dass die Gewinne der Unternehmen geringer werden. Dies hat einen direkten Einfluss auf die Steuereinnahmen des Staates, diese werden ebenfalls gemindert. Daneben müssen Ressourcen dafür aufgewandt werden, Betrug einzudämmen. Dazu zählen die Kapitalbindung in den Versicherungen für Kapital, das sonst anderweitig investiert werden könnte, und Aufwendungen beim Staat zur Verfolgung und Bekämpfung von Betrug. Gäbe es keinen Betrug, könnten die verbrauchten Ressourcen woanders eingesetzt werden und mehr Nutzen stiften. Der nPA reduziert das Risiko von Betrug in seinen Einsatzgebieten und sorgt damit für einen gesamtwirtschaftlichen Nutzen. Wie groß dieser Nutzen ist, lässt sich nur schwer prognostizieren und quantifizieren. Es hängt direkt von der Intensität der Nutzung des nPA ab. In einem Szenario, in dem der nPA sich innerhalb von 5 Jahren durchsetzt und alle großen Marktteilnehmer im eCommerce ihre Angebote entsprechend umgestellt haben, ist der Nutzen sicher im ein Vielfaches höher, als wenn der nPA eine recht geringe Nutzung erfährt und fast ausschließlich im eGovernment eingesetzt wird.

Ein weiterer volkswirtschaftlicher Nutzen ist der Zeitgewinn eines jeden Bürgers, der durch die Nutzung von eGovernment-Lösungen realisiert werden kann. Es kann davon ausgegangen werden, dass online angebotene Dienstleistungen nicht so viel Zeit in Anspruch nehmen, wie dieselben Dienstleistungen vor Ort in einem Amt. Dies ergibt sich allein schon aus dem Wegfall von Warte- und Anfahrtszeiten. Ob die eigentliche

Durchführung der Dienstleistung schneller geht, müsste im Einzelfall geprüft werden. Daneben kann sich jeder Bürger den Zeitpunkt der Diensterbringung aussuchen und ist nicht auf Öffnungszeiten der Ämter angewiesen. Dieser Nutzen ist jedoch nicht quantifizierbar.

Volkswirtschaftliche Kosten des nPA sind zunächst einmal die Gebühren, die dem Bürger bei der Beantragung abverlangt werden. Dieses Geld kann nicht mehr für andere Zwecke ausgegeben werden und schmälert somit zunächst einmal den Konsum. Allerdings sind die Kosten von heute 8,-€ verteilt auf 10 Jahre Gültigkeit pro Person als gering einzuschätzen. Selbst eine zu erwartende Steigerung der Kosten wird diese Einschätzung nicht grundsätzlich ändern. Wobei zu erwähnen ist, dass diese Kosten nicht kennzeichnend für den nPA sind. Jede Form von Ausweisdokument verursacht in seiner Erstellung Kosten, deren zunächst kein direkter Nutzen aus dem Dokument an sich entgegensteht. Man besitzt es erst einmal nur. Die Diskussion der Sinnhaftigkeit der Anschaffungskosten impliziert eine Diskussion der Frage, ob überhaupt ein allgemeines Ausweisdokument gebraucht wird. Einige Staaten wie Großbritannien oder die USA verneinen diese Frage, andere wie die Bundesrepublik bejahen sie. Soll diese Frage nicht in die Beurteilung der Wirtschaftlichkeit des nPA einfließen, so dürfen lediglich die Mehrkosten eines elektronischen Personalausweises gegenüber der klassischen Variante in die Betrachtung einbezogen werden.

Kosten verursacht auch die Umstellung der Verwaltung auf den nPA. Hard- und Software müssen angepasst werden, das Personal muss auf die neuen Prozesse geschult werden. Dazu verursacht die Entwicklung des nPA und die Durchführung der Testprojekte Kosten. Auch bei diesen Kosten gilt, dass im Grunde nur die Differenz zu dem herkömmlichen, nichtelektronischen Ausweises angeführt werden kann. Daneben wird die nötige Hard- und Software nicht nur für den Personalausweis genutzt. So gibt es beispielsweise schon Fingerabdruckscanner, da diese für den ePass verwendet werden. Korrekt wäre es also, die anfallenden Kosten nach der Nutzung aufzuteilen, praktikabel erscheint dies allerdings nicht. So lassen sich im Grunde nur die Kosten für das Entwickeln und Testen des nPA anführen.

Zusammengefasst lässt sich sagen, dass volkswirtschaftlich gesehen die Entwicklungskosten dem Nutzen durch den Sicherheitsgewinn entgegenstehen. Die

anderen Kosten und Nutzen erscheinen eher klein, so dass die abschließende Wertung an den beiden zuvor genannten Kriterien vorgenommen werden kann. So lässt sich, betrachtet man den Gesamtumsatz im eCommerce von rund 21,7 Mrd. Euro[45], schon mit kleinen Verbesserungen in der Sicherheit ein großer Betrag sparen, der die Kosten der Einführung des nPA überwiegt.

[45] siehe [Bun10]

7 Abschließende Beurteilung und Fazit

Lohnt sich die Einführung des neuen Personalausweises? Diese Frage gilt es mit den gewonnenen Erkenntnissen zu beantworten. Eine klare, zu 100 Prozent sichere Antwort gibt es auf diese Frage nicht. Der nPA ist, das wurde gezeigt, mit einigen Kosten verbunden. Zunächst kostet die Entwicklung und Einführung das Land und damit den Steuerzahler Geld. Geld, dessen Ausgabe in Zeiten chronisch leerer Staatskassen gut überlegt sein muss. Andere Staaten haben auch einen elektronischen Ausweis eingeführt, daher lässt sich wohl sagen, dass diese Kosten im Vergleich mit anderen Staatsausgaben eine eher unter geordnete Rolle spielen. Um nicht nur bei der hoheitlichen Nutzung an der Grenze oder im Kontakt mit der Polizei von Vorteil zu sein, muss jeder interessierte Bürger allerdings weitere Investitionen tätigen. Die benötigten Kartenleser sind heute noch recht teuer, was zunächst den Zugang zur eID-Funktion erschweren wird. Solange keine günstige und einfache Version eines Lesers auf den Markt kommt, kann nicht davon ausgegangen werden, dass der nPA zu einer „Killer-Applikation“ wird. Hier sind Staat und/oder Industrie gefordert, preisgünstige Modelle anzubieten und vielleicht sogar mit Subventionen zu helfen. Die neue Technologie wird sich nur verbreiten können, wenn eine große Nutzerbasis vorhanden ist, die allen Marktbeteiligten die Entscheidung für die Nutzung des nPA leicht macht.

Unternehmen aus den untersuchten Bereichen müssen weiter in die nötige Infrastruktur investieren. Dies bedeutet, dass sie ihre Online-Portale auf die Nutzung mit dem nPA umstellen müssen, soll dieser Erfolg haben. Bleibt eGovernment lange Zeit die einzig vernünftige Nutzungsmöglichkeit, so wird die eID-Funktion des neuen Ausweises ein Schattendasein fristen. Aber auch hier ist der Staat gefordert, seine Schnittstelle zum Bürger möglichst attraktiv und benutzerfreundlich zu gestalten. Schafft er es nicht, die Vorteile des nPA zu kommunizieren und die Bürger zur Nutzung zu bewegen, dann wird man retrospektiv von einem gescheiterten und überflüssigen Projekt sprechen.

Das Potential des nPA und seine breiten Einsatzmöglichkeiten wurden ausführlich dargelegt. Er kann auf Märkten eingesetzt werden und helfen, die Produktivität zu steigern, die schon heute Milliardenmärkte sind und die weiter wachsen. Es wurden

eine Reihe von Nutzenpotentialen vorgestellt, die zusammengenommen ein deutliches Argument für den neuen Ausweis sind. Der Umfang des Nutzens wächst in vielen Fällen mit der Größe der Nutzerbasis, weshalb zuvor angesprochene Subventitionsmodelle nicht unrealistisch sind. Es bleibt die Frage, ob die Ersparnisse auf Seiten der Anbieter ausreichen, um eine solche Subvention zu rechtfertigen.

Die Einführung ist für den 1.November 2010 geplant. Ab diesem Zeitpunkt wird sich zeigen, wie gut der neue Ausweis angenommen wird. Einen ersten Blick auf den Erfolg des nPA kann man wohl in 3-4 Jahren wagen, wenn eine große Zahl alter Ausweise umgetauscht wurde. Gerade die Generation junger Menschen, die mit dem Internet aufwächst, wird die Ausweise aufgrund kürzerer Gültigkeitsdauer schneller erhalten und so bietet sich dann eine gute Basis für eine erste Evaluation. Wird der nPA ein Erfolg, so ist auch damit zu rechnen, dass viele Menschen vor Ablauf der Gültigkeit ihres alten Ausweises einen neuen beantragen.

Die Prognose, die Abschluss dieser Arbeit sein soll, ist, dass sich der nPA durchsetzen wird. Die Vorteile sind zu groß, um von Verbrauchern und Unternehmen ignoriert zu werden. Der alte Personalausweis hat sich im normalen Geschäftsverkehr durchgesetzt, es wäre überraschend, wenn der neue Ausweis Akzeptanzproblem beim Gebrauch im Internet hat. Die Preisprobleme der nötigen Hardware werden sich auch lösen lassen. Gerade der Markt für Computerelektronik zeichnet sich dadurch aus, dass Preise im Laufe der Zeit relativ stark fallen. Einer sicheren Nutzung der eigenen Identität im Internet steht bald nichts mehr im Weg.

8 Literaturverzeichnis

[Ben08] Bender, J., Kügler, D., Margraf, M., & Naumann, I. (2008). Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. *Datenschutz und Datensicherheit* , 173-177.

[BIT09] BITKOM. (22. 02 2009). Abgerufen am 25. 02 2010 von http://www.bitkom.org/de/presse/62013_57847.aspx

[BIT093] BITKOM. (2009). *E-Commerce - Konsumenten*. Abgerufen am 25. 02 2010 von http://www.bitkom.org/de/markt_statistik/46259_38540.aspx

[BIT092] BITKOM. (2009). *E-Government – Angebot*. Abgerufen am 25. 02 2010 von http://www.bitkom.org/de/markt_statistik/46259_38538.aspx

[BIT091] BITKOM. (2009). *E-Government – Nachfrage*. Abgerufen am 25. 02 2010 von http://www.bitkom.org/de/markt_statistik/46259_38537.aspx

[BIT07] BITKOM. (20. 06 2007). *ePA Workshop.* Abgerufen am 25. 02 2010 von http://www.bitkom.org/files/documents/ePA_Workshop_Resultate-2007-11-28-revision_(3).pdf

[BIT08] BITKOM. (18. 09 2008). *ePA Workshop II.* Abgerufen am 25. 02 2010 von http://www.bitkom.org/files/documents/ePA_Workshop_II_(7).pdf

[BSI10] BSI. (25. 02 2010). *Extended Access Control (EAC)*. Abgerufen am 25. 02 2010 von https://www.bsi.bund.de/cln_156/sid_A7C9DD1B56D70E5A7A286C575C3C0DD1/DE/Themen/ElektronischeAusweise/Sicherheitsmechanismen/sicherEAC/eac_node.html

[BSI101] BSI. (25. 02 2010). *Passive Authentication (PA)*. Abgerufen am 25. 02 2010 von https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Sicherheitsmechanismen/sicherPA/pa_node.html

[BSI102] BSI. (25. 02 2010). *Password Authenticated Connection Establishment (PACE)*. Abgerufen am 25. 02 2010 von

https://www.bsi.bund.de/cln_156/DE/Themen/ElektronischeAusweise/Sicherheitsmechanismen/sicherPACE/pace_node.html

[Bun09] Bundesamt für Sicherheit in der Informationstechnik. (17. 12 2009). Abgerufen am 25. 02 2010 von https://www.bsi.bund.de/cae/servlet/.../51686/BSI-TR-03119_V1_pdf.pdf

[Bun101] Bundesdruckerei. (25. 02 2010). *Sicherheitsmerkmale der Personalausweiskarte.* Abgerufen am 25. 02 2010 von http://www.bundesdruckerei.de/de/kunden/kunden_government/governm_persPass/persPass_sichmPersausw.html

[Bun091] Bundesministerium des Innern. (11. 02 2009). Abgerufen am 25. 02 2010 von http://www.bmi.bund.de/cae/servlet/contentblob/435832/publicationFile/20199/Umsetzungsplan2009_eGovernment.pdf

[Bun08] Bundesministerium des Innern. (02. 07 2008). Einführung des elektronischen Personalausweises in Deutschland.

[Bun10] Bundesverband des deutschen Versandhandels. (02. 02 2010). *2009 war Rekordjahr für den Versand- und Online-Handel.* Abgerufen am 25. 02 2010 von http://www.versandhandel.org/Pressemitteilung.96+M528eef50ab1.0.html

[Deu08] Deutsche Post. (07 2008). Leitfaden für die Nutzung der drei Postident-Verfahren.

[eBa10] eBay. (25. 02 2010). *eBay Presse Portal - Fakten Deutschland*. Abgerufen am 25. 02 2010 von http://presse.ebay.de/news.exe?content=FD

[Fre08] Frerichs, A., & Schumann, M. (08. 09 2008). *Peer-to-Peer Banking - State of the Art.* Abgerufen am 25. 02 2010 von http://www2.as.wiwi.uni-goettingen.de/getfile?DateiID=694

[Fri] Fritsch, L., & Rossnagel, H. (2005). Die Krise des Signaturmarkts – Lösungsansätze aus betriebswirtschaftlicher Sicht. In H. Federrath, *Sicherheit 2005* (S. 129-139). Regensburg.

[Gar10] Gartner. (05. 01 2010). Abgerufen am 25. 02 2010 von http://www.gartner.com/it/page.jsp?id=1272313

[Hec06] Hecker, A., & Gundel, S. (2006). *Identitätsdiebstahl und -betrug.* Freiburg: Identitätsdiebstahl und -betrug.

[Hom06] Homburg, C., & Krohmer, H. (2006). *Grundlagen des Marketingmanagements.* Wiesbaden: Gabler.

[ibi09] ibi research. (18. 08 2009). E-Commerce-Leitfaden. Regensburg.

[ibi091] ibi research. (10. 08 2009). Erfolgsfaktor Payment. Regensburg.

[ICA08]ICAO. (17. 04 2008). *electronic machine readable travel documents & passenger faciliation.* Abgerufen am 25. 02 2010 von http://www2.icao.int/en/MRTD/Downloads/Guidance%20Material/Machine%20Readable%20Travel%20Documents%20-%20Passenger%20Facilitation.pdf

[ide10] id.ee. (25. 02 2010). *Web-based services with ID-card support*. Abgerufen am 25. 02 2010 von http://www.id.ee/11108

[IDA05] IDABC. (07 2005). *eID in action: Estonia*. Abgerufen am 25. 02 2010 von http://ec.europa.eu/idabc/en/document/4487/5584

[Ini08] Iniative Geldkarte e.V. (29. 08 2008). Abgerufen am 25. 02 2010 von http://www.geldkarte.de/_www/files/pdf2/chipkartenleser_uebersicht_initiative-geldkarte_280808.pdf

[Ins10] Institut für Internet-Sicherheit FH Gelsenkirchen. (25. 02 2010). Abgerufen am 25. 02 2010 von http://www.internet-sicherheit.de/forschung/aktuelle-forschungsprojekte/elektronischer-personalausweis/epa-web-authentication-demo-video/

[ITB10] IT-Beauftragte der Bundesregierung. (25. 02 2010). *Teilnehmer am zentral koordinierten Anwendungstest*. Abgerufen am 25. 02 2010 von http://www.cio.bund.de/cln_102/sid_8DA042F403F27C0BDBF81D95E7E3BF09/DE/IT-Projekte/Neuer_Personalausweis/Anwendungstest_Neuer_Personalausweis/anwendungstest_node.html

[Kas09] Kaske, B.-O. (01. 07 2009). Abgerufen am 25. 02 2010 von https://www.sicher-im-netz.de/files/documents/privatnutzer/ePA_Allianz.pdf

[Kir08] Kirchmer, M. (2008). Process innovation through open BPM. In N. Pal, & D. Pantaleo, *From Strategy to Execution: Turning Accelerated Global Change Into Opportunity* (S. 87-105). Springer.

[Lay01] Layne, K., & Lee, J. (2001). Developing fully functional E-Government: A four stage model. *Government Information Quarterly* , 122-136.

[Mar10] Margraf, M. (07. 01 2010). Abgerufen am 25. 02 2010 von https://www.e-konsultation.de/netzpolitik/sites/default/files/Hintergrundinfo_Elektronischer%20Identit%C3%A4tsnachweis%20PA.pdf

[Rei05] Reichl, H. (2005). *Digitaler Personalausweis: eine Machbarkeitsstudie.* DUV.

[Sch09] Schaeff, A. (2009). Attraktive Anwendungen, Interview mit Hans Bernhard Beus. *Kommune 21* (9), 16-19.

[Sch00] Schedler, K. (2000). eGovernment und neue Servicequalität der Verwaltung. In M. Gisler, & D. Spahni, *eGovernment - Eine Standortbestimmung.* Bern: Verlag Paul Haupt.

[Sch03] Schultz, V. (2003). *Basiswissen Rechnungswesen.* München: dtv.

[SCM10] SCM Micro. (18. 01 2010). Abgerufen am 25. 02 2010 von http://www.scmmicro.com/fileadmin/products/datasheets/Flyer_SCL011_low.pdf

[Uni10] United Tickets. (25. 02 2010). *About us*. Abgerufen am 25. 02 2010 von http://www.unitedtickets.ee/about-us

[Ver09] Verhaeghe, P., Lapon, J., De Decker, B., Naessens, V., & Verslype, K. (2009). Security and Privacy Improvements for the Belgian eIDTechnology. *SEC*, (S. 237-247).