c't 23/10

Jürgen Kuri

# Der Internet-Ausweis

## Personalausweis mit elektronischer ID und Signatur

**Die letzten Vorbereitungen laufen, die letzten Zertifizierungen und Softwareanpassungen werden umgesetzt: Am 1. November startet der neue Personalausweis für alle Bundesbürger. Er soll nicht einfach nur den Bürger an der Grenze und im Inland gegenüber staatlichen Stellen identifizieren. Er soll auch das Internet sicherer machen und rechtssichere elektronische Anwendungen ermöglichen.**

Wo hab' ich denn jetzt nur wieder den Perso hingelegt? Aufräumen, hm. Ach, hier. In den Leser. Und die PIN. 123456. So, alles klar, die Bücher sind unterwegs. Okay, wenn ich schon dabei bin: Wo hab ich denn die URL der Krankenkasse? Eine Zusatzversicherung wollt' ich doch die ganze Zeit schon…" Einfacher, sicherer, bequemer – so ist das Leben mit dem neuen elektronischen Personalausweis, lautet das große Versprechen des Bundesinnenministeriums: „Der neue Personalausweis. Meine wichtigste Karte." Ab dem 1. November ist es nun tatsächlich soweit: Wer einen im Volksmund Perso genannten Ausweis beantragt, bekommt die neue elektronische Variante, von offizieller Seite nur noch als „neuer Personalausweis" oder kurz „nPA" tituliert.

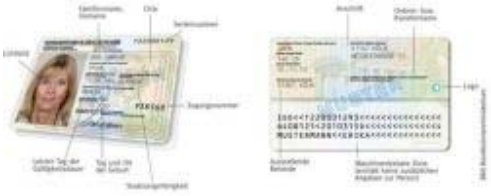
Die Basisdaten: Der nPA ist ein Ausweis im Kreditkartenformat mit RFID-Chip, der kontaktlos auslesbar ist. Er erfüllt die üblichen hoheitlichen Funktionen, wie man sie vom bisherigen Personalausweis kennt; Bürger weisen sich damit gegenüber offiziellen Stellen aus. Diese, nunmehr wie beim ePass biometriegestützte, Identitätsfunktion ist ausschließlich den zur Identitätsfeststellung berechtigten Behörden vorbehalten. Die hoheitliche Funktion ergänzt die normale Sichtprüfung des Ausweises, indem spezielle Lesegeräte, die nur befugten Behörden zur Verfügung stehen, die im Ausweis gespeicherten biometrischen Daten auslesen können. Dazu muss der Ausweis physisch vorliegen. Neben dem auch auf dem Chip gespeicherten Lichtbild können zwei Fingerabdrücke des Inhabers gespeichert werden – dies wurde aber zur freiwilligen Funktion erklärt, nachdem es heftige Kritik an einer erkennungsdienstlichen Zwangsbehandlung aller Bürger gegeben hatte.

Über die hoheitliche Funktion hinaus bietet der nPA zwei Neuerungen (siehe dazu den **Artikel auf S. 142[1]**). Erstens dient die eID (electronic Identity) der sicheren Online-Authentisierung am PC. Mit den auf dem Ausweis-Chip gespeicherten Daten kann sich der Inhaber auch im elektronischen Rechts- und Geschäftsverkehr über das Internet ausweisen. Dafür wird eine Infrastruktur aufgebaut, die auch Anwendungen und Anbieter gegenüber dem Nutzer, also dem Ausweisinhaber, zertifiziert (siehe **Artikel auf S. 138[2]**). Zweitens steht den Bürgern optional auch die qualifizierte elektronische Signatur (QES) auf der Ausweiskarte zur Verfügung, die allerdings jährliche Zusatzkosten von derzeit 60 bis 80 Euro verursacht. Die Signatur muss bei einem Dienstleister erworben und immer wieder erneuert werden. Für die meisten Nutzer genügte zwar eine fortgeschrittene Signatur, mit der man Dokumente signieren und verschlüsseln kann. Jedoch hat sich die Bundesregierung, trotz mancher Kritik auch aus Sicherheitskreisen, dagegen entschieden: Auf dem nPA sind nur qualifizierte Signaturen zulässig, die per Zertifikat abgesichert und rechtlich der Unterschrift gleichgestellt sind.

### Intelligentes Konzept

Also alles prima: Der Staat übernimmt eine Aufgabe, mit der lange gewünschte Funktionen wie etwa die elektronische Unterschrift oder sichere Authentisierung im Internet ermöglicht werden, die bislang an der fehlenden Infrastruktur scheiterten. Der Bundesdatenschutzbeauftragte Peter Schaar lobte gar, der

eID-Funktion des neuen Personalausweises liege „ein intelligentes und datenschutzfreundliches Konzept“ zugrunde. Das Lob von Schaar verdeutlichte eines: Angst vor Datensammelwut versuchten die Konstrukteure des nPA schon in der technischen Infrastruktur zu begegnen. Nicht alle wollen aber in die Lobeshymnen einstimmen. Die Kritik am neuen Personalausweis konzentrierte sich schnell auf die Frage, ob er überhaupt notwendig ist – und vor allem, ob er sicher ist.



Der neue Personalausweis (nPA) und seine einzelnen Bereiche
Bild: Bundesinnenministerium

Die hoheitliche Funktion erfüllt der nPA wohl weder schlechter noch besser als der bisherige maschinenlesbare Personalausweis. Dieser ist nicht durch besondere Fälschungsanfälligkeit aufgefallen, im Gegenteil. Die Sicherheitspolitiker sprechen aber trotzdem davon, dass die zusätzlichen biometrischen Identifikationsmerkmale, die auf dem nPA gespeichert sind, die Sicherheit noch erhöhten. Mit den auf dem nPA gespeicherten Fingerabdrücken könnte er „ähnlich wie der elektronische Reisepass als sicheres Reisedokument eingesetzt werden“, meint etwa das „Kompetenzzentrum neuer Personalausweis“. Die Freiwilligkeit der Fingerabdruck-Speicherung macht diese Funktion aber nicht zu einem offiziellen Bestandteil der Ausweisfunktion.

Heftiger unter Beschuss geriet der nPA in den letzten Wochen vor allem wegen angeblicher Sicherheitsmängel. Besonders der Chaos Computer Club hat diese Kritik etwas polemisch vorgetragen; dabei unterlief ihm auch eine falschen Analogie zur SuisseID, einem einfachen USB-Stick für fortgeschrittene Signaturen, den die Privatwirtschaft ausgibt. Konkret belegt hat der CCC lediglich einen eigentlich banalen Sachverhalt: Auf einem Computer, der nicht vor Schadsoftware geschützt ist, können Tastatureingaben abgehört werden.

**Trojaner**

Das Problem, das das Szenario des CCC illustrierte, resultierte aus der Kombination eines Basis-Kartenlesegeräts mit einem Trojaner-verseuchten PC. Dass beim Einsatz des Basislesers die Integrität des PC, an den er angeschlossen ist, eine zentrale Voraussetzung für die Sicherheit des gesamten Systems ist, stellt allerdings keine Neuigkeit dar. Basisleser (Cat B), Standardleser (Cat S) und Komfortleser (Cat K) bieten alle eine kontaktlose Schnittstelle nach ISO 14443 zur Karte sowie die eCard-API zum Host-PC. Cat-S-Geräte bieten aber zudem unter anderem die Möglichkeit, über ein eigenes PIN-Pad die sechsstellige nPA-PIN sicher einzugeben, ohne Nutzung eines virtuellen PIN-Pads oder der PC-Tastatur wie beim Basisleser (siehe dazu den **Artikel auf S. 142[3]**). Beim Komfortleser kommen darüber hinaus ein zweizeiliges Display, ein kontaktbehaftetes Interface nach ISO 7816 sowie die Zertifizierung nach den Common Criteria hinzu. Komfortleser sind für den Einsatz der digitalen Signatur Voraussetzung.

Der Ausweis vermag keine Wunder zu vollbringen. Er macht infizierte PCs nicht sicher, auf denen Keylogger die Zugangsdaten zu Online-Shops, Bezahldiensten und anderen Plattformen ausspionieren oder Banking-Trojaner die Konten leerräumen. Doch er kann sogar unter solchen Umständen – auch in Verbindung mit dem Basisleser – das Schadensrisiko

**Die Kosten**

Neben den Kosten für den elektronischen Personalausweis selbst muss der Bürger unter Umständen für den neuen Personalausweis zusätzliche Ausgaben einplanen. Der Ausweis selbst schlägt für im Normalfall für Bürger ab 24 Jahren mit 28,80 Euro zu Buche, Bürger unter 24 Jahren zahlen 22,80 Euro. Das Aktivieren der Online-Funktion des Ausweises (eID) ist nur bei Ausweisausgabe gebührenfrei. Wird die Online-Funktion zu einem späteren Zeitpunkt im Amt aktiviert, kostet dies 6 Euro.

Das Deaktivieren der Online-Funktion oder das Sperren dieser Funktion beim Ausweisverlust bleibt gebührenfrei, ein Entsperren (etwa bei einem wiedergefundenen Ausweis) kostet 6 Euro. Auch die im Online-Verkehr benötigte sechsstellige PIN-Nummer ist nur bei der Ausweisausgabe kostenlos. Wird die PIN vergessen oder besteht der Verdacht auf einen Missbrauch, so kostet die PIN-Änderung wiederum 6 Euro.

Kosten für eine qualifizierte digitale Signatur sind durch den Gesetzgeber nicht festgelegt, ihre Festsetzung bleibt den Signaturanbietern überlassen. Derzeit bewegen sie sich im Rahmen von 60 bis 80 Euro pro Jahr; das Innenministerium erhofft sich von der Signatur-Funktion des nPA einen Schub für die Signaturen, der sie auch verbilligen soll.

Um die ID-Funktionen des nPA zu Hause

verringern. Denn es ist etwas anderes, ob ein Betrüger mit ausspionierten Zugangsdaten von jedem beliebigen Internet-Zugang aus auf Online-Konten zugreifen kann, oder ob er ihm nur über Schadsoftware auf dem Computer des Konto-Inhabers möglich ist – und das nur, sofern der gerade seinen Ausweis auf dem Lesegerät liegen hat. Dabei muss die Schadsoftware die AusweisApp so manipulieren, dass sie den Zugriff auf die eID-Funktion nicht meldet, und eventuell auch noch die PIN-Eingabe am virtuellen Tastaturpad analysieren. Allerdings belegen Banking-Trojaner, dass Betrüger durchaus bereit sind, vergleichbaren Aufwand zu betreiben, wenn nur der Gewinn hoch genug ist.

Der Bundesdatenschutzbeauftragte Peter Schaar hatte deshalb gefordert, einfache Lesegeräte nicht einzusetzen. Andere Datenschützer kritisieren zudem, dass das Bundesinnenministerium mit seiner Werbung für den nPA zu sehr den Eindruck erweckt, mit dem neuen Ausweis werde automatisch alles besser. Sehr viel Verantwortung wird auf den Anwender übertragen, der dafür zu sorgen hat, dass seine Systeme für den nPA-Einsatz geeignet und ausreichend gesichert sind.

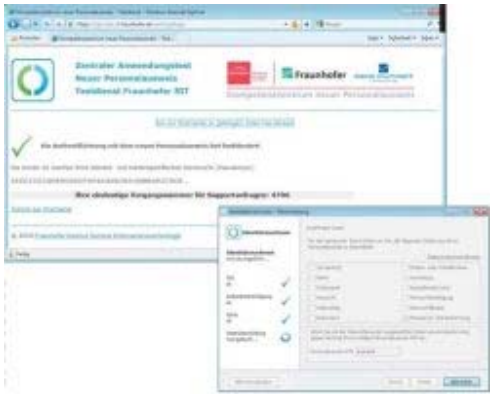
Trotz der Sicherheitsbedenken hat auch der Basisleser eine Daseinsberechtigung: Er ebnet mit günstigen Einstiegskosten und der Möglichkeit, ihn etwa in Notebooks zu integrieren, dem System den Weg in die Breite. Wenn der Markt groß genug ist, werden die Preise für sichere Lesegeräte sinken: Ein Standardleser für 35 und ein Komfortleser für 60 Euro sollten dann möglich sein. Aber auch der Einsatz von Standard- oder Komfortlesern enthebt den Anwender nicht der Verantwortung für die Sicherheit seines PC – und sollte auch nicht zur Aufgabe eines gewissen Misstrauens und immer neuer Kontrolle der Vorgänge rund um den nPA führen. Zwar lässt das BSI alle beteiligten Komponenten – sieht man vom Anwender-PC selbst ab – prüfen und zertifiziert sie. Dass dies jedoch kein Allheilmittel ist, zeigte im Juni diesen Jahres der Hack von Kartenlesern, die vom BSI zertifiziert und unter anderem fürs Homebanking zugelassen waren.

einzusetzen, benötigt jeder User einen Kartenleser. 1,5 Millionen Sicherheitskits mit Kartenlesern sollen bis Dezember 2011 an die Bürger ausgegeben werden, im Rahmen des Konjunkturpakets II sind dafür 24 Millionen Euro vorgesehen. Basis-Kartenleser sollen teilweise mit Zeitschriften zu den Bürgern kommen, aber auch auf anderem Wege sollen Bürger die Kits kostenlos erhalten können. Bis zum Redaktionsschluss stand immer noch nicht endgültig fest, welche Leser kostenlos oder zu einem geringen Aufpreis mit diesem Programm verteilt werden – unter anderem deswegen, weil die Zertifizierung der Kartenleser für die nPA-Infrastruktur nicht abgeschlossen war. Im normalen Verkauf kosten den Basis-Lesern entsprechende Klasse-1-Leser derzeit rund 20 bis 30 Euro, Klasse-2-Leser (Standard-Leser) sind für rund 30 bis 80 Euro zu haben. Die Klasse-3-Leser (die den Komfort-Lesern entsprechen) sind unter anderem für die Nutzung der digitalen Signatur Voraussetzung und schlagen mit rund 90 bis 160 Euro zu Buche.

**Politische Sicherheit**

Die technische Sicherheit des nPA ist die eine Seite. Grundsätzlichere Kritik richtet sich aber gegen die politische Sicherheit: Peter Schaar wies darauf hin, dass der Staat mit der eID „eine neue Schlüsselfunktion“ zwischen Konsumenten und Diensteanbietern einnimmt und durch die Zertifikatausteilung und -entziehung „eine enorme Macht ausübt“, ohne dass geklärt wurde, an welche Voraussetzungen dies geknüpft ist und welche Vorstellung von Zuverlässigkeit des Diensteanbieters dem zugrunde liegt. Oder, anders formuliert: Die politischen Rahmenbedingungen für den nPA können sich jederzeit ändern.

Immer wieder tauchen daher Bedenken auf, der nPA werde zu einer Art Eintrittsberechtigung für das Internet. Die Debatten um illegale Downloads urheberrechtlich geschützten Materials, um Online-Kinderpornographie, um Cyber-Mobbing, also um Rechtsverstöße, die einige Politiker und Lobbyisten im Internet entdecken, bringen Forderungen nach eindeutiger und ständiger Identifikation jeden Internet-Nutzers hervor. Was also läge näher, die Identifikation per nPA zur Voraussetzung für den täglichen Eintritt ins Netz zu machen?



Solche Begehrlichkeiten tauchen in den verschiedensten

Der Personalausweis enthält auch eine Pseudonym-Funktion, mit der man sich gegenüber Anbietern eindeutig identifizieren kann, ohne etwa den Namen oder andere persönliche Merkmale preisgeben zu müssen. Für einige Internet-Anwendungen reicht diese Art der Identifizierung vollständig.

Gewändern auf; ein Bundestagsabgeordneter stellte gar in Frage, ob man denn auf öffentlichen Plattformen wie abgeordnetenwatch.de überhaupt Fragen an Abgeordnete ohne eindeutige Legitimation stellen dürfe. Auch Lobby-Gruppen bringen ab und zu Vorschläge aufs Tapet, eine genauere Identifikation der Internet-Nutzer solle von vornherein ausschließen, dass in der mehr oder weniger ausgeprägten Anonymität des Netzes ein rechtsfreier Raum entstünde. Noch unter Wolfgang Schäuble, dem eher als Scharfmacher bekannten Vorgänger des gegenwärtigen Bundesinnenministers Thomas de Maizière, dementierte das Innenministerium: „Pläne zu einem Internet-Ausweis mit der Möglichkeit der Rückverfolgung“ lägen nicht vor. Es gebe keine Vorhaben, Internet-Nutzer staatlicherseits zu identifizieren. Die Befürchtung bleibt aber bei vielen Skeptikern bestehen, dass sich diese politischen Vorgaben auch schnell ändern können – und mit dem nPA die technische Infrastruktur dafür vorhanden ist.

**Startschuss**

Ärgern werden sich die Bürger aber möglicherweise erst einmal über viel einfachere – und auch viel gewohntere – Unbilden. Die entstehen, wer hätte es gedacht, auf dem Amt. Die Kommunen und Ordnungsämter stöhnen unter den Belastungen und Kosten, die die Einführung des nPA mit sich bringt – und hängen mit der Integration der Technik ebenso mit der Ausbildung der Mitarbeiter weit hinterher. So meinte etwa Anton Hanfstengl, Leiter des Bürgerbüros München, dass man die Zeit bis zur Einführung und die mit dem Projekt verbundenen Schwierigkeiten unterschätzt habe. Manchen Kommunalbeamten graut es zudem schon davor, dass die Bürger möglicherweise bei technischen Problemen mit Kartenlesern und nPA-Software Rat bei den Ordnungsämtern suchen – wofür die Ämter weder ausgerüstet noch die Mitarbeiter ausgebildet sind.

Fast wie beim Abschluss eines Mobilfunkvertrags: Nach Erhalt des neuen Personalausweises trudelt auch ein Brief mit PIN und PUK ein.

Bislang hat die Beantragung des Personalausweises fünf bis zehn Minuten gedauert, heißt es in den Kommunen. Künftig dürfte die Prozedur eine halbe Stunde beanspruchen. Verantwortlich dafür ist der zusätzliche Informationsbedarf angesichts der neuen Funktionen, die der nPA mit sich bringt, außerdem müssen die Bürger bis zu vier Unterschriften während des Antragsprozesses leisten: die Unterschrift für den Ausweis; die Bestätigung, dass man auf die Fingerabdrücke verzichtet oder die Fingerabdrücke haben will; die Bestätigung, dass man die Belehrungsbroschüre erhalten hat und sie lesen wird; die Unterschrift, dass man zur Kenntnis nimmt, was alles beim nPA auf dem Amt kostenpflichtig ist. Weitere Probleme erwarten die Kommunen durch zusätzliche Informationsbedürfnisse der Bürger etwa beim Neusetzen der PIN. Allein die Aufgaben, die die Mitarbeiter am sogenannten Änderungsterminal, mit dem etwa die eID nachträglich aktiviert, die PIN geändert oder die PUK neu gesetzt werden kann, zu erfüllen haben, verlängern die Wartezeiten für den einzelnen Bürger.

Klagen hörte man aus den Kommunen vier Wochen vor dem Starttermin, dass die Technik bei weitem noch nicht funktioniert. Besonders die Änderungsterminals, die von der Bundesdruckerei geliefert werden, machten Ärger – dass Microsoft-Software vorausgesetzt werde, sei da nur ein Nebenaspekt.

Nur am Rande sei angemerkt, dass ebenfalls vier Wochen vor dem offiziellen Einführungstermin des nPA die Zertifizierungsprozesse für die Lesegeräte nicht abgeschlossen waren. Überraschenderweise aber auch nicht für den NXP-Chip, der auf den nPA verbaut wird: Die Zertifizierung für die digitale Signatur war noch nicht vollständig in trockenen Tüchern. All das sollte sich aber zum Starttermin erledigt haben, versprachen die beteiligten Techniker. Zumindest für den RFID-Chip mag dies gelten. Lesegeräte allerdings dürften erst nach und nach in größerer Zahl mit der notwendigen Zertifizierung ausgestattet sein. Dass trotzdem am Einführungstermin 1. November festgehalten wird, illustriert die Dringlichkeit, mit der der Gesetzgeber dies Projekt verfolgt.

Bei aller Kritik aufgrund technischer und politischer Bedenken, bei allem Stöhnen über den Zeitdruck zur Behebung der Schwierigkeiten kurz vor dem Start: Der nPA, das dazugehörige Softwaresystem und die technische sowie organisatorische Infrastruktur stellen das bislang ambitionierteste IT-Projekt dar, das tatsächlich auch erfolgreich realisiert zu werden verspricht – ganz anders also als beispielsweise die unselige Gesundheitskarte. Aber lohnt sich denn dieser ganze Aufwand, haben nicht vielmehr die Kritiker recht, die Sicherheit, politische Sinnhaftigkeit und Notwendigkeit des Großprojekts in Frage stellen?


An den Änderungsterminals, die in den zuständigen Behörden der Kommunen zu finden sind, können Ausweisinhaber die eID nachträglich freischalten lassen, die PIN ändern oder die PUK neu setzen.

Oder, anders gefragt: Ob's wirklich einfacher wird? Für gewohnte Transaktionen im Web, die man bislang etwa mit User-ID und Passwort abwickelte, wird mindestens eine Umgewöhnung notwendig; neue Anwendungen erleichtern das Leben. Ob's sicherer wird? Grundsätzlich ja, viele Dienste können vom ePerso profitieren – wenn auch die Anwender mitspielen. Ob sich neue Möglichkeiten eröffnen? In vielen Bereichen lassen sich Angebote realisieren, die bislang nicht oder nur sehr aufwendig umzusetzen waren. Am 1. November habe ich jedenfalls schon was vor: Sollte das Bürgerbüro ums Eck nicht völlig überlastet sein, besorge ich mir einen nPA. (jk)

**Der Internet-Ausweis**

Artikel zum Thema "Der Internet-Ausweis" finden Sie in c't 23/2010:

- Der neue Personalausweis: eID und digitale Signatur - **Seite 132[4]**
- Anwendungen für den digitalen Personalausweis - **Seite 138[5]**
- Der neue Personalausweis im Praxistest - **Seite 142[6]**

---

**URL dieses Artikels:**
http://www.heise.de/ct/artikel/Der-Internet-Ausweis-1111003.html

**Links in diesem Artikel:**
[1] http://www.heise.de/kiosk/archiv/ct/10/23/142/
[2] http://www.heise.de/kiosk/archiv/ct/10/23/138/
[3] http://www.heise.de/kiosk/archiv/ct/10/23/142/
[4] http://www.heise.de/kiosk/archiv/ct/10/23/132/
[5] http://www.heise.de/kiosk/archiv/ct/10/23/138/
[6] http://www.heise.de/kiosk/archiv/ct/10/23/142/