

Standpunkt

Der neue Personalausweis – mehr Chancen, mehr Risiken, mehr Verantwortung für den Bürger. Seit dem 1. 11. 2010 ist der neue Personalausweis im Scheckkartenformat verfügbar. Die auf dem Ausweis sichtbar aufgeführten Daten sind mit Ausnahme der Unterschrift, einschließlich des biometrischen Gesichtsbildes und der fakultativ zu speichernden Fingerabdrücke in einem Chip gespeichert und elektronisch auslesbar und bieten neue Funktionen zum Identitätsmanagement. Der Ausweis ist nach Meinung der offiziellen Stellen gegen den unbefugten Zugriff auf dem aktuell höchsten Stand der Technik gesichert. Inwieweit diese Einschätzung zutrifft, wird verlässlich erst die Praxis zeigen.

1. eID-Funktion. Der neue Personalausweis kann auch als elektronischer Identitätsnachweis (eID) im Internet genutzt werden. Die eID-Funktion ermöglicht dem Ausweisinhaber, sich sowohl im E-Government als auch im E-Commerce gegenüber berechtigten Stellen zu identifizieren. Wer die eID-Funktion nicht verwenden möchte, kann die Funktion bei der Ausgabe deaktivieren lassen. Die Daten, die im Chip auf dem Ausweis gespeichert sind, können nach Zustimmung des Ausweisinhabers mit seiner PIN an einen Internet-Dienst übertragen werden. Diese Funktion soll im Zeitalter des Internets das Alltagsleben erleichtern, dem Gebot der Datensparsamkeit dienen und den Geschäftsverkehr sicherer machen. Dabei werden stets nur die Daten übertragen, die der Anbieter für die Erbringung seines Dienstes benötigt. Entscheidender Vorteil: Gegenüber der herkömmlichen Authentisierung durch Passwörter besteht eine weitere Absicherung des Verfahrens durch das Besitzerfordernis des Ausweises. Die Legitimation erfordert sowohl das Wissen der PIN als auch den Besitz der Karte. Um die eID-Funktion am PC nutzen zu können, benötigt man einen Kartenleser. Wer diese Funktion nutzen will, sollte sich einen Komfortleser anschaffen, der über eine eigene Tastatur zur Eingabe der PIN und über ein eigenes Display verfügt. Die einfachen Basis-Lesegeräte, die von der Bundesregierung in großer Stückzahl kostenlos zur Verfügung gestellt wurden, erfüllen die Anforderungen der Datensicherheit hingegen nicht umfassend.

2. Elektronische Signatur. Eine weitere neue Funktion des elektronischen Personalausweises ist die Unterschriftsfunktion. Mit der elektronischen Signaturfunktion können Verträge sowie Transaktionen, die eine eigenhändige Unterschrift erfordern, über das Internet geschlossen werden. Die Speicherung der Signatur auf dem Chip des Personalausweises erfolgt jedoch nur, wenn der Ausweisinhaber dies möchte und sich die Signatur nach der Ausgabe des Ausweises besorgt. Hierfür entstehen zusätzliche Kosten.

3. Biometrische Merkmale. Neben dem obligatorischen Lichtbild können auf Antrag auch Fingerabdrücke auf dem neuen Personalausweis gespeichert werden. Mit der Preisgabe und Speicherung der Fingerabdrücke als äußerst sensible Daten werden Missbrauchsrisiken eröffnet, denen kein entscheidender Vorteil für den Ausweisnutzer

gegenübersteht. Daher sollte sich jeder Antragsteller genau überlegen, ob er seine Fingerabdruckdaten auf dem Personalausweis speichern lassen will.

4. Neue Verantwortung für die neue Technik. Die elektronischen Funktionen des Personalausweises bieten eine Reihe interessanter und durchaus zeitsparender Neuerungen. Gleichzeitig resultieren für die Ausweisinhaber aus den neuen Einsatzfeldern aber auch Risiken, so dass eine höhere Verantwortung des Bürgers im Umgang mit dem neuen Ausweis erforderlich wird. Dies hat auch der Gesetzgeber erkannt.

4.1 Hinterlegungsfähigkeit. Nach dem neuen Personalausweisgesetz darf vom Ausweisinhaber grundsätzlich nicht mehr verlangt werden, den Ausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben (§ 1 I 3 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften, BGBl I 2009, 1346). Ausweisinhaber sollten ihren neuen Personalausweis daher möglichst nie aus der Hand geben oder unbeobachtet lassen.

4.2 Unzulässigkeit des Vervielfältigens? Umstritten ist die Frage nach der Zulässigkeit des Kopierens und des Scannens von Ausweisen. Das Bundesinnenministerium vertritt eine sehr restriktive Auffassung: Aus der Eigentums- und Verfügungsbefugnis des Bundes über Pässe und Personalausweise folge, dass eine Vervielfältigung durch fotokopieren, scannen oder sonstige Ablichtung unzulässig sei. Daran bestehen erhebliche Zweifel: Der Gesetzgeber wollte allein der missbräuchlichen Nutzung des Ausweises zu Zwecken der elektronischen Kommunikation einen Riegel vorschieben. Anders als bei der Hinterlegungsfähigkeit hat der Gesetzgeber daher kein Verbot des Vervielfältigens erlassen. § 20 II Personalausweisgesetz regelt lediglich die Unzulässigkeit des automatisierten Abrufs sowie der automatisierten Speicherung von personenbezogenen Daten zu anderen Zwecken als dem elektronischen Identitätsnachweis durch öffentliche und nicht öffentliche Stellen. Ein Vervielfältigen durch den Betroffenen ist gesetzlich nicht ausgeschlossen. Aus datenschutzrechtlichen Gründen ist daher wie folgt zu differenzieren: Grundsätzlich ist eine Anfertigung von Ausweiskopien durch den Ausweisinhaber oder mit dessen Einwilligung oder auf Grund gesetzlicher Regelung auch durch dritte Stellen möglich. Zu beachten ist jedoch, dass die Ausweisdaten durch dritte Stellen grundsätzlich nicht automatisiert gespeichert werden dürfen. Daher ist Sorge zu tragen, dass bei Kopien durch Dritte eine sofortige Löschung im Speicher des Kopiergeräts erfolgt. Das Scannen von Ausweisen durch dritte Stellen sollte demgegenüber nicht erfolgen, da der Scanvorgang gerade auf dem Prinzip einer automatisierten Speicherung und Übermittlung beruht. In jedem Fall gelten für Stellen, die Kopien anfordern oder solche selbst vornehmen, die Regelungen der Datensparsamkeit und der Erforderlichkeit. Personenbezogene Daten, die nicht benötigt werden, sollten daher in den Kopien geschwärzt werden.

4.3 *Sicherheitsanforderungen an den Nutzer.* Insgesamt hat der Ausweisinhaber die gleichen Sicherheitsanforderungen zu beachten wie der Internetnutzer. So ist die PIN geheim zu halten und von dem Ausweis getrennt zu verwahren. Bei Bekanntwerden der Geheimnummer an Dritte muss der Inhaber die PIN entweder sofort ändern oder die Funktion des elektronischen Identitätsnachweises ausschalten lassen.

5. *Ausblick.* Der elektronische Personalausweis hat das Potential, sich für die künftigen Prozesse der elektronischen Kommunikation als ein wichtiger Schrittmacher zu erweisen. Die Akzeptanz seiner neuen Funktionen wird wesentlich von der Nutzung durch Bürgerinnen und Bürger abhängig sein, aber auch von der Bereitschaft der Diensteanbieter, sich zertifizieren zu lassen und die für ihre Geschäftszwecke oder die Wahrnehmung ihrer Aufgaben erforderlichen Daten des Identitätsnachweises beim Ausweisinhaber abzufragen.

Prof. Dr. Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, Hamburg