

Die Sicherheit des elektronischen Personalausweises.

Eine Frage des Einkommens?

Einleitung

Der neue elektronische Personalausweis ist ein umstrittenes Projekt, welches Vorteile bietet, aber auch Risiken in sich trägt. Seit November 2010 ist er schon im Umlauf. Nach Angaben des Personalausweisportals wurde er bereits an 9 Millionen Mal ausgestellt. *„Im praktischen Scheckkartenformat eröffnet der neue Personalausweis mit der Online-Ausweisfunktion die Möglichkeit, sich auch auf elektronischem Wege verlässlich auszuweisen. In den nächsten Jahren wird er sich zum Standard-Identitätsnachweis im Netz entwickeln und die Angebote von Wirtschaft und Verwaltung deutlich sicherer und einfacher machen.“*¹ Das Personalausweisportal ist nach außen von den Sicherheitsstandards des neuen Dokuments überzeugt, sie seien auf höchstem Niveau, heißt es. Doch von dem Sicherheitsniveau, wie es von den offiziellen Behörden dargestellt wird, ist die Realität scheinbar noch weit entfernt. So konnte der Chaos Computer Club (CCC) noch im Oktober 2010, also noch vor der offiziellen Einführung des Dokuments in Deutschland, erhebliche Sicherheitsprobleme des Dokuments praktisch demonstrieren². Der CCC kritisierte zudem die Informationspolitik des Ministeriums des Innern in Bezug auf die Sicherheitsrisiken des elektronischen Personalausweises. Zudem scheint das Sicherheitsniveau bei der Nutzung der Online-Funktionen auch eine Frage des Geldes zu sein, denn sicherere Lesegeräte kosten auch mehr.

In dieser kurzen Abhandlung geht es um den elektronischen Personalausweis aus der Sicht der Datensicherheit. Dabei werden zunächst die wesentlichen Funktionalitäten (die Online-Ausweisfunktion und die Unterschriftsfunktion) des Dokumentes umrissen. Daraufhin werden potentielle Risiken angesprochen, die daraus resultieren könnten. Dabei wird kein Anspruch auf Vollständigkeit erhoben.

1 [2]

2 [3]

Die wesentlichen Funktionalitäten des elektronischen Personalausweises

Der elektronische Personalausweis kann zunächst einmal wie der klassische Ausweis in der „analogen“ Welt eingesetzt werden, um die eigene Identität nachzuweisen. Wenn die erweiterten Online-Funktionen deaktiviert sind, bietet er gegenüber der alten Version keinen Vorteil, außer dass er bedingt durch seine Größe besser ins Portemonnaie passt. Eine Weiterentwicklung stellen die elektronischen Funktionen dar, die freiwillig genutzt werden können, aber auch das Leben erleichtern sollen. Dafür *„enthält er einen Mikroprozessor, der in der Lage ist, [... kryptografisch] Protokolle [...] auszuführen, und der geheime Schlüssel und Zertifikate speichern sowie weitere Schlüssel sicher erzeugen kann. Außerdem können in seinem Speicher persönliche Daten des Inhabers abgelegt werden. Dieser Chip wird über eine kontaktlose Schnittstelle angesprochen“*³. Um die Online-Funktionen nutzen zu können, benötigt der Nutzer einen Chipkartenleser für kontaktlose Chipkarten sowie ein Programm, die AusweisApp. Damit ausgerüstet kann der Ausweis im Wesentlichen zum einen dazu genutzt werden, sich online auszuweisen, also die Identität nachzuweisen und zum anderen dazu, digitale Dokumente *„rechtsverbindlich zu unterzeichnen“*⁴. Beide Funktionalitäten bringen Risiken mit sich, aber dazu später.

Borges, Schwenk, Stuckenberg und Wegener zählen zwei Haupteinsatzbereiche der Ausweisfunktion auf: E-Commerce (elektronische Kommunikation zwischen privaten Parteien, also Personen, Unternehmen etc.) und E-Government (elektronische Kommunikation zwischen Staat und Bürgern). Zu den Einsatzmöglichkeiten zählen sie im ersten Fall Handel (z.B. Altersnachweis, Onlineeinkauf etc.), Banken (Online-Banking inkl. Kontoeröffnung), Versicherungen (z.B. Onlineanträge, Schadensmeldungen etc.), allgemein Wirtschaft (Vertragsabschlüsse

³ [1], S. 157

⁴ [2]

zwischen Unternehmen, Arbeitsverträge etc.). Zusätzlich wäre ein Einsatz als Identitätsnachweis in Social Networks denkbar. Zum zweiten Haupteinsatzbereich zählen die Autoren Einätze im Bereich Soziales (z.B. Anträge auf staatliche Sozialleistungen), Verkehr (Auszüge aus dem Verkehrsregister), Umzug (Melderegister), Arbeit (polizeiliches Führungszeugnis) sowie Antragsstellungen aus dem Bereich Justiz⁵.

Bei der Unterschriftfunktion geht es darum, digitale Dokumente zu rechtsverbindlich zu unterschreiben, ohne sie ausdrucken und per Post verschicken zu müssen. Auf diesem Wege sollen rechtsverbindliche Willenserklärungen abgegeben oder Verträge abgeschlossen werden können⁶. Wie bei der Ausweisfunktion ist auch der Einsatz der Unterschriftsfunktion sowohl zwischen privaten Parteien als auch zwischen Bürger und Staat (z.B. bei Anträgen) denkbar.

Risiken der Online-Ausweisfunktion – eine Frage des Geldes?

Der wohl schlimmste Fall, der bei der Nutzung der Online-Ausweisfunktion auftreten kann, ist Identitätsdiebstahl. Es wäre in diesem Fall z.B. denkbar, dass jemand mit einer fremden Identität ein Bankkonto eröffnet und damit kriminelle Geschäfte betreibt, für die theoretisch der Besitzer des Ausweises verantwortlich gemacht werden könnte. Denn der Ausweisinhaber hat *„zumutbare Maßnahmen zu treffen, damit keine andere Person Kenntnis von der Geheimnummer erlangt“*⁷. Ferner soll er den Identitätsnachweis nur in einer Umgebung nutzen, *„die nach dem jeweiligen Stand der Technik als sicher anzusehen ist“*⁸.

Die Online-Ausweisfunktion beinhaltet von sich aus Sicherheitsfunktionen.

⁵ [1], S. 153f.

⁶ vgl. [2]

⁷ [4], 5. (2)

⁸ [4], 5. (3)

So ist der alleinige Besitz des Ausweises genauso wenig ausreichend, wie der alleinige Besitz der dazugehörigen PIN. Erst wenn der Ausweis Kontakt zum Lesegerät hat und der Nutzer im Besitz der PIN ist, kann er zum Ausweisen genutzt werden. D.h. selbst wenn ein Angreifer im Besitz der PIN ist, muss der Angriff in dem Moment erfolgen, in dem der Ausweis Kontakt mit dem Lesegerät hat, was zugegebenermaßen einen erfolgreichen Identitätsdiebstahl wesentlich erschwert.

Doch wie kommt der Angreifer an die PIN? Das Personalausweisportal versichert, dass selbst das Sicherheitsniveau der Basislesegeräte (günstigste Variante ohne eigene Tastatur für die PIN-Eingabe) sehr hoch sei, da die Übertragung dabei verschlüsselt erfolge. Jedoch solle der Nutzer beachten, dass Schadsoftware unter Umständen Tastatureingaben mitlesen könne. Und in dem Fall nützt auch die Verschlüsselung nichts. Der CCC konnte bereits vor der Einführung des Dokuments demonstrieren, wie einfach es ist, mittels eines einfachen Trojaners, den man ohne tiefgründiges technisches Verständnis aus dem Internet laden kann, die PIN auszulesen und den Ausweis beliebig zu nutzen, solange er auf dem Lesegerät liegt⁹. Die Schwierigkeit liegt dann eher darin, den Trojaner auf einen Rechner des Opfers zu schleusen.

Auch wenn technisch versierte Nutzer in der Lage sind, ihren Rechner vor Schädlingen zu schützen, so muss doch bedacht werden, dass der Personalausweis ein Dokument ist, den alle Bürger haben müssen (zumindest wenn sie keinen Reisepass besitzen), jedoch bei weitem nicht alle in der Lage sind, ihren Rechner zu schützen geschweige denn einen Trojaner zu erkennen. Daher ist zu erwarten, dass viele Rechner mit einem Schädling dieser Art infiziert sind und die Nutzer es gar nicht wissen.

Einen besseren Schutz vor Trojanern bieten nur höherwertigere Lesegeräte, die über eine eigene Tastatur für die PIN-Eingabe verfügen und idealerweise auch über ein eigenes Display, auch Komfortleser genannt. Sie bieten zumindest einen Schutz in dem Fall, dass ein Rechner mit einem Trojaner

⁹ Vgl. [3]

infiziert ist, der Tastatureingaben, den Bildschirminhalt und Mausbewegungen mitlesen kann. Es ist aber nicht ausgeschlossen, dass Trojaner entwickelt werden, die auch die Tastatur des Lesegerätes auslesen können. Während die eher unsicheren Basislesegeräte für 0 (staatlich gefördert) bis maximal 50 € zu haben sind, kosten die sichereren Komfortleser um die 160 €¹⁰. Da das Personalausweis auch die Basisleser als sehr sicher darstellt, werden vermutlich zahlreiche Nutzer nicht in mehr Sicherheit investieren.

Aufgrund des Vorhandenseins von Geräten verschiedener Sicherheits- und der damit auch verbundenen Preisniveaus, sollte darüber nachgedacht werden, ob es akzeptabel ist, dass die Sicherheit der eigenen Identität auch eine Frage des Einkommens sein darf, denn theoretisch hat jeder Bürger die gleichen Rechte und Pflichten. Schließlich ist auch jeder verpflichtet, ein Ausweisdokument zu besitzen. Selbst wenn jemand auf die Nutzung der Online-Funktionen des Ausweises verzichtet, so zahlt er für sie trotzdem mit, weil die Funktionen nur deaktiviert sind.

Risiken der Unterschriftsfunktion

Der wohl schlimmste Fall, der durch die Nutzung der Unterschriftsfunktion eintreten kann, ist dass einem Opfer eine Willenserklärung, ein Vertrag, eine Vollmacht oder Ähnliches untergejubelt wird.

Um digital unterschreiben zu können, wird laut dem Personalausweisportal ein Signaturzertifikat benötigt, welches zusätzlich erworben werden muss und auf dem Chip des Personalausweises gespeichert wird. Zusätzlich wird eine Signatur-PIN, die AusweisApp und ein Komfortlesegerät benötigt¹¹. Immerhin ist die Nutzung eines verhältnismäßig sicheren Lesegerätes hier im Gegensatz zur Ausweisfunktion Pflicht. Daher dürfte es sich für den Angreifer nicht ganz so einfach gestalten lassen, die PIN des Opfers zu stehlen. Borges,

¹⁰ [5]

¹¹ [2]

Schwenk , Stuckenberg, Wegener betonen jedoch, dass die Sicherheit der Signatur auf einem Nutzer-PC bereits in Zweifel gezogen wurde. Mit einem trojanischen Pferd ließen sich qualifizierte Signaturen auch ohne Einwilligung des Nutzers erzeugen¹².

Der Chaos Computer Club weist aber auch auf ein anderes Problem im Zusammenhang mit der Signaturfunktion hin: Es sei durchaus denkbar, dass das zu signierende Dokument in unterschiedlichen Signierungsprogrammen unterschiedlich dargestellt werden. Es sei also möglich, ein Dokument zu signieren, obwohl es gar nicht korrekt dargestellt wird¹³. Das wäre dann so, als würde der Nutzer einen Vertrag unterschreiben, obwohl der Inhalt möglicherweise ein anderer war. Er müsste auch die Haftung übernehmen, weil der Vertrag rechtsgültig ist. Bevor für das letztgenannte Problem eine akzeptable Lösung gefunden wird, ist von der Nutzung der Unterschriftsfunktion also eher abzuraten.

Fazit

Der elektronische Personalausweis bringt Funktionen mit, die den Alltag erleichtern sollen. Allerdings bringt die Nutzung der erweiterten Funktionen, die einen Online-Identitätsnachweis ermöglichen, Risiken mit sich, die zudem davon abhängen, welche Art des Lesegerätes verwendet wird. Sicherere Lesegeräte sind deutlich teurer in der Anschaffung und somit wird der Schutz vor Identitätsdiebstahl zu einer Frage des Einkommens.

Auch die Unterschriftsfunktion hat das versprochene Sicherheitsniveau nicht erreicht. Da zur Zeit nicht einmal gewährleistet ist, dass zu signierende Dokumente von allen Programmen gleich dargestellt werden, besteht das Risiko, dass der Nutzer etwas rechtsbindend unterschreibt, deren Inhalt er nicht kennt.

12 [1], S. 163

13 [2]

Literatur

[1] Georg Borges, Jörg Schwenk , Carl-Friedrich Stuckenberg, Christoph Wegener : „*Identitätsdiebstahl und Identitätsmissbrauch im Internet - Rechtliche und technische Aspekte*“, Springer Verlag Berlin Heidelberg 2011, S. 151-193

Internetquellen:

[2] http://www.personalausweisportal.de/DE/Home/home_node.html

[3] <http://www.ccc.de/de/updates/2010/sicherheitsprobleme-bei-suisseid-und-epa>

[4] § 27 PAuswG: <http://www.buzer.de/gesetz/8806/a161522.htm>, Zugriff am 5.1.2012

[5] <http://www.personalausweis-kartenlesegeraete.de/komfort-kartenleser/>, Zugriff am 5.1.2012