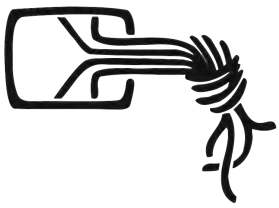
Chaos Computer Club



Stellungnahme eID

Gesetz zur Förderung des elektronischen Identitätsnachweises
(PAuswG-E, Passgesetz)

19. April 2017

Constanze Kurz
Jan Krissler, Linus Neumann, Frank Rieger

Dauerhafte Aktivierung der eID-Funktion

Das Ziel des Gesetzes zur Förderung des elektronischen Identitätsnachweises (eID) spricht bereits aus dem Titel: Die Nutzung der eID-Funktion soll sowohl beim elektronischen Personalausweis (ePA) als auch beim elektronischen Aufenthaltstitel (eAT) flächendeckend ausgebaut werden. Das soll vor allem dadurch erreicht werden, dass die Funktion standardmäßig und dauerhaft eingeschaltet wird, „bürokratische Hürden“ abgebaut und mögliche Anwendungsfelder erweitert werden.

Mit dem vorliegenden Gesetzentwurf wird also eine Förderung der Nutzung der eID-Funktion im Personalausweis versucht. Der elektronische Ausweis enthält einen Chip mit einer drahtlosen Schnittstelle, der drei verschiedene Funktionen anbietet. Eine davon ist der elektronische Identitätsnachweis (eID). Zur Nutzung dieser eID sind prinzipiell zwei Faktoren notwendig: der Besitz der Ausweis-Karte und die Kenntnis eines Geheimnisses (Zwei-Faktor-Authentisierung). Diese Zwei-Faktor-Authentisierung ist für den Nutzer ein technischer Vorteil in Fragen der Sicherheit, aber kein Alleinstellungsmerkmal gegenüber nicht-staatlichen Alternativen zur eID im Ausweis. Mittlerweile setzt eine Vielzahl von Anbietern Verfahren ein, die auf mehreren Authentisierungsfaktoren beruhen.

Verbreitung der eID-Nutzung

Die eID-Funktion hat nach ihrer kostenintensiven Einführung im November 2010 keine nennenswerte Verbreitung gefunden. In der Begründung des Gesetzentwurfes wird dies offenbar der bisherigen Möglichkeit zugeschrieben, diese eID-Funktion gar nicht erst zu aktivieren oder später zu deaktivieren. Kern des Gesetzentwurfes ist daher deren automatische Aktivierung.

Insgesamt liegt die eID-Nutzung deutlich unter den Erwartungen, die Aktivierungsquote hat nicht einmal ein Drittel der Ausweisbesitzer erreicht.

Die Aktivierung ist aber nur eine Seite der Medaille, denn die tatsächliche Nutzung liegt noch weit darunter, da sinnvolle Angebote rar sind. Nur etwa fünfzehn Prozent der Besitzer mit aktivierter eID-Funktion haben den Einsatz überhaupt getestet. Die Zahl der Test-Nutzer darunter, die zudem ein sicheres Lesegerät nutzen, ist statistisch nahe Null.

Die Hoffnung ist, dass die zwangsweise Aktivierung einen Anreiz zur Implementierung von eID-Diensten setzen könnte. Während behördliche Angebote zur Nutzung der eID-Funktion seitens der Bundes- und Landesregierungen stimuliert werden könnten, ergibt sich bei Angeboten aus der Wirtschaft eine Art Henne-Ei-Problematik: Angebote werden nicht gemacht, wenn niemand die eID nutzt; niemand nutzt die eID, wenn es keine guten Angebote gibt.

Doch bisher haben sich selbst staatliche Stellen in den letzten sieben Jahren dem überwältigendem Votum der Bürger gegen die eID angeschlossen: Leuchtturmprojekte, die als potentielle Zugpferde Werbung für die Benutzung machen könnten, sind quasi nicht existent.

Selbst das mit großem Rummel angekündigte besondere elektronische Anwaltspostfach (beA) lässt die eID links liegen, obwohl deren Notarsfunktion quasi ein Heimspiel wäre.

Welche Vorteile die Nutzung der eID-Funktion gegenüber anderen alltäglichen und marktgängigen Identifikationsmethoden haben soll, konnte bisher nicht überzeugend dargestellt werden. Die damit ganz praktisch befassten Mitarbeiter in den Meldeämtern sind weder dafür ausgebildet noch zeitlich in der Lage, Fragen der Ausweisbesitzer nach Vor- und Nachteilen zu beantworten. Der Begründung des neuen Gesetzentwurfes gelingt das auch nicht. Warum bestehende Lösungen bei Online-Diensten durch die vergleichsweise komplexe Nutzung der eID ersetzt werden soll, erschließt sich nicht.

Es drängt sich der Eindruck auf, dass die mit vielen Versprechungen und hohen finanziellen Investitionen an den Start gegangene Digitalisierung des Ausweises von einem Angebot an die Bürger nun per Gesetz zu einem Zwang ausgebaut werden soll, obgleich sich der besondere Nutzen weder aus Sicht des Bürgers noch aus Sicht von Anbietern nicht begründen lässt.

Es ist nicht das erste Mal, dass durch ein derartiges Nachbesserungsgesetz ein teures und aus guten Gründen nie benutztes totes Pferd wiederbelebt werden soll. Die mangelnde Verbreitung und Nutzung der eID-Funktion dürfte vielmehr dem mangelnden Vertrauen und Interesse der Bürger zuzuschreiben sein als der Möglichkeit der Aktivierung und Deaktivierung. Dieses fehlende Vertrauen lässt sich auch durch eine zwangsweise Aktivierung nicht zurückgewinnen. Es stellt sich zudem die einfache Frage: Warum sollte jemand eID nutzen wollen, nur weil sie dann verpflichtend eingeschaltet ist?

Es sollte anerkannt werden, dass sich auch die Online-Welt in den vergangenen sieben Jahren weitergedreht hat. Heute wird das eID-Verfahren den Anforderungen der mobilen Welt kaum gerecht. Identitätsabgleiche verlagern sich mehr und mehr auf Smartphones, wofür auch nach Jahren so gut wie keine Angebote gemacht werden.

Das ausbleibende Interesse betrifft dabei sowohl die Ausweisbesitzer als auch die Anbieter. Offenbar konnten auch potentielle Anbieter von der Sinnhaftigkeit der eID-Funktion gegenüber bestehenden Alternativen nicht überzeugt werden. Von den ausgestellten Berechtigungszertifikaten vom Bundesverwaltungsamt sind derzeit mit 233 Zertifikaten etwa die Hälfte für den behördlichen oder eGovernment-Bereich vergeben worden, die andere Hälfte für kommerzielle Anbieter.

Beantragungsverfahren für Zertifikate

Unternehmen zögern mit der Nutzung der eID-Funktion auch aufgrund des aufwendigen Beantragungsverfahrens, allerdings sichert das bisherige Vorgehen auch gegen Missbrauch. Das betrifft vor allem Haftungsfragen sowie die Vorlage von Sicherheitskonzepten.

Die Notwendigkeitsprüfung vor der Erstellung eines Berechtigungszertifikats soll künftig entfallen, ebenso der Dienstbezug und die Bußgeldhöhe bei Verstößen. Damit soll die Bürokratie vor Erteilung eines Berechtigungszertifikats abgebaut werden. Die Befürchtung ist dabei, dass diese bürokratischen Pflichten die eID-Nutzung behindern. Allerdings war die Prüfung auch ein wichtiges Versprechen an den Bürger im Sinne seiner Datenschutzinteressen, das vor Missbrauch schützen sollte. Obwohl gar nicht belegt ist, dass die Prüfung tatsächlich ausschlaggebend oder gar ursächlich für die klägliche Anzahl an Berechtigungszertifikaten ist, soll nun darauf verzichtet werden. Um Anbietern eine zweifelhafte Incentivierung für eID-Anwendungen anzubieten, wird letztlich beim präventiven Datenschutz zurückgesteckt.

Dass durch den Wegfall der Notwendigkeitsprüfung das mangelnde Vertrauen in die eID seitens der Nutzer gestärkt wird, ist nicht zu erwarten. Wenn das Gegenüber im Netz bei der Beantragung des Zertifikats kaum mehr geprüft wird, fiele ein Vertrauensaspekt der eID weg. Bisher kann jeder bei Interesse die notwendigen Daten sichten und sich auf die Prüfung verlassen, die bei Erstellung der Berechtigungszertifikate erfolgte.[1] Mindestens das Bußgeld bei Verstoß sollte wesentlich erhöht werden, um Missbrauch entgegenzuwirken.

[1] Vgl. Erteilte Berechtigungszertifikate: http://download.gsb.bund.de/VfB/npavfb.pdf

Inflationärer Einsatz der eID führt zu Überidentifizierung

Die Vermischung von hoheitlichen Identifizierungsaufgaben mit den Erfordernissen der Wirtschaft zur Identifizierung im Rechtsverkehr ist konzeptionell problematisch. Es steht zu erwarten, dass die einfache Verfügbarkeit eines Identitätsdienstes auf Basis des Personalausweises zu einer Überidentifizierung führt: Die einfache Identifizierung könnte dann für immer mehr Services und Angebote verlangt werden, was wiederum die Verknüpfung mit anderweitig gewonnenen Profilinformationen zu einem eindeutig zuzuordnenden Persönlichkeitsprofil ermöglicht. An separaten Stellen von verschiedenen Anbietern gesammelte Daten würden so sehr viel einfacher kombinier- und abgleichbar.

Bisher ist der Großteil der bei Anbietern gesammelten Profilinformationen nicht eindeutig mit einer hoheitlich garantierten Identität verknüpft. Durch eine einfache staatlich verifizierte und vertrauenswürdige Personalisierung dieser Profilinformationen entstünden daher umfängliche Probleme in Fragen des Datenschutzes und der Privatsphäre. Während derzeit etwa zu einem alltäglichen Social-Media-Profil fast nie Adressinformationen gespeichert werden, könnte dies mit einem niederschwelligen quasi-hoheitlichen Identitätsservice zum Standard werden. Dies wäre beispielsweise für Stalking-Opfer im Netz gefährlich.

Eine Lösungsmöglichkeit hierfür wäre eine rechtliche und preisliche Gestaltung, die die Nutzung der Personalausweis-basierten Identität nur möglich und attraktiv macht, wenn für Zwecke eines Vertragsabschlusses eine solche Identifizierung wirklich benötigt wird. Das widerspräche aber gerade dem Ziel des Gesetzentwurfes, der die Nutzung der eID explizit fördern will und die Beantragung der Zertifikate zu erleichtern.

Alternativen: größere Einsatzmöglichkeiten und geringere Einstiegshürden

Es bestehen bereits Alternativen zur Identifikation, die vom privaten Sektor angeboten werden bzw. kurz vor ihrer Einführung stehen. Ein Beispiel ist das von der weltweiten Mobilfunk-Vereinigung GSMA spezifizierte „Mobile Identity“-System. Dieses verwendet die bei den Netzanbietern vorhandenen Kundenbeziehungen über das Mobiltelefon des Nutzers zur Identifikation in verschiedenen Sicherheitsstufen. Dieses Verfahren ermöglicht insbesondere das selektive Preisgeben von Identitätsinformationen, um Datensparsamkeit sicherzustellen. Theoretisch denkbar ist dabei auch die pseudonyme Nutzung, bei der einem Anbieter gegenüber nur versichert wird, dass es sich um eine dem Mobilfunkanbieter bekannte Identität handelt, bei der dieser einzugsermächtigt ist.

Dieses alternative Verfahren hat dank globaler Standardisierung und der länderübergreifenden Struktur der großen Mobilfunkanbieter (Vodafone, Telefonica, Telekom etc.) eine hohe Chance auf umfassende Akzeptanz und Marktdurchdringung. Als Vertrauensanker dient dabei die SIM-Karte, welche über weitgehend vergleichbare Sicherheitsattribute wie für eID verwendeten SmartCards verfügt. Es offeriert den Anbieter vor allem eine internationale Lösung, die von nationalen Eigenheiten wie bei der deutschen eID frei ist.

Es ist davon auszugehen, dass solche in ihrer Konzeption nicht national begrenzten Ansätze eine schnellere und größere Akzeptanz finden. Grund dafür ist auch, dass die Anbieter weniger Kosten erwartet, wenn sie eine internationale Lösung statt einer nationalen umsetzen.

Zugriff auf biometrische Lichtbilder

Der Gesetzentwurf enthält auch mit der Förderung der eID nicht in Zusammenhang stehende Inhalte, die den Zugriff auf biometrische Passbilder betreffen. Die digitalisierten biometrischen Pass- und Ausweisbilder stehen der Polizei zum automatisierten Abruf zur Verfügung. Der nun vorgesehene automatisierte Zugriff von Geheimdiensten auf die biometrischen Passbilder in elektronischer Form wäre ein Schritt in eine umfassende und kaum kontrollierte Überwachung. Der Gesetzentwurf sieht diese Möglichkeit der automatisierten Übermittlung der biometrischen Passbilder vor, also einen unmittelbaren geheimdienstlichen Zugriff auf die Daten in den Meldeämtern. Die Protokollierung dieser Zugriffe soll aber nur bei der abfragenden Stelle, also den Geheimdiensten selbst, erfolgen.

Dieser Datenzugriff weitet die Nutzung in einem kaum überschaubaren und wenig kontrolliertem Maße aus und sollte unterbleiben, mindestens aber sollte jede dauerhafte Speicherung und Weitergabe der so erlangten Daten untersagt werden.

Die Möglichkeit des automatisierten Zugriffs sowohl für Polizeien als auch für Geheimdienste muss im Kontext des immer weiteren Ausbaus der Videoüberwachung und der laufenden Tests der Behörden mit automatischer Gesichtserkennung in Videoüberwachungs-Streams gesehen werden. Die einfache elektronische Abfrage großer Mengen Gesichtsbilder erlaubt den Aufbau von Überwachungssystemen, bei denen die Eingabe eines Namens und eines Geburtsdatums in die entsprechende Abfragemaske ausreicht, um das persönliche Passbild abzurufen und direkt in automatischen Gesichtserkennungssysteme einzuspeisen. Auch die umgekehrte Abfrage persönlicher Daten zu einem automatisch identifizierten Gesichtsbild wird für die abgerufenen und bei Polizei oder Geheimdienst gespeicherten Gesichtsbildern dadurch technisch ermöglicht. Die schon heute gegebene Vollüberwachung der digitalen Welt erhält so mittelfristig Einzug in die „reale Welt“ und macht auch diese zu einer digital überwachten Sphäre.

Da die Videoüberwachung des öffentlichen Raums immer weiter ausgebaut wird und die Erprobung automatischer Gesichtserkennung bereits erklärtes Ziel der Behörden ist, muss dieses Szenario für die Bewertung des Gesetzentwurfes bedacht werden.

Ein weiteres Problem ist der weitgehend unkontrollierte Datenaustausch der Geheimdienste mit ausländischen Partnerdiensten. Die jüngsten Aktivitäten türkischer Geheimdienste in Deutschland im Kontext des Präsidial-Referendums offenbarten, dass auch als „befreundet“ klassifizierte Dienste alle Mittel nutzen, um politische Ziele zu verfolgen und Opposition gegen ihre Regierung auch in Deutschland zu unterdrücken. Über den Weg der deutschen Geheimdienste ist hier also von einem Zugriff solcher Partnerdienste auf die gespeicherten deutschen Meldedaten zu warnen, die elektronischen Aufenthaltstitel eingeschlossen. Mit der kontinuierlich zunehmenden Intensität und Automatisierung des Datenaustauschs unter Behörden in Europa und darüber hinaus ist davon auszugehen, dass auch die Gewährung des Zugangs für ausländische Geheimdienste und Polizeien innerhalb weniger Jahre Realität wird.

Dass der Zugriff erst ab dem Jahr 2021 vorgesehen ist, ändert nichts daran, dass ein Einfließen der Meldedaten in die geheimdienstlichen Kreisläufe eine Zweckentfremdung der Daten darstellt.

Vertrauen in das eID-Verfahren

Bei der Betrachtung des Erfüllungsaufwands durch den Normenkontrollrat werden Einsparpotentiale unter anderem dadurch gesehen, dass erstens die Bürger nicht mehr über eine Möglichkeit der Deaktivierung aufgeklärt werden müssen, zweitens die Deaktivierung grundsätzlich nicht mehr angeboten wird und damit auch drittens die Reaktivierung wegfällt. Aus diesem Grund soll auch auf fünfzig Prozent der Informationsmaterialien verzichtet werden. Die erhofften Kosteneinsparungen sind allerdings praxisfern.

Laut dem vorliegenden Gesetzentwurf soll es der ausstellenden Behörde überlassen bleiben, „in welcher praxisgerechten Form“ eine Unterrichtung der Bürger über die eID-Funktion stattfindet. Dies lässt entweder den Schluss zu, dass die durch diesen Zeitaufwand entstehenden Kosten bei der Betrachtung nicht berücksichtigt werden, oder dass ein Verzicht auf diese Unterrichtung billigend in Kauf genommen wird.

Es zeugt vom Geist dieses Gesetzes, dass den Bürgern in Zukunft eine Funktionalität aufgezwungen wird, gegen die sich bisher mehr als zwei Drittel der Bürger entschieden haben, nachdem sie darüber informiert wurden. Diese Bürger sollen nun nicht nur zur Nutzung zwangsweise animiert, sondern über die Funktion auch nicht mehr vollständig und einheitlich aufgeklärt werden. Es bleibt schleierhaft, wie das Vertrauen in eine Funktion dadurch gesteigert werden soll, geschweige denn in deren Anwendung.

Es ist eine langjährige Forderung des Chaos Computer Clubs, die Informationen für den Ausweisnutzer verständlicher, umfassender und risikobezogener zur Verfügung zu stellen. Statt bunter Broschüren sollte eine ehrliche und auch die Risiken betrachtende Information mit dazu geschulten Mitarbeitern erfolgen. Das Gegenteil sieht der Gesetzentwurf vor, obgleich die eID und auch der elektronische Personalausweis insgesamt ein anspruchsvolles und technisch komplexes Angebot ist.

Nach wie vor sollte der Bürger darauf hingewiesen werden, dass der elektronische Personalausweis nicht länger als notwendig in ein Lesegerät gesteckt werden sollte, um etwa Relay-Angriffe zu vermeiden. Handfeste Informationen über die Unterschiede in Fragen der IT-Sicherheit, die zwischen den angebotenen Lesegeräten („Basisleser“, „Komfortleser“ usw.) bestehen, sollten ebenso an den Bürger gegeben werden. Dazu sind bei Interesse weitergehende Behördeninformationen zu Lesegeräten und Software sowie zur IT-Sicherheit im Alltag, insbesondere zu Schadsoftware auf den heimischen Rechnern der Nutzer, anzubieten.

Dass noch keine speziell auf den Missbrauch der eID zugeschnittenen Trojaner im Umlauf sind, dürfte an der spärlichen Verbreitung liegen. Wenn sich die Erfahrungen der Missbrauchsmöglichkeiten nur ähnlich langsam durchsetzen, wie in der Vergangenheit bei Online-Banking oder den PINs der EC-Karten, wären gerade unter den frühzeitigen Anwendern die von Identitätsdiebstahl Betroffenen – auch in Hinsicht auf das deutlich höhere Schadpotential – einem mühsamen Kampf zum Nachweis des Missbrauchs ausgesetzt. Ein weiteres Beschneiden der Aufklärungsarbeit in den Meldeämtern würde diese Schieflage noch verschlimmern.

Ausweis- und Passkopien

Bisher ist das Erstellen einer Ausweiskopie an die Erforderlichkeit gebunden. Wenn der Ausweis vor Ort vorgezeigt und geprüft werden kann, liegt diese Erforderlichkeit nicht vor. Das automatisierte Speichern von Personalausweiskopien durch nicht-öffentliche Stellen ist bisher nach dem Personalausweisgesetz nicht möglich.

Der Gesetzentwurf soll die Erstellung von Kopien des elektronischen Personalausweises nun erlauben. Kopien sollen auch für den elektronischen Pass möglich werden. Damit wird zugleich die Kopie der aufgedruckten maschinenlesbaren Zone (MRZ) zum Problem, da der Zugang zu den Daten auf dem Chip damit verbunden ist.

Diese Kopien sollen künftig dann hergestellt werden dürfen, wenn der Ausweisbesitzer darin freiwillig einwilligt. Die Kopien sollen aber nicht an Dritte weitergegeben werden dürfen. Die Freiwilligkeit ist aber regelmäßig in der Praxis keine echte, wenn etwa ein Dienstleister schlicht danach verlangt und den Besitzer zu einer Ausweiskopie drängt, um eine Dienstleistung oder einen Vertragsabschluss durchzuführen. Die Vermietung von Wohnraum, Fahrzeugvermietungen oder Hotelübernachtungen sind typische Beispiele dafür.

Ob und wie lange eine Kopie gespeichert wird, entzieht sich im Regelfall der Kenntnis des Ausweisbesitzers, auch eine Weitergabe kann er praktisch kaum erfahren noch verhindern.

Zudem gibt die Kopie regelmäßig mehr Daten preis als für den Vertrag oder die Dienstleistung nötig wäre, inklusive der MRZ. Zwar wird empfohlen, nicht erforderliche Daten zu schwärzen. Dass aber in der Praxis tatsächlich Bereiche wie die maschinenlesbare Zone aus Sicherheitsgründen physisch abgeklebt werden, ist lebensfremd und schlicht unpraktisch.

Generell wird statt der heute üblichen Vorlage und Einsichtnahme die Ausweiskopie durch die neue Regelung wieder häufiger werden und damit – anders als bei den aus dem Chip freigegebenen eID-Datenfeldern – die aufgedruckten Informationen vollständig preisgeben. Das sind auf der Vorderseite typischerweise neben Lichtbild, Name und Vorname: das Geburtsdatum und der Geburtsort, die Seriennummer des Ausweises, das Gültigkeitsdatum, die Staatsangehörigkeit sowie die Zugangsnummer (für den hoheitlichen Bereich des Chips). Wird auch die Rückseite kopiert, sind zusätzlich die Anschrift, die Körpergröße, die Augenfarbe, eventuelle Künstler- und Ordensnamen, die ausstellende Behörde sowie die MRZ aufgedruckt.

Erforderlich sind hingegen bei typischen Identitätsnachweisen nur Vorname, Nachname, Anschrift und häufiger auch das Geburtsdatum. Da beim Ausweis jedoch Name und Anschrift auf unterschiedlichen Seiten aufgedruckt sind, besteht eine Ausweiskopie regelmäßig aus beiden Seiten und damit aus den vollständigen aufgedruckten Informationen. Als besonders sensibel kann dabei die MRZ und die Zugangsnummer gelten. Der Gesetzgeber sollte daher das Abkleben vorschreiben. Da das im Alltag nicht besonders praktisch ist, wird das zugleich nicht unbedingt notwendigen Ausweiskopien entgegenwirken.

Fazit

Nachdem das Desinteresse von Bürgern und Anbietern an der eID nun seit Jahren besteht und auch keine Art der Selbstverpflichtung der Industrie erreicht werden konnte, soll die Nutzung der eID jetzt mit dem gesetzlichen Holzhammer verordnet werden. Statt mit attraktiven behördlichen Angeboten aufzuwarten, die Vertrauen und Nutzungszufriedenheit fördern könnten, wird eine Methode gewählt, die mit hoher Wahrscheinlichkeit erneut scheitern wird.

Die vorgesehene Erlaubnis für Kopien von Ausweis und Pass birgt Gefahren für den Datenschutz und die IT-Sicherheit, insbesondere durch die Kopie der MRZ.

Bei der Nutzung des elektronischen Personalausweises sollte auf Sicherheitsprobleme hingewiesen werden anstatt die Aufklärung in den Meldeämter weiter zu reduzieren. Die Benutzung des elektronischen Identitätsnachweises ist technisch komplex, auf Risiken sollten die Bürger aufmerksam gemacht werden, insbesondere wenn sie keine der teureren Lesegeräte benutzen.

Der automatisierte Zugriff auf die biometrischen Lichtbilder aus den elektronischen Personalausweisen und Pässen für die Geheimdienste ist kaum kontrollierbar und daher abzulehnen.