

Neuer Personalausweis

Potenziale ungenutzt?

[28.10.2011] Hat sich der neue Personalausweis (nPA) beinahe ein Jahr nach seiner Einführung zum Katalysator für E-Government-Projekte entwickelt und welche Aufgaben stellen sich den Kommunen künftig?

Er ist kleiner, handlicher und macht das Leben leichter. So überschrieb die Bundesregierung auf ihrem Web-Portal im Februar 2009 die Meldung zur Billigung des Gesetzentwurfes zum neuen Personalausweis (nPA) durch den Bundesrat. An einem Freitag. Einem dreizehnten. Ein schlechtes Omen?

Ein Jahr nach der Einführung des neuen Personalausweises stellt sich – mit Fokus auf die Kommunen – die Frage, inwieweit sich die überall geäußerte Hoffnung bestätigt findet, der nPA könne zum Katalysator für neue E-Government-Projekte werden. Unterstellt man, jenseits von Informationsbeschaffung, Terminvereinbarung oder Formular-Download über kommunale Portale, eine Win-win-Situation als Kernkriterium für E-Government-Vorhaben, dann wurde mit der Einführung des neuen Ausweises eine zentrale Voraussetzung für die Umsetzung eines nachhaltigen und nutzenorientierten E-Government geschaffen. Stichworte sind hier Aufwand- und Zeitersparnis für den Bürger, Daten- und Informationssicherheit sowie die 24/7/365-Verfügbarkeit von Verwaltungsdienstleistungen. Auf der anderen Seite stehen Bürgerfreundlichkeit, Bürokratieabbau, medienbruchfreie Kommunikation zwischen Online- und Fachanwendung mit hoch validen Daten, Optimierung von Verwaltungsprozessen sowie Kostensenkung.

Potenziale des neuen Personalausweises

Diese Potenziale haben sich bereits im Vorfeld der Einführung des neuen Personalausweises im Anwendungstest des Bundesinnenministeriums gezeigt. Eine zügige und breite Umsetzung von elektronischen Bürgerservices mit der eID-Funktion oder die Implementierung in bereits bestehende Systeme war durchaus zu erwarten. Entsprechende Software-Lösungen sind bereits bis zur Marktreife entwickelt. Bei aller strukturellen, mithin nachvollziehbaren Trägheit im Bereich öffentlicher Verwaltungen, sieht die Realität allerdings anders aus. Dafür lassen sich zwei wesentliche Ursachen identifizieren: Zum einen die hohen Kosten und zum anderen die daraus resultierenden kommunalen Geschäftsmodelle.

Die Kosten für eine von der Vergabestelle für Berechtigungszertifikate erteilte Genehmigung zum Auslesen der für einen Online-Service benötigten personen- und/oder ausweisbezogenen Daten, sind mit etwas mehr als 100 Euro vergleichsweise gering. Anders sieht es bei den Kosten für die Ausstellung eines Berechtigungszertifikates durch ein Trustcenter und den Kosten für den eID-Service aus. Derzeit kostet das Berechtigungszertifikat für eine Laufzeit von drei Jahren rund 6.000 Euro. Der eID-Service zur Verwaltung eines Berechtigungszertifikats kostet zusätzlich noch einmal etwa 2.500 Euro im Jahr.

Die organisatorische Implementierung von Online-Verwaltungsdienstleistungen mit dem nPA, für die nur ein Berechtigungszertifikat benötigt wird (zum Beispiel An- und Abmeldung der Hundesteuer), dürfte im Jahr also etwa 4.500 Euro kosten. Für Online-Services aus anderen Verwaltungsbereichen sind weitere Berechtigungszertifikate notwendig. Damit erhöhen sich die Kosten entsprechend. Insbesondere für kleine und mittlere Kommunen ist das mit Blick auf die dünne Finanzdecke ein erheblicher finanzieller Aufwand. Darüber hinaus lassen sich die Einsparpotenziale durch E-Services im kommunalen Haushalt kaum darstellen.

Der derzeit präferierte Weg, den finanziellen und bürokratischen Aufwand zu minimieren, wird im so genannten Bürgerkonto oder ID-Safe gesehen. In diesem Fall kann sich der Bürger auf dem (kommunalen) Online-Portal registrieren und dort im Sinne eines digitalen Identitätsmanagements alle personen- und ausweisbezogenen Daten hinterlegen. Die Kommune kann dann für alle Verwaltungsdienstleistungen, die der Bürger künftig in Anspruch nehmen möchte, auf die Daten aus dem ID-Safe zurückgreifen – mit nochmaliger Zustimmung des Bürgers. Die Vorteile scheinen zunächst überzeugend: Für ein Bürgerkonto ist nur ein Berechtigungszertifikat erforderlich. Das spart Geld und organisatorischen Aufwand. Die Datenhaltung kann zentral vor Ort erfolgen oder sogar über Landesportale oder auf Gemeinde- und Zweckverbandsebene. Der Bürger ist Herr seiner Daten. Bei genauerer Betrachtung konterkariert dieses Einsatzszenario allerdings die Nutzenpotenziale des neuen Personalausweises als ID-Karte mit Blick zum einen auf den Datenschutz und die Datensicherheit und zum anderen auf unsere Alltagserfahrungen.

Zunächst stellt sich die grundsätzliche Frage nach der Aktualität und Integrität der Daten im ID-Safe. Nach der Erstregistrierung meldet sich der Bürger mit einem Pseudonym an. Ist er mittlerweile umgezogen, wurde die Anschrift zwar im Melderegister und auf dem Ausweis-Chip geändert, nicht aber in seinem Bürgerkonto, denn die personenbezogenen Daten im ID-Safe werden nach der Erstregistrierung nicht erneut überprüft. Hinzu kommt, dass das karten- und dienstespezifische Kennzeichen ausweisbezogen ist. Das heißt, ein neuer Ausweis hat ein neues Pseudonym. Die Anmeldung am Bürgerkonto schlägt fehl, eine Neuregistrierung ist damit unumgänglich. Darüber hinaus bergen die zentrale Datenhaltung der Bürgerkonten zusätzliche Risiken und müssen durch geeignete Maßnahmen vor unberechtigtem Zugriff geschützt werden. Und haben wir es nicht alle satt, uns überall im Internet zu registrieren? Mit dem nPA ist das nicht mehr nötig. Bei durchschnittlich einem Behördenkontakt im Jahr stellen sich vermutlich viele die Frage, warum sie ein permanentes Bürgerkonto benötigen, nur um online die Fernleihe der Gemeindebibliothek nutzen zu können.

Fazit

Eine sinnvolle Lösung des Problems könnte kostenseitig darin bestehen, mit dem nPA zu nutzende kommunale E-Services durch Bund und Länder zu fördern. Die Nutzenpotenziale des nPA werden erst dann ausgeschöpft, wenn eine Vielzahl von Verwaltungsdienstleistungen online angeboten wird. Hier gilt es zwingend, die Aufklärungs- und Informationsarbeit zu intensivieren. Dieser Aufgabe sollten sich Kommunen, Länder und Bund gemeinsam stellen.

()

Stichwörter: Digitale Identität,