ZUSAMMENFASSENDE EMPFEHLUNGEN

Ein möglichst einfacher Zugang zu Verwaltungsleistungen gilt als kritischer Erfolgsfaktor für das E-Government in Deutschland. Identifikation und Authentifikation der Nutzer bilden dabei einen neuralgischen Punkt. Fehler an dieser Stelle eröffnen Missbrauchspotenziale, die teilweise zu erheblichen Schäden führen können. Sind die Verfahren aber zu komplex, wird das Angebot von den Nutzern nicht angenommen. Die Online-Ausweisfunktion des Personalausweises steht sinnbildlich für dieses Spannungsfeld. Sie ist für das höchste Vertrauensniveau geeignet und gesetzlich der Schriftform gleichgesetzt. In der Anwendung stellt sie jedoch hohe Anforderungen an Nutzer und Dienstanbieter, sodass die Nutzungszahlen hinter den Erwartungen zurück bleiben.

Es ist davon auszugehen, dass zahlreiche Verwaltungsleistungen auch mit den geringeren Vertrauensniveaus „normal“ oder „substanziell“ realisiert werden können.[1] Hierfür herrscht allerdings Unsicherheit über die Einsatzmöglichkeiten von niedrigschwelligen Identifikationslösungen, die verwaltungsseitig akzeptiert werden und – für den jeweiligen Einsatzzweck – auch hinreichend rechtssicher sind. Dabei ist der angemessene Ausgleich zwischen Benutzbarkeit und Sicherheit das Eine, das Andere, und vermutlich mindestens ebenso wichtig ist die Frage, ob und wie eine womöglich staatliche Stelle das Risiko für den Bereich übernimmt, der eben nicht technisch abgesichert werden kann oder soll („Restrisiko“) – und nicht die Bürgerinnen und Bürger.

Ein Blick auf erfolgreiche Identifikationslösungen zeigt, dass Identifizierung und Authentifizierung einfach, verständlich und dem Anwendungsfall angemessen sein müssen. Andere Länder wie Estland, Österreich oder Dänemark zeigen, wie man mit leichtgewichtigen und mobilfähigen Identifizierungslösungen E-Government-Angebote wesentlich bürgernäher gestalten kann.

Parallel zu den staatlich entwickelten Lösungen entstehen eine Reihe von Identifizierungslösungen in der Wirtschaft. Eingesetzt werden offene Standards genauso, wie proprietäre Lösungen. Ziel, neben einem Single Sign-on, ist zumeist, bisherige, als unsicher einzustufende Nutzername-Passwort-Authentifizierungs-Verfahren abzulösen. Dabei setzt sich vermehrt die 2-Faktor-Authentifizierung als Mittel durch.

Vor dem Hintergrund der Europäischen Datenschutzgrundverordnung müssen Unternehmen, die mit Kundendaten agieren, zukünftig europaweit einheitliche Regeln für den Umgang mit personenbezogenen Daten einhalten. In Deutschland haben sich inzwischen mehrere Industriekonsortien gebildet, die sich jeweils mit einem eigenen Identitätsmanagementdienst etablieren wollen. Dahinter stehen große namhafte Konzerne mit teilweise großem Kundenstamm.

Diese Entwicklung zeigt, dass die öffentliche Verwaltung auf viele existierende Lösungen und einem breiten Erfahrungsschatz aufbauen kann. Um digitale Verwaltungsangebote attraktiver zu gestalten, wird in diesem Papier empfohlen, leichtgewichtige Ergänzungen zur Online-Ausweisfunktion für die Verwaltung nutzbar zu machen, das heißt konkret:

1 Vgl. ausführlich Abschnitt 3.1.

- **Vertrauensniveaus nutzerorientiert und realistisch festlegen**

  Wir empfehlen grundsätzlich, zunächst die Onlinedienste und damit verbundenen Prozesse aus Nutzersicht zu definieren, dann die Datenströme zu betrachten, den Schutzbedarf festzulegen und erst dann das Vertrauensniveau sowie das „passende" Identifikationsverfahren zu bestimmen.

- **Leichte Zugänglichkeit als oberstes Gebot leben**

  Besonders für Gelegenheitsnutzer ist ein einfacher Zugang zu Verwaltungsleistungen von hoher Bedeutung, wobei möglichst eine Variante zum Einsatz kommen sollte, die den Bürgerinnen und Bürgern aus anderen Lebensbereichen vertraut ist. Für Onlinedienste, die das Vertrauensniveau „substanziell" erhalten, sollte geprüft werden, ob und wie Servicekonten bspw. das ELSTER-Zertifikat zur Identifikation nutzen können.

- **Zusammenarbeit mit privaten Initiativen prüfen**

  Derzeit entstehen viele privatwirtschaftliche Initiativen im Bereich der Identifizierung und Authentifizierung. Noch ist offen, wie erfolgreich die teilweise noch jungen privatwirtschaftlichen Initiativen sind. Sollte die Nutzung schnell Verbreitung finden, bieten sich hier ggf. weitere Möglichkeiten, um Onlinedienste der Verwaltung leicht zugänglich und damit attraktiv zu gestalten.

- **Registervernetzung vorantreiben**

  Der Zugang zu und die Nutzung von Onlinediensten der Verwaltung könnte erheblich erleichtert werden, wenn das Prinzip des Once Only[2] konsequent umgesetzt wird. Hierzu bedarf es einer stärkeren Vernetzung der Register und damit verbunden geeigneter Mechanismen, um registerübergreifend die Daten einer Person zu identifizieren. Hier bestehen in Deutschland vor dem Hintergrund des Grundrechts auf informationelle Selbstbestimmung hohe Hürden. Der Blick auf andere Länder, etwa Österreich, zeigt jedoch, dass es Lösungsansätze gibt, die diesen Anforderungen gerecht werden können. Diese Lösungsansätze sollten weiter verfolgt und an die deutschen Bedingungen angepasst werden.

Schlagworte: Identitätsmanagement, Online-Ausweisfunktion (eID), Personalausweis, Servicekonto, Identifizierung, Authentifizierung

2 Once Only bedeutet, „dass Daten und Dokumente der Bürger und Unternehmen […] nur genau einmal – once only – in der Verwaltung produziert oder dort erfasst und bei Bedarf von anderen Behörden wiederverwendet, soweit dem keine Datenschutzinteressen der Betroffenen entgegenstehen." Siehe Gabriele Goldacker et al. 2019, No-Government, In: Jens Fromm und Mike Weber (Hrsg.), 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/-/no-government.