Freie Universität Berlin

Fachbereich Mathematik und Informatik
ID-Management

Prof. Dr. Marian Margraf
Takustraße 9
14195 Berlin

+49 30 838 75-245
marian.margraf@fu-berlin.de

Innenausschuss des
Deutschen Bundestages

nur per E-Mail

Betr.: Öffentliche Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises"

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung zum Gesetzentwurf. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form. Dabei beziehe ich mich ausdrücklich nur auf die im vorliegenden Gesetzentwurf aufgeführten Änderungen des aktuellen Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) vom 18.06.2009 mit dem Ziel, den elektronischen Identitätsnachweis (auch eID-Funktion genannt) zu fördern. Darüber hinaus bewerte ich die im Gesetzentwurf vorgeschlagenen Änderungen hinsichtlich ihrer sicherheitstechnischen Folgen. Dies betrifft die folgenden Änderungsvorschläge:

1) Automatische und dauerhafte Einschaltung der eID-Funktion, Neufassung §10.
2) Löschung der Abwahlmöglichkeit einzelner im Rahmen der eID-Funktion übermittelbaren Daten, Neufassung §18.
3) Nutzung der eID-Funktion ohne Eingabe der PIN für Vor-Ort-Diensteanbieter, neuer §18a.
4) Nutzung der eID-Funktion über einen Identifizierungsdiensteanbieter, neuer §19a.
5) Vereinfachung der Vergabe von Berechtigungszertifikaten, Neufassung §21.

zu 1) Aus sicherheitstechnischer Sicht ergibt sich in Bezug auf eine automatische und dauerhafte Einschaltung der eID-Funktion keine Gefährdung. Nutzerinnen und Nutzer können weiterhin verhindern, dass die eID-Funktion ihres Ausweisdokuments missbraucht wird, indem sie z.B. diese Funktion über die Sperrhotline sperren lassen. Selbst wenn diese Maßnahme nicht durchgeführt wird, die eID-Funktion also nicht gesperrt ist, können Angreifer die eID-Funktion nur missbrauchen, wenn sie im Besitz

von Ausweisdokument und der für die Nutzung der eID-Funktion notwendigen PIN sind (2-Faktor-Authentisierung). Eine weitere Maßnahme, die Nutzerinnen und Nutzer umsetzen können, besteht also darin, den PIN-Brief sicher zu verwahren oder die hiermit übermittelte PIN unkenntlich zumachen.

zu 2) Das derzeit aktuelle PAuswG sieht vor, dass Nutzerinnen und Nutzer einzelne Datenfelder für die Übermittlung ausschließen können. Diensteanbieter müssen eine Berechtigung bei der Vergabestelle für Berechtigungszertifikate (VfB) beantragen. Diese prüft insbesondere, abhängig vom Zweck der Datenübermittlung, auf welche Datenkategorien der Diensteanbieter zugreifen darf. Ein Abwählen einzelner Datenkategorien wird also im Allgemeinen dazu führen, dass der Dienst nicht erbracht werden kann. Vor diesem Hintergrund ergibt ein Abwählen einzelner Datenkategorien keinen Sinn.

Dies ändert sich aber, wenn, wie in der Neuregelung in §21 vorgesehen (siehe auch Punkt 5) zukünftig Berechtigungen nicht mehr zweck-, sondern organisationsgebunden vergeben werden. Damit erhält ein Dienstanbieter eine Berechtigung für unterschiedliche Geschäftsprozesse, die aber auch, abhängig vom Zweck, unterschiedliche Anforderungen hinsichtlich der hierfür benötigten Datenkategorien haben können. Technisch ist es möglich, dass sich der Diensteanbieter in solchen Fällen nicht alle laut Berechtigung erlaubten Datenkategorien aus dem Ausweis übermitteln lässt, sondern nur die für diesen Geschäftsprozess benötigten. Meines Wissens ist dies auch in der heutigen Infrastruktur technisch so umgesetzt.

Da Diensteanbieter, unabhängig von den Regelungen im Personalausweisgesetz an das geltende Datenschutzrecht gebunden sind (z.B. Erforderlichkeitsgrundsatz und Gebot der Datensparsamkeit), müssen sie die oben aufgeführte technische Lösung umsetzen, um diesen gesetzlichen Verpflichtungen nachzukommen. Die zuständigen Datenschutz-aufsichtsbehörden sollten dies zukünftig stichprobenartig prüfen.

zu 3) Mit diesem Änderungsvorschlag werden weitere Anwendungsfälle für die eID-Funktion ermöglicht. Für Vor-Ort-Diensteanbieter wird ein spezielles Berechtigungszertifikat benötigt, das den Zugriff auf die Datenkategorien der eID-Funktion ohne Eingabe einer geheimen PIN ermöglicht. Der Zugriff setzt auf Seiten der Vor-Ort-Diensteanbieter die Kenntnis der auf dem Ausweis aufgedruckten Zugangsnummer voraus. Weiter muss der Vor-Ort-Diensteanbieter die Ausweisinhaberin bzw. den Ausweisinhaber eindeutig über das auf dem Ausweis aufgedruckte Lichtbild identifizieren.

All diese Maßnahmen führen dazu, dass ein Missbrauch der eID-Funktion in diesem Einsatzszenario verhindert wird. Nutzerinnen und Nutzer müssen bewusst ihren Ausweis einem Vertreter des Vor-Ort-Diensteanbieters übergeben, damit dieser die nach Berechtigung erlaubten Datenkategorien aus dem Ausweis auslesen kann.

zu 4) Identifizierungsdiensteanbieter sollten in der aktuellen Fassung des Gesetzes verhindert werden. Dazu heißt es in §21 Absatz 2: „Die Berechtigung nach Absatz 1 ist zu erteilen, wenn der Zweck nicht in der geschäftsmäßigen Übermittlung der Daten besteht und keine Anhaltspunkte für die geschäftsmäßige oder unberechtigte Übermittlung der Daten vorliegen". Dies hat aber dazu geführt, dass gerade kleine Diensteanbieter die eID-Funktion nicht einsetzen und weiterhin auf das potentiell unsichere Authentisierungsverfahren Benutzername/Passwort zurückgreifen.

Da Identifizierungsdiensteanbieter in der Regel die Identifizierung von Nutzerinnen und Nutzern für viele Diensteanbieter übernehmen können, kann das Verhalten der Nutzerinnen und Nutzer von diesen nachverfolgt werden. Die besonderen Anforderungen an Identifizierungsdiensteanbieter hinsichtlich Datenschutz und Datensicherheit trägt das Gesetz aber Rechnung. So heißt es in §19a Absatz 2: „Der Identifizierungsdiensteanbieter hat die personenbezogenen Daten des Ausweisinhabers zu löschen...". Weiter muss er nach §21b Absatz 2 Nummer 2 weitere Anforderungen hinsichtlich Datenschutz und Datensicherheit umsetzen, die in einer Rechtsverordnung geregelt werden. Eine aktualisierte VO, die Identifizierungsdiensteanbieter berücksichtig, liegt nicht vor. Diese sollte aber beinhalten, dass der Identifizierungsdiensteanbieter für seinen Dienst IT-Sicherheitsmaßnahmen umsetzt, die nach einem standardisierten Vorgehensmodellen erarbeitet wurden und regelmäßig aktualisiert werden.

zu 5) Berechtigungen sollen zukünftig nicht mehr zweckgebunden, sondern organisationsgebunden vergeben werden. Ein Nachteil, der bereits unter Punkt 2) diskutiert wurde, ist, dass hier für einen Geschäftszweck Daten im Rahmen der eID-Funktion erhoben werden könnten, die nicht benötigt werden (Verstoß gegen die Datensparsamkeit). Wie unter Punkt 2) erläutert, muss der Diensteanbieter dieses Gebot aber umsetzen und hat dazu auch die technischen Möglichkeiten.

Ein weiteres Problem könnte sich ergeben, wenn der Diensteanbieter für einen seiner Geschäftsprozesse die laut Berechtigungszertifikat übermittelten personenbezogenen Daten in unzulässiger Weise verarbeitet oder nutzt. In diesem Fall wird die Berechtigung widerrufen (§21 Absatz 5). Dieser Widerruf gilt dann für alle Geschäftsprozesse, in denen die eID-Funktion genutzt wird. Ob dieser Widerruf zukünftig tatsächlich vollzogen wird, trotz der für den Diensteanbieter erwarteten Folgen aus diesem Schritt, wird die Praxis zeigen.

Alternativ haben Diensteanbieter zukünftig immer noch die Wahl, für verschiedene Geschäftsprozesse verschiedene Berechtigungen zu beantragen. Dies wird durch den Gesetzentwurf hiesigen Erachtens nicht ausgeschlossen.

Zusammenfassung

Grundsätzlich ist die Entscheidung, die eID-Funktion weiter zu fördern, begrüßenswert. Mit der eID-Funktion des Personalausweises und des elektronischen Aufenthaltstitels ist grundsätzlich eine Authentifizierung der Nutzerinnen und Nutzer

ohne einen vorab häufig aufwendigen, weil nicht medienbruchfreien Erstregistrierungsprozess, möglich. Die vorgeschlagenen Änderungen führen nicht zu einer Schwächung der eID-Funktion hinsichtlich Datenschutz und Datensicherheit. Eine Verbreitung dieser Funktion würde darüber hinaus die IT-Sicherheit in vielen Einsatzgebieten deutlich erhöhen. Auch Firmen wie Apple und Google haben erkannt, dass eine Anmeldung allein über Benutzername/Passwort nicht mehr dem heutigen Sicherheitsstandard genügt und führen Verfahren ein, die auf mehr als einem Authentisierungsfaktor basieren.

Ob die oben aufgeführten Änderungen an der eID-Funktion die gewünschte Wirkung zeigen, kann zum jetzigen Zeitpunkt noch nicht mit Sicherheit gesagt werden. Gerade die Abschaffung des Ausschalten der eID-Funktion und die vereinfachte Beantragung von Berechtigungszertifikaten könnten aber hierzu beitragen. Darüber hinaus ermöglicht die Einführung von Identifizierungsdiensteanbietern die Nutzung der eID-Funktion auch für kleinere Diensteanbieter.

Mit freundlichen Grüßen

Prof. Dr. Marian Margraf