

Gläserne Bürger wegen der staatlichen E-ID?

Autoren : Annett Laube, Gerhard Hassenstein, Marc Kunz

Datum : 3. September 2018



Das E-ID-Gesetz soll es allen Bürger ermöglichen, einfach und sicher verschiedene Dienstleistungen im Internet zu beziehen. Wichtig für eine grosse Akzeptanz ist das Vertrauen in die Sicherheit und vor allem in den Schutz der persönlichen Daten und damit der Privatsphäre. Genügt der aktuelle Entwurf diesen Anforderungen oder wird durch die staatliche E-ID eine flächendeckende Überwachung der Bürger ermöglicht?

Am 1. Juni 2018 wurde der Entwurf des Bundesgesetzes über elektronische Identifizierungsdienste (E-ID-Gesetz) [1] vom Bundesrat vorgestellt. Ziel des E-ID Gesetzes ist es, eine staatlich anerkannte elektronische Identität zu schaffen, die für die Verwendung von verschiedenen Dienstleistungen im Internet genutzt werden kann. So soll es z. B. für einen Webshop möglich sein, anhand der E-ID festzustellen, wer gerade einen Artikel kaufen möchte. Dem Benutzer bleibt es erspart, ein Benutzerkonto beim Webshop zu erstellen und sich zu registrieren (auch wenn dies im Hintergrund automatisiert gemacht wird). Auf der Webseite des Bundesamtes für Justiz befinden sich Videos, die den Vorgang veranschaulichen [2].

Im E-ID Gesetz wird u.a. geregelt, dass beim Ausstellen einer E-ID dieser zusammen mit den

Personenidentifizierungsdaten (amtl. Name, Vorname, Geburtsdatum) eine eindeutige Identifikationsnummer zugewiesen wird (Art. 5). Laut Botschaft zum E-ID Gesetz [3] wird diese E-ID-Registrierungsnummer dauerhaft und widerspruchsfrei einer Person zugewiesen. Wie in der folgenden Abbildung 1 dargestellt, bildet diese Registrierungsnummer damit den Anker zu den Daten der E-ID-Inhaber, indem die zertifizierten IdP diese Nummer als Identifikator erhalten (2). Sie dient in der Folge der automatisieren Abfrage von Personendaten durch die zertifizierten IdPs.

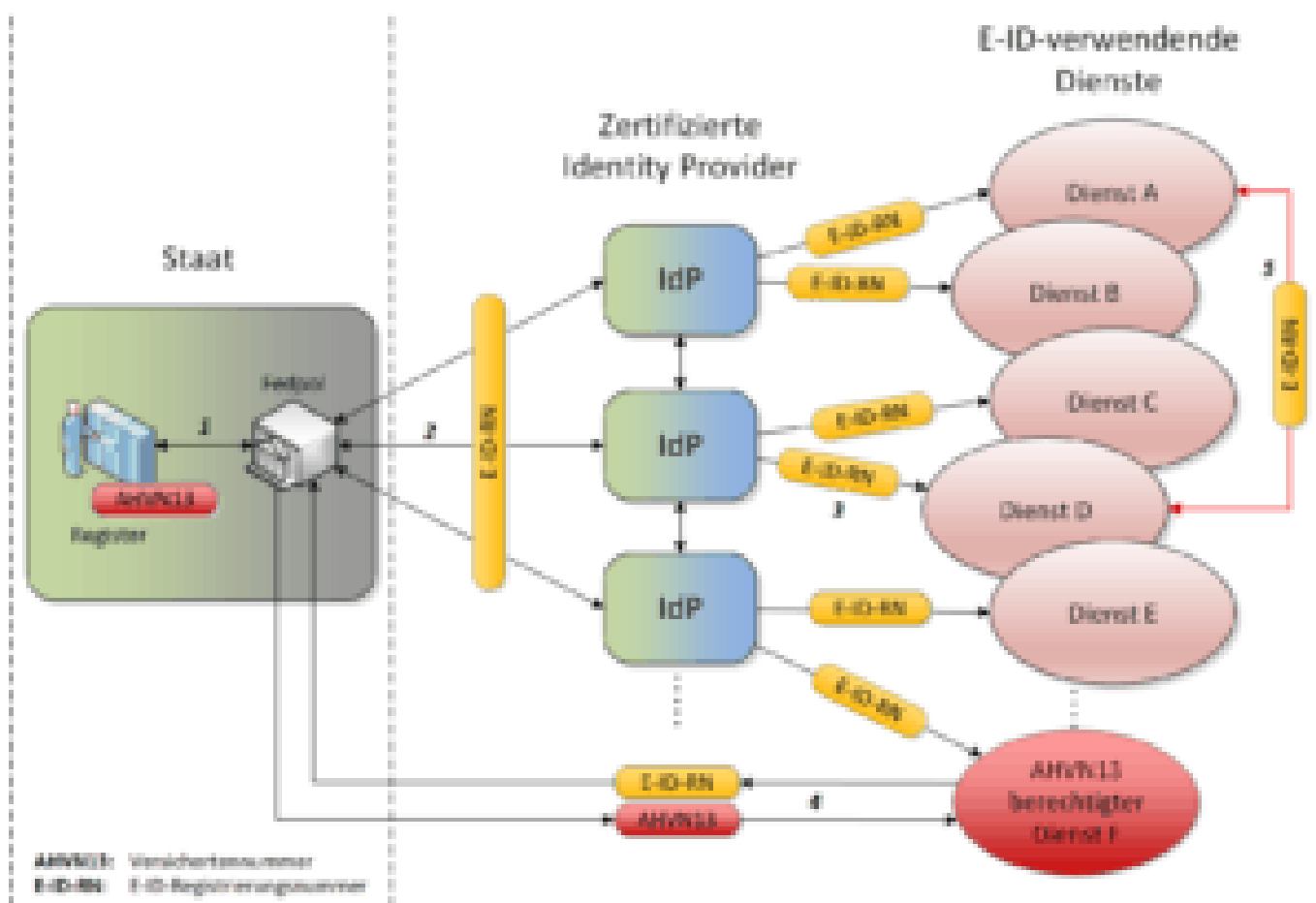


Abbildung 1: Anwendungsbereiche der Identifikatoren

Art. 8 des E-ID Gesetzes bestimmt, dass das Fedpol zum Abgleich von Personendaten mit Registern und Datenbanken die Versicherungsnummer (AHVN13) als eindeutigen Identifikator verwenden darf, um eine eindeutige Zuordnung zu ermöglichen (1). Die AHVN13 wird nie als Attribut an die zertifizierten IdP geliefert, um einer missbräuchlichen Nutzung durch unberechtigte Dienste vorzubeugen. Wenn aber ein zur Nutzung der AHVN13 berechtigter Dienst diese als Attribut benötigt, so kann er nach Übermittlung der E-ID-Registrierungsnummer (E-ID-RN) die entsprechende AHVN13 abfragen (4).

Laut Art. 21 des E-ID-Gesetzes darf die E-ID-RN von allen E-ID verwendeten Diensten zur

Identifizierung von Personen genutzt werden. Das heisst, die zertifizierten IdPs können mit dem Einverständnis des Inhabers die E-ID-RN an einen E-ID verwendenden Dienst weitergeben (3). Wird das Realität, hat man einen eindeutigen Personenidentifikator, der nun nicht mehr nur in Teilbereichen des E-Governments verwendet darf, wie die AHVN13, sondern übergreifend sowohl im E-Government als auch in allen anderen Bereichen der Gesellschaft.

Auch wenn die Betreiber von E-ID-verwendenden Diensten laut Datenschutzgesetz, die Personenidentifizierungsdaten, inkl. der E-ID-Registrierungsnummer, nur mit expliziter Zustimmung des Inhabers (weiter-)verwenden dürfen, besteht ein hohes Risikopotential von ungewollten Verknüpfungen der Daten (5).

Beispiel: Ein E-ID-Inhaber verwendet seine E-ID zum E-Banking bei seiner Bank 'credit4you'. Unabhängig davon kauft er online beim Webshop 'allyouneed' ein und nutzt auch hier seine E-ID zur Authentifizierung. Sowohl die E-Banking-Anwendung, wie auch der Online-Shop bekommen nach der expliziten Freigabe die Personendaten des E-ID-Inhabers einschliesslich der E-ID-Registrierungsnummer. Der Zufall will es, dass beide Dienste demselben Anbieter gehören. Es ist deshalb nicht unwahrscheinlich, dass Informationen zum Kaufverhalten des E-ID-Inhabers mit seinen Bank-Informationen verknüpft werden und zum Beispiel - basierend auf dem eindeutigen Personenidentifikator - beim Online-Kauf sehr einfach und schnell Bonität und Liquidität des Kunden geprüft werden können. Auch der Kauf von Sportartikeln zu Risiko-Sportarten könnte demnach zu einer veränderten Betrachtung z.B. bei der Kreditvergabe führen.

In der Botschaft zum E-ID Gesetz wird darauf hingewiesen, warum auf eine systematische Verwendung der AHVN13 verzichtet wird. Die Gefahr einer Vernetzung von Personendatensätzen wird als zu gross eingeschätzt. Warum die Gefahr einer systematischen Verwendung der E-ID-Registrierungsnummer sowohl im privaten Bereich als auch im E-Government geringer sein soll, ist unklar. Die Freiwilligkeit der E-ID und die daraus geschlossene fehlende Abdeckung sind als Argumente in keiner Weise ausreichend.

Zum Glück ist noch genug Zeit, geeignete Massnahmen zu definieren, um dem Schadenspotential entgegen zu treten. Aus unserer Sicht hat dabei eine Massnahme erste Priorität:

- Die E-ID Registrierungsnummer bleibt den zertifizierten Identity Providern (IdP) vorbehalten und darf von diesen nur zur regelmässigen Aktualisierung der Personendaten mit dem Fedpol verwendet werden. Die Weitergabe an E-ID-verwendende Dienste ist untersagt.

Als zweite Massnahme folgt:

- Der IdP übergibt jedem E-ID verwendenden Dienst einen immer gleichbleibenden aber individuellen Identifikator (IND-E-ID). Anhand dieses Identifikators kann der Dienst den E-ID-Inhaber jederzeit wieder identifizieren. Damit wird eine einfach herzustellende

Verknüpfung der Personendaten eines E-ID Inhabers über die Grenze eines E-ID verwendenden Dienstes hinweg mehrheitlich verhindert.

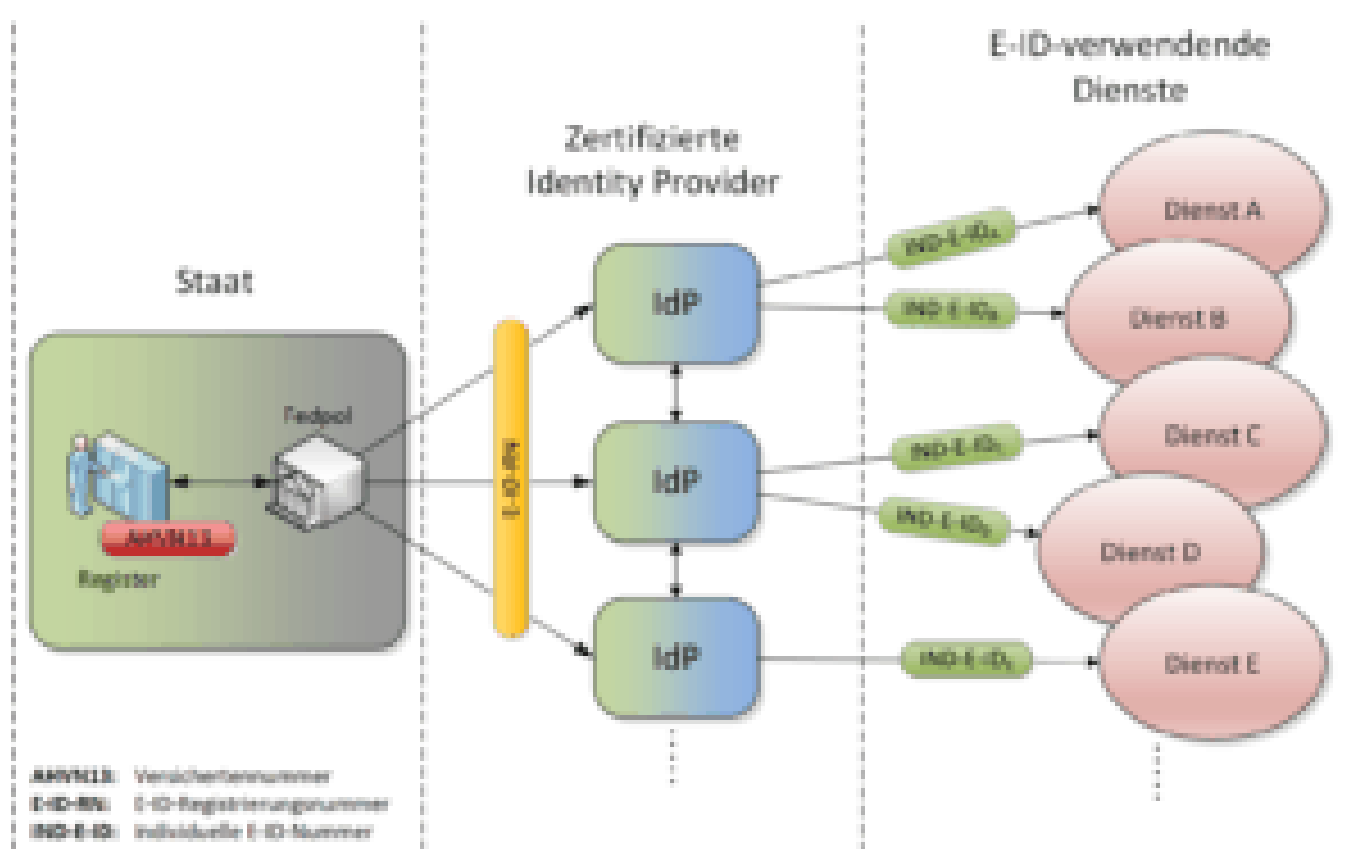


Abbildung 2: Individuelle E-ID-Nummern pro Dienst

Damit die Abfrage der AHVN13 für berechtigte Dienste dennoch möglich ist (vgl. Abbildung 1), sind weitere Massnahmen notwendig. Ein zusätzlicher Baustein in einem E-ID Ökosystem könnte auch die Einführung eines sektoriellen Identifikators sein, bei welchem mehrere berechtigte Dienste sich einen gemeinsamen Identifikator teilen.

Die oben erwähnte Massnahme und weitere Vorschläge werden in zusätzlichen Artikeln vertieft betrachtet.

Referenzen

- [1] <https://www.admin.ch/opc/de/federal-gazette/2018/3989.pdf>
- [2] <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html>
- [3] <https://www.admin.ch/opc/de/federal-gazette/2018/3915.pdf>