SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Erweiterungen beim Einsatz von individuellen E-ID-Nummern

Autoren : Annett Laube, Gerhard Hassenstein, Marc Kunz

Datum : 21. September 2018

Für die personalisierte Anmeldung würde sich auch die AHV-Nummer der Bürgerinnen und Bürger eignen, zeigen unsere AutorInen in ihrem Beitrag über den aktuellen Entwurf zur E-ID.

Wie im Artikel Gläserne Bürger wegen staatlicher E-ID? bereits aufgezeigt, kann ein wichtiger Beitrag zum Schutz der Privatsphäre geleistet werden, indem die E-ID Registrierungsnummer nur den zertifizierten Identity Providern (IdP) vorbehalten bleibt und von diesen nicht an E-ID-verwendende Dienste weitergegeben wird. Mit dieser Massnahme kann der einfache und automatisierte Abgleich von persönlichen Daten durch E-ID konsumierende Dienste in verschiedenen gesellschaftlichen Bereichen verhindert werden. Diese Einschränkung macht aber kleine Anpassungen in den Prozessen beim Fedpol, wie auch bei den zertifizierten IdPs notwendig.

Individuelle E-ID Nummern

Da die IdPs jedem E-ID verwendenden Dienst einen individuellen, aber immer gleichbleibenden Identifikator übergeben sollen (vgl. dazu Abbildung 2 in ‘Gläserne Bürger wegen staatlicher E-ID ?’), müssen sie diesen aus der E-ID-Registrierungsnummer (E-ID-RN) und der Identität des E-ID verwendenden Dienstes einmalig ableiten und als Attribut zu den Daten des E-ID Inhabers in ihrer Datenhaltung beifügen. Wichtige Bedingungen: Die individuelle E-ID (IND-E-ID) muss pro Dienst einmalig sein und dieser darf aus dieser abgeleiteten IND-E-ID nicht auf die ursprüngliche E-ID-RN zurückschliessen können.

Verwendung der AVHN13 nach E-ID Gesetz

Laut Entwurf des E-ID Gesetzes kann ein Dienst die E-ID-Registrierungsnummer (E-ID-RN) auch dazu verwenden um beim Fedpol die AHVN13 abzufragen. Dazu wird das Fedpol einen speziellen Abfragedienst zur Verfügung stellen, welcher zuvor prüft ob ein Dienst überhaupt dazu berechtigt ist. Der Benutzer selbst ist bei dieser Abfrage nicht mehr involviert.

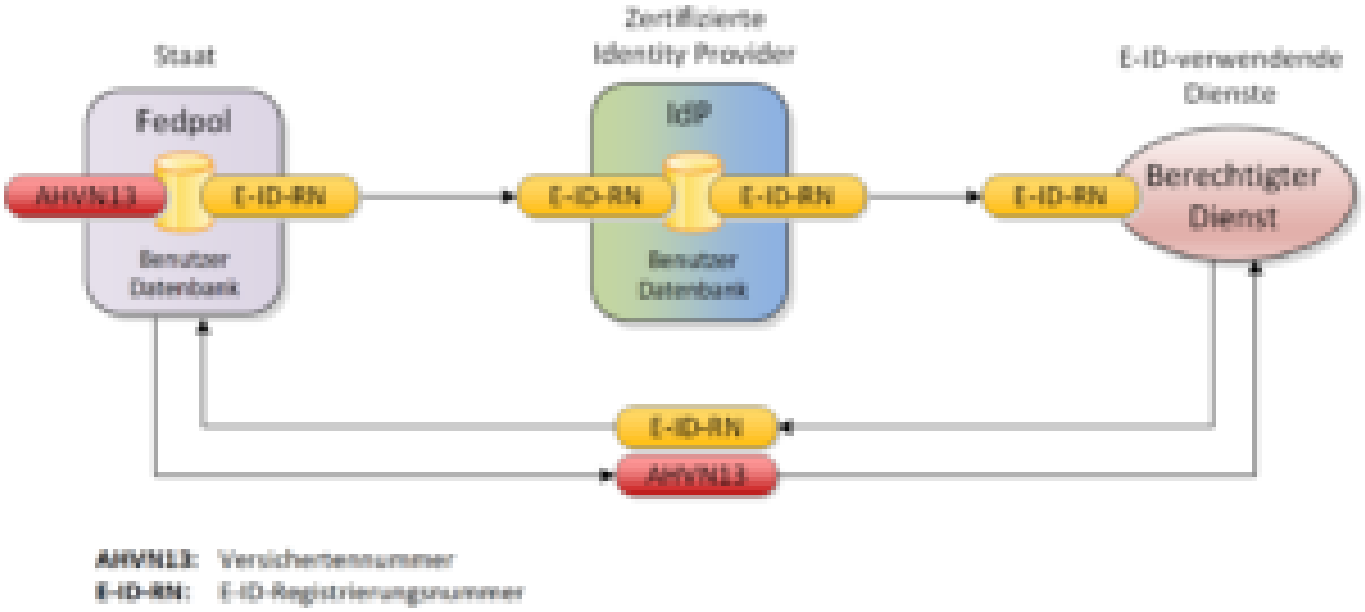

Abbildung 1: AHVN13-Abfrage nach E-ID Gesetz

Der Vorteil dieser Lösung liegt in deren Einfachheit. Jeder berechtigte Dienst ist in der Lage zu jedem Zeitpunkt die AVHN13 mit Hilfe der E-ID-RN - welche vom Fedpol ausgegeben wurde - abzufragen. Der IdP hat davon keine Kenntnis, da er an diesem Prozess nicht beteiligt ist. Bei der Verwendung von individuellen E-ID Nummern, funktioniert aber die oben aufgezeigte Abfrage der AHVN13 gemäss E-ID Gesetz nicht mehr, da ein E-ID verwendender Dienst vom IdP eine individuelle Nummer erhält, die dem Fedpol nicht bekannt ist.

Erweiterte Methode

Dieses Problem kann auf verschiedene Arten gelöst werden. An dieser Stelle soll eine Methode

aufgezeigt werden, welche sehr einfach umzusetzen ist und nur kleine Anpassungen auf Seiten Fedpol und IdP erfordern. Diese Anpassung beinhaltet eine kleine Erweiterung, indem der zertifizierte IdP die individuelle E-ID Nummer wie oben beschrieben bildet, diese aber nun für den vom Fedpol zur Verfügung gestellten Abfragedienst verschlüsselt. Wenn der IdP diese individuelle E-ID so an den E-ID verwendenden Dienst übermittelt, kann dieser ohne Kenntnis des entsprechenden Schlüssels die darin enthaltene E-ID-RN nicht entziffern. Er kann diese IND-E-ID aber dazu verwenden, um beim Fedpol die AHVN13 abzufragen, da dieses die verschlüsselte Zeichenkette dechiffrieren und damit die E-ID-RN extrahieren kann. Da jeder Dienst für einen bestimmten E-ID Inhaber aber eine andere IND-E-ID erhält, können diese nicht korreliert werden.

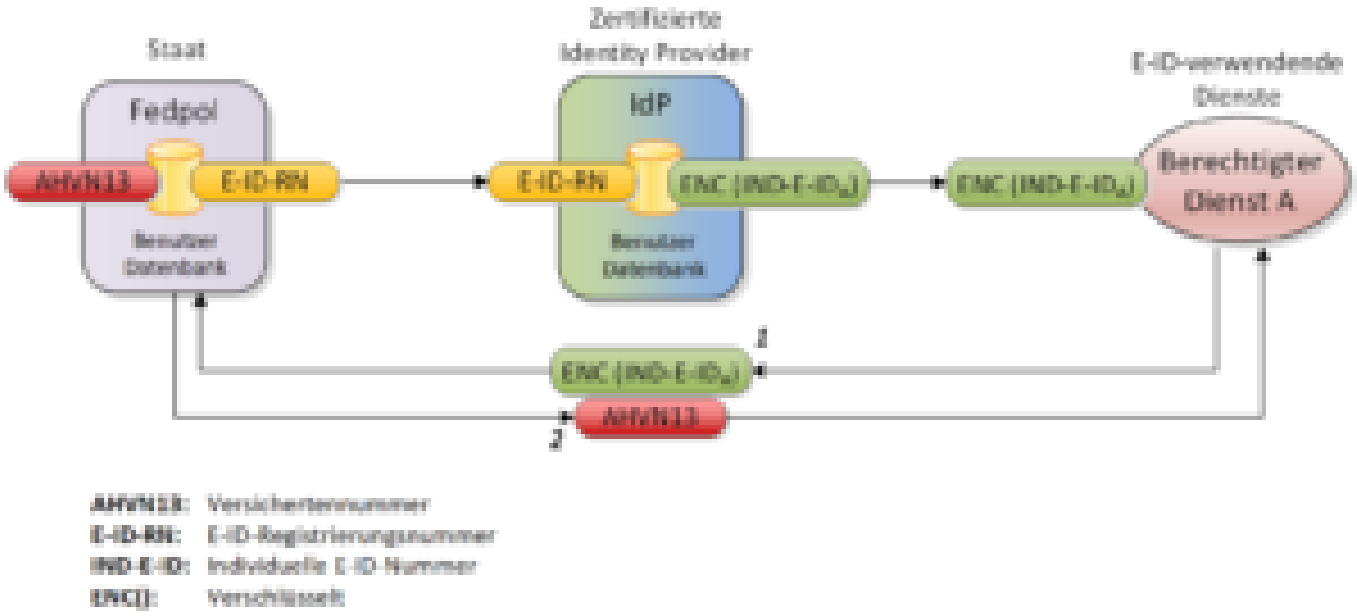

Abbildung 2: AHVN13-Abfrage mit verschlüsselter IND-E-ID

Zur Abfrage der AHVN13 sendet der Dienst dem Staat die verschlüsselte IND-E-ID in seiner Anfrage (Schritt 1). Der Staat entschlüsselt die IND-E-ID, extrahiert die E-ID-RN und sendet die AHVN13 an den Dienst zurück, sofern er berechtigt ist diese abzufragen (Schritt 2).

Sektorenspezifische Identifikatoren

Wie die Studie zur Klärung von identifikatorspezifischen Risiken [4] als Massnahme vorschlägt, sollte - wenn immer möglich - anstelle der AHVN13 ein sektorenspezifischer Identifikator zum Einsatz kommen, um damit bestimmte Angriffsvektoren zu verhindern.
Die Verwendung eines sektorenspezifischen Identifikators ist auf einen bestimmten gesellschaftlichen Bereich (z.B. Gesundheitswesen, Bildungswesen) beschränkt. Abbildung 3 zeigt die Verwendung von sektorenspezifischen Identifikatoren auf. Das Fedpol würde in diesem Fall eine Liste der sektorenspezifischen Dienste führen und folglich sektorenabhängig einem anfragenden Dienst eine sektorenspezifische E-ID (SEKT-E-ID) und nicht die AHVN13 zurückgeben.

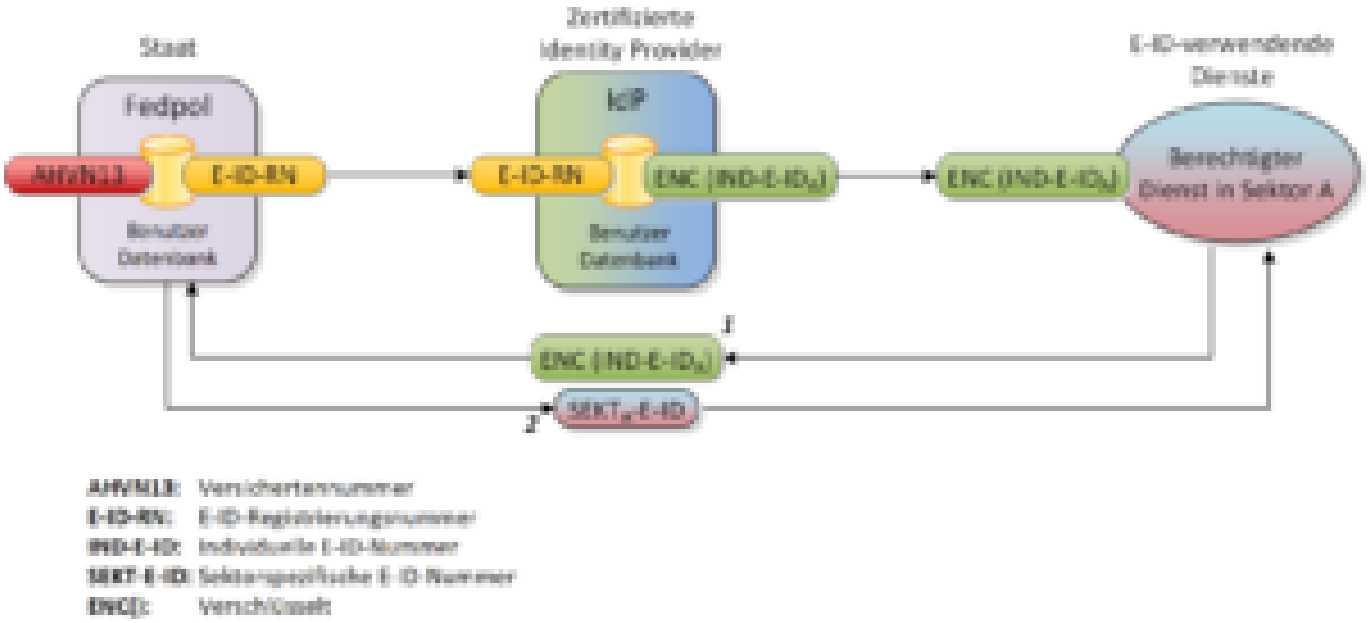

Abbildung 3: Sektorenspezifische E-ID

Durch die Verwendung von sektorenspezifischen Identifikatoren können sich mehrere berechtigte Dienste einen gemeinsamen Identifikator teilen, was innerhalb eines Sektors sinnvoll ist. Das Risiko zur Verknüpfung grosser Mengen von Personendaten über die Sektorengrenze hinweg, kann damit aber verhindert werden. Um sektorenspezifische Identifikatoren einzusetzen zu können, müssen Dienste bestimmten Sektoren zugewiesen werden. Wie diese Zuweisung erfolgen soll, ist Aufgabe des Gesetzgebers.

Trennung von Identifikatoren und personenidentifizierenden Merkmalen

Als weitere Massnahme zur Minimierung der Risiken schlägt die Studie eine Trennung von Identifikatoren und personenidentifizierenden Daten vor. Damit auch bei unterschiedlichen Identifikatoren eine Re-Identifizierung und damit Verknüpfung der Personendaten mit Hilfe der personenidentifizierenden Daten verhindert werden kann. Dies hat aber weitreichende Änderungen in der Datenhaltung zur Folge und ist deshalb mit grösserem Aufwand verbunden.

Fazit

Mit diesen Anpassungen kann ein E-ID Gesamtsystem bezüglich ‘Schutz der Privatsphäre’, Datenschutzrisiken und möglicher Angriffspotenziale für künftige Anwendungen und für die zu erwartende Entwicklung erheblich besser vorbereitet werden.
Der Aufwand für die erste erwähnte Massnahme (verschlüsselte, individuelle E-ID) ist minimal und kann kurzfristig eingeplant werden, da ein zertifizierter IdP nicht mehr einfach die E-ID-RN an irgend einen Dienst weitergeben soll, sondern an deren Stelle eine individuelle E-ID mit

verschlüsseltem Inhalt generieren und weitergeben soll, welche bei Bedarf nur der AHVN13-Abfragedienst des Fedpol entschlüsseln kann. Der konsequente Einsatz von sektorenspezifischen Identifikatoren hingegen, kann mit recht hohem Mehraufwand verbunden sein und sollte deshalb eher in eine mittel- bzw. langfristige Planung einfliessen.

Referenzen

https://www.admin.ch/opc/de/federal-gazette/2018/3989.pdf

https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html

https://www.admin.ch/opc/de/federal-gazette/2018/3915.pdf

https://www.admin.ch/opc/de/classified-compilation/19470240/201806010000/831.101.pdf