BUNDESGESETZ ÜBER DEN ELEKTRONISCHEN IDENTITÄTSNACHWEIS UND ANDERE ELEKTRONISCHE NACHWEISE (EID-GESETZ, BGEID)

VERNEHMLASSUNGSANTWORT

Verfasser
Dr. Bruno Wildhaber

Version
1.0

Datum
2022—10—09

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen

eID

Zum krm:

DAS KRM (Kompetenzzentrum Records Management AG) IST EIN UNABHÄNGIGES BERATUNGSHAUS auf den Gebieten des Datenmanagements und der Informationssicherheit

Das krm kombiniert interdisziplinäre Kompetenz und langjährige Erfahrung im Daten- und Informationsmanagement zum Nutzen des Kunden. Der Fokus liegt auf der Beherrschung der Datenflut und den Anforderungen der Cybersecurity. Das Unternehmen bietet nebst Beratung und Schulungen verschiedene Lösungen und ist Kompetenzpartner einiger führender Lösungsanbieter. Dabei setzt das krm auf eigene Methoden bei der Umsetzung von Projekten in allen Industriezweigen und der Verwaltung.

Das krm verfügt über jahrzehntelange Erfahrung in der Konzeption und Gestaltung von rechtskonformen Identitätssystemen und -verfahren. Experten des krm waren u. a. bei der Erstellung der Signaturgesetze in D und CH tätig. Das krm und seine Partner haben mehrere Fachbücher zu diesen Themen verfasst und wir dozieren regelmässig an nationalen und internationalen Hochschulen.

Kompetenzzentrum Records Management AG Hegnaustr. 60 6802 Wangen
Tel. +41 44 888 10 11 Info@krm.swiss www@krm.swiss

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen

ZUSAMMENFASSUNG
EXECUTIVE SUMMARY

Die Ausgabe eines einfachen digitalen Ausweises (eID) ist so rasch als möglich umzusetzen.

Bevor über Ökosysteme nachgedacht werden soll, muss mit höchster Dringlichkeit diese EINE eID SOFORT umgesetzt werden (nutzbar für Bund und Kantone). Wir finden es unnötig, dass der vorliegende Vorentwurf bzw. die vorgesehene Infrastruktur unterschiedliche elektronische Nachweise vorsieht und ein umfangreiches Ökosystem gemäss Ambitionsniveau 3 beschreibt. Letzteres führt zu einer Verzettelung der Kräfte und wird die Einführung der dringend benötigten eID unnötig verzögern. Eine Beschränkung auf das Wesentliche bildet den Schlüssel zum Erfolg.

Ohne massive Vereinfachung droht der eID das Schicksal des ePD (el. Patientendossier).

Die Erfüllung von Sicherheitsanforderungen und Datenschutzanliegen sind zwar wichtig, stehen aber klar hinter der Einfachheit und offenen Anwendbarkeit der eID.

Die Drittnutzung der Infrastruktur erzeugt unbekannte Risiken.

Die Nutzung der Infrastruktur für andere elektronische Nachweise ausserhalb der eID ist zu überdenken. Die damit verbundenen Risiken sind nicht zu unterschätzen und können für den Bund nicht abschätzbare Folgen haben. Das schliesst nicht aus, dass unterliegende ID-Aussteller die eID nutzen können (im Vordergrund stehen z.B. die Kantone), sie sind dann aber lediglich Konsumenten und haben keinen Einfluss auf die Sicherheit des Gesamtsystems. Ob im Einzelfall andere Anwender die eID nutzen können, müsste im Einzelfall rigorosen Risikobeurteilungen unterliegen (ins Gesetz aufzunehmen).

Der Grundsatz der Technologieneutralität wurde gut berücksichtigt.

Die Technologieneutralität ist im Entwurf gut umgesetzt und sollte nicht verwässert werden. Insbesondere ist auf eine detaillierte Beschreibung der technischen Verfahren und Systeme bei den Endbenutzern zu verzichten.

Nutzen, was bereits existiert: Für die eID-Infrastruktur existiert bereits ein Gesetz!

Völlig übersehen wurde offenbar, dass für die Umsetzung der Infrastruktur in Kapitel 5 bereits Gesetze existieren, nämlich die ZertES und die VZertEs. Wir empfehlen dringend, diese Gesetze zu harmonisieren. Die ZertEs enthält 80–90 % der im eID-Entwurf beschriebenen Verfahren: Kapitel 5 aus dem Gesetz streichen und ein separates Infrastrukturgesetz erlassen bzw. besser

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen

die ZertES anpassen. Das eID-Gesetz sollte sich auf die Verfahren zur Umsetzung der «Root»-Identität (=eID) beschränken.

Keine Anwendungsfälle ins Gesetz

Wir begrüssen, dass darauf verzichtet wurde, konkrete Anwendungsfälle ins Gesetz aufzunehmen. Diese gehören nicht ins BGEID.

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen

ERLÄUTERUNGEN UND KOMMENTARE

Welches sind die drei wichtigsten Anforderungen an eine staatliche eID als digitaler Ausweis?

Absolut vordringlich und vor allen anderen Überlegungen muss der Entscheid zur sofortigen Umsetzung einer elektronischen Identität fallen. Die Schweiz hat den Zug für die Umsetzung der elektronischen Identität schon lange verpasst. Bereits 1996 fanden unsererseits Besprechungen mit dem EJPD statt, um abzuklären, wann man mit der Einführung einer elektronischen Identität rechnen dürfe. In der aktuellen Situation kann es nur noch um Schadensbegrenzung gehen. Das zu schaffende Gesetz muss möglichst schlank und ohne unnötige Detailregelungen entworfen und im Eilverfahren umgesetzt werden.

Die digitale Identität muss durch den Staat herausgegeben und finanziert werden. Sie ist der «Trust Anchor» und das hochwertigste Identifikationsmittel des Bürgers. Kein System kann eine vergleichbare Vertrauensbasis schaffen (das gilt im Speziellen auch nicht für DLT-basierte Systeme). Aber: Es gibt keine kommerziellen Business Cases, die für die Finanzierung herangezogen werden können. Es handelt sich hierbei um eine Basis-Infrastruktur. Niemand hat sich bei der Einführung des physischen Passes oder der Identitätskarte gefragt, wie häufig man diese werde nutzen können. Noch weniger, ob derjenige, der sich darauf verlässt, daraus einen Business Case ableiten kann. Diese illusionäre Annahme hat unter anderem dazu geführt, dass die Abstimmung zum eID-Gesetz verlorengegangen ist.

Die Umsetzung der digitalen Identität muss möglichst einfach und auf etablierten Technologien erfolgen. Dazu am besten geeignet und praxisbewährt sind Public-Key-Infrastrukturen, welche ohne grossen Aufwand implementiert werden können. Alle anderen Lösungsansätze sind entweder noch nicht reif oder basieren im Kern auch auf PKI- und DLT-Technologie.

Welche Anwendungsfälle der eID stehen im Vordergrund?

Im beleuchtenden Bericht wurde wiederholt von Privacy und Sicherheit gesprochen. Mit kaum einem Wort werden jedoch die wirklich wichtigen Anforderungen angesprochen: Interoperabilität (ausdrücklich gemäss nationaler Datenbewirtschaftung, NaDB) und Einfachheit. Diesen Aspekten wurde zu wenig Augenmerk verliehen.

Wir sind seit 30 Jahren im Geschäftsfeld digitaler Identitäten, Trust Center und digitaler Signaturen tätig. Wir haben viele gute Lösungen kommen und vor allem gehen sehen. Diese sind schlicht daran gescheitert, dass die Benutzerakzeptanz fehlte. Erfolgsfaktoren bei der Umsetzung sind (in dieser Reihenfolge):

1. Zuerst kommt die «Usability», d. h. die möglichst einfache und simple Anwendbarkeit, dann die
2. Kosten: Vergleichbare Kosten wie bei einer traditionellen ID/einem Pass, die

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen

3. Interoperabilität, die Nutzung der ID für Behördengänge (Bund, Kanton), die
4. Sicherheit und ganz zuletzt
5. der Datenschutz.

Selbst wenn man alles perfekt macht, wird die Hemmschwelle nach wie vor sehr hoch sein. Themen wie Datensparsamkeit sind für den Normalbenutzer irrelevant, wenn das System nicht funktioniert. Auch bei der Sicherheit gilt: Im Zweifelsfall wird unverschlüsselt kommuniziert, Verfügbarkeit kommt immer vor Vertraulichkeit. Dieses Verhalten wird sich durch die eID NICHT ändern.

Schlägt man den vorgesehenen Weg ein, riskiert man das Schicksal des ePD: Unendlich hohe Kosten und keine realisierbaren Lösungen. Der Gesetzesentwurf weist in die richtige Richtung. Man hat es vermieden, die übertriebenen und kaum realisierbaren Anforderungen der IT-Lobbyisten zu bedienen. Wir lehnen den SSI-Ansatz derzeit ab (unausgegoren, zu komplex, auf wackligem Grund). Eine Beschränkung auf das Wesentliche bildet den Schlüssel zum Erfolg.

Das fehlgeleitete Dogma: Der Bund muss ein Ökosystem für die Nutzung der eID liefern.

Wie oben bereits erfasst, geht es bei der Schaffung der EID nicht um deren Anwendung. Es ist nicht Aufgabe des Staates, dafür zu sorgen, dass die digitale Identität eingesetzt werden kann (ausser natürlich für seine eigenen Verfahren). Ebenso wenig, wie der Staat Autos gebaut hat, um Autobahnen zu nutzen, muss er Anwendungen für die EID liefern. Sobald eine vertrauenswürdige Identitätsinfrastruktur steht, werden sich sofort Anwendungen anbieten, welche heute entweder bereits in Betrieb sind oder in kurzer Frist in Betrieb genommen werden können.

Die alleinige Kernaufgabe des Staates damit des Bundes ist es, den digitalen Ausweis zu erstellen.

Wichtig ist jedoch, dass die Anzahl staatlicher Identitäten zwingend auf 1 (= eine) eingeschränkt wird! Es kann nicht sein, dass Verwaltungseinheiten oder Kantone zusätzliche Identitäten und Infrastrukturen aufbauen. Dies wäre ein Föderalismus, welcher die EID verunmöglichen würde. Wie erwähnt, die EID soll das Pendant zum physischen Identifikationsdokument sein. Andere Nutzer sollen darauf aufbauen können, aber auf keinen Fall Parallellösungen bauen.

Sobald eine digitale Identität für eine Anwendung genutzt werden soll, gibt es hierzu verschiedene Möglichkeiten für die Umsetzung. Hier darf und soll sich der Herausgeber der EID nicht einmischen. Über die Zeit werden heute isolierte Lösungen die EID als Identifikationsanker nutzen, weil der Aufwand für die Weiterführung eigener Identifikationslösungen zu gross werden wird.

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen

Gefahren der Komplexität und fehlender Akzeptanz

Die im Vorfeld durchgeführten Abklärungen, in welche Richtung die Umsetzung der eID gehen soll, sind fehlgeleitet. Das von der IT-Industrie und den Digitalverbänden geliebte Ambitionsniveau 3 ist ein Irrweg. Statt sich auf das Wesentliche zu beschränken, wird versucht, möglichst viel in das Gesetz zu packen. Das wird nicht funktionieren. Wir haben bereits beim ePD gesehen, dass zu viele Sicherheitsvorgaben zum Scheitern führen. Der SSI-Ansatz ist dabei ein interessanter Versuch, man sollte ihn aber als das behandeln, was er ist: Eine Sammlung von Ideen und ersten Gehversuchen auf einem weitgehend unpräparierten Terrain.

Für die Infrastruktur existiert bereits ein Gesetz

Mit Erstaunen stellen wir fest, dass dasjenige Gesetz, welches bereits 90 % der Infrastrukturfragen regelt, nicht einmal zitiert wurde. Es handelt sich dabei um das ZertEs, es regelt bereits umfassend die wichtigsten Strukturen und Verfahren. Dessen Titel lautet:

943.03: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)

Konkret werden eIDs in Form digitaler Zertifikate herausgegeben werden. Eine eID ist in einem digitalen Zertifikat verkörpert. Damit können diese unter dieses Gesetz fallen. Es erübrigt sich, die Trust-Infrastruktur im BGEID neu zu regeln. Ggf. kann man die Regelungen auf die eID-spezifischen Verfahren und Systeme reduzieren.

Was uns im Detail aufgefallen ist

Die Verfahren in Kapitel 5 sind zumindest noch im Anfangsstadium. Wie erwähnt kann man sich hier an der ZertES orientieren.

Die Verfahren sind sicher noch nicht zu Ende gedacht: So widerspricht der Ablauf in Art. 17 Abs. 3 fundamentalen Sicherheitsprinzipien als auch dem Gebot der Datensparsamkeit. Würde dieses Verfahren so etabliert, ist mit einer sehr hohen Fehlerquote zu rechnen. Zudem lassen sich solche Einträge, wenn das System sauber aufgesetzt wurde, kaum mehr entfernen. Passende Verfahren aufzusetzen ist mit sehr hohen Anforderungen verbunden und man muss mit Sicherheitskompromissen, also Risiken, rechnen.

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | CH 8602 Wangen