Möglichkeit und Notwendigkeit von Standards im Umfeld des Bundesgesetzes über elektronische Identifizierungsdienste (BGEID)

Name	Möglichkeit und Notwendigkeit von Standards im Umfeld des Bundesgesetzes über elektronische Identifizierungsdienste (BGEID)
Kategorie	Potentialanalyse
Reifegrad	Zur Veröffentlichung
Status	In der FG besprochen, dann nochmals überarbeitet und geprüft.
Ausgabedatum	16. September 2020
Sprachen	Deutsch
Autoren	Daniel Muster (it-rm IT-Riskmanagement GmbH)
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Das Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz oder BGEID) wurde Ende der Herbstsession 2019 vom Bundesparlament verabschiedet. Dagegen wurde das Referendum ergriffen und von der Bundeskanzlei im Februar 2020 als zustande gekommen erklärt.

So wie das BGEID konkret ausgestaltet ist, fehlen indessen wichtige Regelungen. Da gewisse Bereiche aber nicht in den Grundzügen geregelt worden sind, darf deren Ausformulierung wegen Art. 164 BV (Bundesverfassung) nicht dem Verordnungsgeber überlassen werden. In anderen Bereichen fehlt es an der Legitimation aus Gesetz, was dazu führt, dass auch dort keine Vorschriften per Verordnung durch den Bundesrat erlassen werden dürfen.

Dort wo keine Vorschrift erlassen werden kann, aber dies für die technische Umsetzung notwendig ist, werden Standards oder „Best Practices“ benötigt.

In diesem Dokument sind eine Reihe solcher Aspekte/Themen in Kürze aufgeführt und erläutert. Die Details hierzu sollen dann separat erarbeitet und festgehalten werden, z.B. in neuen oder bestehenden Standards wie auch in „Best Pratices“. Mit anderen Worten, die Detailarbeit ist nicht Ziel und Bestandteil dieses Dokuments.

Weiter werden Themen aufgegriffen und erläutert, welche durch die Verordnung zwar geregelt werden dürfen. Doch empfiehlt es sich, die Vorschriften hierzu zusammen mit den vom BGEID Betroffenen zu erarbeiten.

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

Inhaltsverzeichnis

1 Status des Dokuments

Dieses Dokument In der FG besprochen und dann nochmals überarbeitet und geprüft worden.

2 Einleitung

In diesem Kapitel wird das Ziel des vorliegenden Dokuments, dessen Abgrenzung wie auch die Struktur und der Nutzen skizziert.

2.1 Ziel des Dokuments

Im Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz oder BGEID) fehlen wichtige Regelungen. Doch diese dürfen nicht über die Verordnung oder über eine Technische Administrative Vorschrift (TAV) zum BGEID ausformuliert werden.

Gründe dafür, dass etwas zwingend in einem Gesetz und folglich nicht in einer Verordnung geregelt werden darf:

> Gemäss Art. 164 der Bundesverfassung (BV) sind Rechte und Pflichten der Personen oder die Verpflichtungen der Kantone bei der Umsetzung und beim Vollzug des Bundesrechts auf Gesetzesstufe festzulegen. Des Weiteren ist der Vollzug von Bundesrecht durch die Kantone nicht blosse Verwaltungsaufgabe. Bei der Wahrnehmung dieses Vollzugs soll den Kantonen möglichst grosse Freiräume belassen werden (Art. 46 BV). Z.B. gemäss Art. 15 UIDG erlassen die Kantone die für den Vollzug notwendigen Ausführungsbestimmungen.
>
> Art. 47 BV verpflichtet den Bund generell, die Eigenständigkeit der Kantone zu wahrend; siehe dazu auch HÄFELIN/HALLER/KELLER, Rz. 945. Weiter haben sie bei der Willensbildung des Bundes beteiligt zu sein (Art. 45 BV).

Selbst wenn der Bund etwas in einer Verordnung regeln darf, bedarf es dazu der Ermächtigung aus Gesetz oder aus der Bundesverfassung.

Das Dokument will Sachbereiche aufgreifen und diese kurz erklären, welche bei der Umsetzung des Bundesgesetzes über elektronische Identifizierungsdienste (BGEID) zu normieren sind; aber, wie erwähnt, nicht über eine Verordnung geregelt werden können/dürfen.

Zudem werden in diesem Dokument Themen aufgegriffen und kurz erläutert, welche durch die Verordnung geregelt werden dürfen. Jedoch empfiehlt es sich, die Vorschriften hierzu zusammen mit den vom BGEID Betroffenen, z.B. mit dem IdP (Identity Provider) und den Kantonen, zu erarbeiten, oder mit Dritten, wie mit der Lehre oder mit Technologiepartnern.

2.2 Abgrenzung

Der hier aufgegriffene Themenbereich beschränkt sich auf folgende Parteien und Aspekte

- E-ID-Inhaber
- E-ID-verwendender Dienst, kurz E-ID-Dienst (Begriff nach Art. 2 Abs. b BGEID)
- E-ID-System (Begriff nach Art. 2 Abs. a BGEID)
- sowie auf die Interaktionen der Parteien untereinander

2.3 Struktur/Inhalt des Dokuments

Struktur und Inhalt des Dokuments präsentieren sich wie folgt:

1. Was nicht vom Gesetz (ausreichend präzise) geregelt ist und durch eine Verordnung nicht vorgeschrieben werden darf, weil die Ermächtigung aus Gesetz fehlt oder in einem Gesetz festgelegt werden muss. Darunter fallen u.a. die Kapitel 3, 5 und 6.
2. Was zwar ausreichend durch eine Verordnung geregelt werden kann, dies aber in Zusammenarbeit mit Privaten festgelegt werden sollte, siehe hierzu Kapitel 9 „Bestimmungen in Zusammenarbeit mit Technologiepartnern“.

Ersteres ist unterteilt in:

- Grundsätzliches. Unter diese Thematik fällt, was grundsätzlich im BGEID fehlt, siehe dazu z.B. Kapitel 3 „Begriffe“
- Aufgaben und Pflichten der involvierten Parteien, siehe Kapitel 5 bis 7.
- Interaktion zwischen den Parteien, siehe Kapitel 8.

Anmerkung: Zwischen den Kapiteln bestehen Überschneidungen, anders formuliert, die Kapitel sind untereinander verzahnt. Doch dies lässt sich hier leider nicht vermeiden.

2.4 Nutzen

Wie dargelegt werden wird, gibt es viele nicht ausdrücklich geregelte Bereiche im BGEID, welche für das Funktionieren aber der Vorschriften bedürfen, zu welchen der Bund jedoch nicht berechtigt ist, Vorschriften zu erlassen. Dies ist bei einem Gesetz oft der Fall. Beispiel:

> Im ZertES und im OR steht nicht, wie eine elektronische Signatur ihre Gültigkeit bewahren soll. Deswegen wurde auch ein entsprechender eCH-Standard (eCH-0220) erarbeitet, basierend auf ETSI-Standards.

Unklarheit (betreffend Vollzug und Einhaltung des Rechts) schafft das Risiko der Rechtsunsicherheit, was wiederum das Risiko des Zwists bei Uneinigkeit über die Rechtslage und folglich der Rechtsstreitigkeit in sich birgt. Letzteres ist der wirtschaftlichen Umsetzung des BGEID und der Ausbreitung der E-ID nicht dienlich.

Auch dort, wo sich die Ausführungsvorschriften auf eine ausreichende Delegation stützen, können ausufernde Ausführungsbestimmungen (Verordnung) dazu führen, dass die Wirtschaftlichkeit aufgrund des durch die Umsetzung verursachten Aufwands nicht mehr gege-

ben ist. Deswegen empfiehlt es sich, gewisse Vorschriften in Zusammenarbeit den davon Betroffenen zu erarbeiten: Beispiel für die Gefahr, ausufernde Bestimmungen zu erlassen:

> Die Forderung nach Technologieneutralität (Art. 1 Abs. 3), nach höchstmöglicher Sicherheit (Art. 4 Abs. 1 Bst. c) oder nach Berücksichtigung des jeweiligen Stands der Technik (Art. 4 Abs. 4 BGEID). Zur potentiellen Uferlosigkeit beim Ausdruck „Stand der Technik“ siehe auch HOLLIGER S. 125 Kommentar zu Art. 8 Abs. 1 Produktsicherheitsgesetz (PrSG).

2.5 Terminologie der Empfehlungen

Richtlinien in diesem Dokument werden gemäss der Terminologie aus [RFC 2119] angegeben, dabei kommen die folgenden Ausdrücke zur Anwendung, die durch **GROSSSCHREIBUNG** als Wörter mit den folgenden Bedeutungen kenntlich gemacht werden (Zitat aus [RFC 2119]):

- **MUST**: This word, or the term "**REQUIRED**" or "**SHALL**", mean that the definition is an absolute requirement of the specification.
- **MUST NOT**: This phrase, or the phrase "**SHALL NOT**" mean that that definition is an absolute prohibition of the specification.
- **SHOULD**: This word, or the adjective "**RECOMMENDED**", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**: This phrase, or the phrase "**NOT RECOMMENDED**" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY**: This word, or the adjective "**OPTIONAL**", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

3 Begriffe

In Folgendem wird eine Reihe von Begriffen erläutert, welche im Gesetz nicht erklärt sind, aber beschrieben werden sollen, weil sie gegebenenfalls relevant für eine juristische Beurteilung zum BGEID sind.

3.1 E-ID

Im BGEID wird nicht definiert, was eine E-ID ist und aus welchen Komponenten sie sich zusammensetzt. Eine Analogie zur Unternehmensidentifikation gemäss UIDG trifft nicht zu, weil mit der E-ID im Unterschied zur UID auch noch ein Authentisierungsmittel verbunden ist. Eine Vorschrift zur Verlinkung der UID mit der Authentisierung besteht bei Art. 7 Abs. 2 Bst. e Bundesgesetz über Zertifizierungsdienste (ZertES).

Im Hinblick darauf, eine Sorgfaltspflichtverletzung festzustellen, ist es wichtig, zuerst dasjenige zu kennen, worauf Sorge zu tragen ist. Z.B. hat der E-ID-Inhaber gemäss Art. 12 Abs. 1 BGEID die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit seine E-ID nicht missbräuchlich verwendet werden kann.

MUST: Der Begriff E-ID muss definiert werden.

3.2 E-ID-Inhaber

Das Gesetz schliesst nicht aus, dass der Käufer einer E-ID identisch mit derjenigen Person ist, für welche die E-ID ausgestellt wird. Analoges gilt für die Ausstellung eines Zertifikats. Um die unterschiedlichen möglichen Rollen in Analogie zum Versicherungsnehmer und zur versicherten Person vorzunehmen, bedarf es weiterer Begriffe.

Es ist denkbar, dass sich jemand als Vertreter eines Unternehmens bei einem E-ID-System authentisieren lässt und dann mit einem E-ID-Dienst verbunden wird. Wie kann dies davon unterschieden werden, dass sich diese Person als Private beim E-ID-Dienst anmeldet? Ein solcher E-ID-Dienst könnte z.B. ein Dienst des Steueramtes zum Ausfüllen der Steuererklärung sein. Daraus ergibt sich zudem die Frage, wer die E-ID für ungültig erklären darf, primär der E-ID-Eigentümer oder auch noch der E-ID-Bezüger. Analoges Beispiel hierfür:

> Ein Mitarbeiter des Bundes bezieht ein Zertifikat der Admin-PKI. Der Bund ist Eigner der Chipkarte und des Zertifikats. Wer ist nun Zertifikatsinhaber nach ZertES, der Bund oder der Mitarbeiter? Z.B. das Zertifikat für ungültig erklären und dies zu publizieren vermag nur der Bund. Ähnliche Fragen treten auf, wenn ein Arbeitgeber eines privaten Unternehmens für seine Arbeitnehmer Zertifikate bezieht.

MUST: Es muss rechtlich abgeklärt werden, ob der E-ID-Eigentümer mit dem E-ID-Nutzniesser identisch sein muss.

Unabhängig davon:

MUST: Das Zusammenspiel zwischen Autorisierung beim E-ID-Dienst und der Authentisierung des E-ID-Inhabers muss geregelt werden, insbesondere wie mit dem Erteilen und dem Löschen der Vertretungsbefugnis beim E-ID-Dienst umzugehen ist.

MUST: Die möglichen Rollen und deren rechtliche Bedeutung im Rahmen des BGEID müssen definiert werden.

Letzteres kann durch Erweiterung des bestehenden Glossars zu IAM (eCH-0219) erfolgen.

3.3 eIDAS

In der eIDAS-Verordnung der EU sind rund 40 Begriffe aufgeführt und definiert worden. Etwas Analoges ist gegebenenfalls auch im Kontext zum BGEID notwendig, damit bei einer landesübergreifenden Verwendung der E-ID ein Vergleich mit der EU hergestellt werden kann und Unterschiede besser erkannt werden. Dies gegebenenfalls, damit in Zukunft grenzübergreifende, juristisch relevante Aspekte betreffend E-ID beurteilt werden können.

SHOULD: Der Abgleich der Begriffe zwischen eIDAS und BGEID soll erarbeitet werden.

Dies kann durch Erweiterung des bestehenden Glossars zu IAM (eCH-0219) erfolgen.

3.4 Anmerkung Technologieneutralität

Das E-ID Gesetz und die darauf abgestützten Verordnungen beachten die Technologieneutralität (Art. 1 Abs. 3 BGEID). In den jeweiligen Technologiestandards werden unterschiedliche Begriffe verwendet, z.B. Client bei OAUTH, Relying Party u.a. bei OpenID Connect.

SHOULD: Folglich soll eine Tabelle mit den für die Vorschriften notwendigen Begriffe und die damit verbundenen Synonyme erstellt werden.

Dies kann durch Erweiterung des bestehenden Glossars zu IAM (eCH-0219) erfolgen.

4 Prozesse/Architektur

Was aus dem Gesetz nicht ersichtlich ist, sind die jeweiligen Komponenten und Prozesse (Aufgaben). Dies ist u.a. nützlich:

- Für das Etablieren der notwendigen (technischen) Rahmenstruktur für das elektronische Identifizieren.
- Für eine Auswahl an möglichen (technischen) Abläufen, z.B. wie das elektronische Identifizieren vonstattengehen soll.
- Für das Fehler- und Change-Management, wie auch für das Logging und Monitoring. Letzteres ist notwendig für die Schaffung der Nachvollziehbarkeit der Abläufe.

SHOULD: Ein Dokument mit möglichen Geschäftsabläufen soll erstellt werden. Damit wird schneller ersichtlich werden, was für den reibungslosen Ablauf im eGovernment betreffend E-ID erforderlich ist.

Anmerkung: Eine Architektur wurde weder im Gesetz noch in der Botschaft zur Gesetzesvorlage ans Parlament referenziert oder meines Wissens dem Parlament im Rahmen der Beratung zum BGEID zugestellt, noch taucht sie im Bericht zur öffentlichen Vernehmlassung zum BGEID auf. Deshalb ist nicht ersichtlich, dass das Gesetz zwingend und nur ein Single-Sign ON Verfahren für die elektronische Identifizierung fordern darf. Die Forderung nach Technologieneutralität (Art. 2 Abs. d BGEID) untermauert dies weiter.

5 IdP (Anbieterin von elektronischen Identitätsdienstleistungen)

Das Anbieten von elektronischen Identitätsdienstleistungen ist ein privatrechtlicher Akt, welcher sich auch in der Haftungsregelung nach Art. 32 BGEID manifestiert. Die Frage ist nun zu klären, ob das Verkaufen von E-IDs ein konzessioniertes Gewerbe nach dem Obligationenrecht (OR) darstellt und somit die vertragliche und ausservertragliche Haftung nur eingeschränkt wegbedungen werden darf, nämlich nur für leichte Fahrlässigkeit (Art. 99 Abs. 3, Art. 100 Abs. 2 und Art. 101 Abs. 3 OR). Wenn die Haftung in den Vertragsbedingungen über das gesetzlich Zulässige wegbedungen wird, ist sie nicht rechtens und somit nicht gültig. Dies hat zur Folge, dass auch das im Rahmen des gesetzlich Möglichen keine Anwendung findet. Folglich ist diese Frage auch für den IdP relevant.

Die Frage der Haftung stellt sich z.B. beim Erwerb einer E-ID, deren Nutzung und in der Vereinbarung zwischen E-ID-Dienst und dem IdP (Art. 20 BGEID).

6 Pflichten/Aufgaben des E-ID-Inhabers

Das Wissen um seine Aufgaben/Pflichten ist für einen E-ID-Inhaber wichtig, will er nicht bei einem durch ihn verursachten Schaden ersatzpflichtig werden. Doch Aufgaben/Pflichten sind im Gesetz nur sehr vage umschrieben und dürfen, wie bereits erwähnt, nicht in einer Verordnung ausformuliert und geregelt werden.

6.1 Umfang der Sorgfalt

Der Inhaber einer E-ID hat die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit seine E-ID nicht missbräuchlich verwendet werden kann (Art. 12 Abs. 1 BGEID).

Problematisch an dieser Formulierung ist einerseits, dass sie suggeriert, dass die Verhinderung eines Missbrauchs einer E-ID einzig in den Händen (in der Verfügungsgewalt) des E-ID-Inhabers liegt. Dies trifft jedoch nicht zu. Denn der Missbrauch einer E-ID kann ebenso durch den IdP wie auch durch den E-ID-Dienst verursacht worden sein. Andererseits ist nicht definiert, was eine E-ID ist. Somit ist der Umfang an Verantwortlichkeit und folglich an Haftung unklar. Beispiele:

> Der IdP lässt bei der Ausstellung einer E-ID nicht die erforderliche Sorgfalt walten und lässt es folglich zu, dass B im Namen von A eine E-ID erhält. B erhält dadurch Zugang zum eBanking Konto von A. Das eBanking System entspricht dem E-ID-Dienst. Ein Verschulden trägt der IdP aufgrund seiner Sorgfaltspflichtverletzung. Diese ermöglicht dann den Missbrauch durch einen Dritten. Jedenfalls ist nicht der vermeintliche E-ID-Inhaber Verursacher des Missbrauchs.
>
> Der E-ID-Dienst prüft die Authentisierungsbestätigung nicht sorgfältig oder ermöglicht es, dass ein Dritter die Verbindung eines berechtigen E-ID-Inhabers übernimmt. Daraus ergibt sich ein Schaden. Auch hier ist nicht der vermeintliche E-ID-Inhaber Verursacher des Missbrauchs.

MUST: Pro verwendete Technologie muss beschrieben sein, wo beim IdP und beim E-ID-Dienst die Ursache für einen Missbrauch der E-ID vorhanden sein kann.

Wenn nun festgehalten worden ist, wo zusätzlich die Ursache einer missbräuchlichen Verwendung einer E-ID bestehen kann, stellt sich die Frage, wie das Risiko minimiert und wie die Ursache festgestellt werden kann. Dieses Risiko sollte auch bei der Erwägung zur Festlegung einer Sicherheitsstufe mitberücksichtigt werden.

Weil aus Gesetz die Nachvollziehbarkeit des gesamten Prozesses des elektronischen Anmeldens beim E-ID-Dienst nicht gefordert wird und folglich die daraus resultierenden Pflichten im BGEID nicht ausformuliert sind, wird das Schaffen der Nachvollziehbarkeit eine schwer zu lösende Aufgabe sein.

Erschwerend kommt hinzu, dass eine Partei bei einem von ihr verursachten Schaden nicht dazu beitragen muss, den Nachweis zu erbringen, dass sie den Schaden verursacht hat.

SHOULD: Risiken zur elektronischen Identitätsübernahme und Massnahmen zu deren Reduktion beim e-ID-Dienst und beim IdP sollen in einem Standard niedergeschrieben und fortlaufend aktualisiert werden.

SHOULD: Dort wo möglich, d.h. wirtschaftlich vertretbar, soll die Nachvollziehbarkeit des elektronischen Anmeldens beim E-ID-Dienst hergestellt werden. Wie dies geschehen soll, soll in einem eCH-Standard festgehalten werden.

Nutzen: Im Allgemeinen ist es dienlich, wenn im Voraus bekannt ist, welche Möglichkeiten des Missbrauchs bestehen und wo dieser auftreten kann. Der Umsetzung des BGEID und der Einführung der E-ID ist es abträglich, wenn ein E-ID-Inhaber versehentlich als für etwas verantwortlich bezeichnet wird und sich nachträglich herausstellt, dass er die haftungsbegründende Situation nicht verursacht hat. Noch abträglicher wäre es, wenn dies dann in der Presse breitgetreten wird.

Anmerkung: Auch bei der UID besteht Potential für Missbrauch, der ausserhalb der Einflussmöglichkeit des UID-Inhabers liegt.

6.2 Aus Gesetz

Wie bereits erwähnt: Der Inhaber einer E-ID hat die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit seine E-ID nicht missbräuchlich verwendet werden kann (Art. 12 Abs. 1 BGEID). Diese notwendigen und zumutbaren Massnahmen unterscheiden sich (gewiss), mit welchem Sicherheitsniveau die elektronische Identifizierung vorgenommen wird. Weil die Berechtigung aus Gesetz fehlt, darf der Bund hierzu keine Vorschriften erlassen wie z.B. im VZertES und der dazugehörigen TAV.

MUST: Die Gepflogenheiten müssen beschrieben werden, wie sich der E-ID-Inhaber beim jeweiligen Sicherheitsniveau einer E-ID zu verhalten hat. Diese Empfehlung ist in Form eines Standards festzuhalten.

Daraus ist dann eine allgemein verständliche Anleitung herzustellen, wie der Otto-Normalverbraucher die E-ID handhaben muss, damit er die Gepflogenheit aus diesem Standard erfüllt.

6.3 Aus Vertrag

Nicht geregelt ist, ob der E-ID-Anbieter (IdP) dem E-ID-Inhaber aus Erwerb einer E-ID weitere Pflichten auferlegen darf/soll oder nicht.

SHOULD: Hierzu soll eine Empfehlung in Form eines eCH-„Best Practices“ abgegeben werden.

7 Pflichten/Aufgaben des E-ID-Dienstes

Das Wissen um seine Aufgaben/Pflichten ist für einen E-ID-Dienst wichtig, soll die elektronische Identifizierung übereinstimmend mit der jeweiligen Sicherheitsstufe erfolgen. Doch diese sind nicht beschrieben und dürfen, wie bereits erwähnt, nicht in einer Bundesvorschrift geregelt werden.

7.1 Grundsätzliches

Die Pflichten und Aufgaben, resp. die Haftung des E-ID-Dienstes sind in den Artikeln 20 bis 22, resp. 32 BGEID festgelegt. Doch welche Aufgaben bei der Zusammenarbeit mit einem IdP oder mit einem E-ID-Inhaber konkret zu erfüllen sind, regelt das Gesetz nicht. Z.B. hängen die Aufgaben/Pflichten zur Verringerung des Missbrauchs einer E-ID u.a. von der Sicherheitsstufe und von der dabei angewandten Technologie ab.

> Im Unterschied hierzu sind die Aufgaben des IdP in gewissen Bereichen detailliert und umfassend geregelt (Art. 13 Abs. 2, Art. 15 bis 18). In Art. 13 Abs. 4, 15 Abs. 3 und 18 Abs. 3 ist eine Ermächtigung enthalten, dass der Bund zu den Bestimmungen im jeweiligen Artikel Ausführungsvorschriften erlassen darf.

MUST: Pro jeweilige Sicherheitstechnologie und pro Sicherheitsniveau müssen die Aufgaben des E-ID-Dienstes beschrieben werden, damit das Risiko für Missbrauch der E-ID reduziert werden kann. Dies muss im Standard definiert werden.

7.2 Festlegen des Sicherheitsniveaus

Der E-ID-Dienst hat grundsätzlich zu bestimmen, mit welchem Sicherheitsniveau die elektronische Identifizierung des E-ID-Inhabers vorgenommen werden soll. Ausnahme davon kann z.B. sein, wenn der E-ID-Inhaber (seine) sensitive(n) Informationen beim E-ID-Dienst hinauflädt. Dann kann der E-ID-Inhaber wünschen, dass der E-ID-Dienst bestimmte Sicherheitsmassnahmen einhält.

MUST: Das gewählte Sicherheitsniveau muss die Anforderung/Rahmenbedingung aus Gesetz beachten.

Eine Anleitung dazu, wie das Sicherheitsniveau bestimmt werden kann, wäre für den Betreiber des E-ID-Dienstes nützlich. Eine Bestimmung aus Gesetz wie „angemessen zu schützen“ ist aus Sicht des IT-Fachmanns des E-ID-Dienstes wenig hilfreich.

SHOULD: Eine Anleitung zur Bestimmung des für den E-ID-Dienst notwendigen Sicherheitsniveaus soll verfasst werden. Dies soll in Form eines eCH-„Best Practices“ festgehalten werden.

Anmerkung: Es besteht ein Unterschied, wie eine Sicherheitsstufe ausgestaltet ist (Massnahme zur Verringerung des Risikos) und wie man eine Sicherheitsstufe auswählt (Klassifikation der Information). **Fiktives Beispiel für die Klassifikation:**

> Für das Anmelden beim Patientendossier mit Schreibrechten oder zu einem Bundesregister mit Schreibrechten wird für das Anmelden die höchste Sicherheitsstufe gefordert.

7.3 Wirtschaftlichkeit in der Umsetzung

Eine für ein bestimmtes Sicherheitsniveau ausgestellte E-ID kann auch auf einem tieferen Sicherheitsniveau eingesetzt werden (Art. 4 Abs. 3 BGEID). D.h. z.B., dass der E-ID-Dienst für das Sicherheitsniveau 1 auch die Interoperabilität für das Niveau 2 und 3 bereitstellen muss. Dies wiederum kann Mehrkosten schaffen.

SHOULD: Einen Modus Vivendi finden, wie dies ökonomisch realisiert werden kann. Dies u.a. in Zusammenarbeit mit denjenigen, welche elektronische Dienste anzubieten haben, weil sie eine E-ID zu akzeptieren haben. Dies soll in Form eines eCH-„Best Practices“ festgehalten werden.

8 Empfehlungen zur Interaktion zwischen den Parteien

Die notwendigen Interaktionen zu kennen, resp. die Schnittstelle zwischen den involvierten Parteien zu definieren, ist für das Funktionieren und die Sicherheit der elektronischen Identifizierung wichtig. Die hier involvierten Parteien sind der E-ID-Inhaber, E-ID-Dienst und der IdP mit dem E-ID-System.

8.1 Zwischen E-ID-Inhaber und IdP

Vieles wird zwischen dem E-ID-Inhaber und dem IdP im Gesetz festgelegt und kann weiter über die Verordnung geregelt werden. Hier werden jedoch weitere technische Bereiche erläutert, welche durch eine Vorschrift nicht geregelt werden können, aber für den störungsfreien Umgang notwendig sind. Dabei wird nicht Anspruch auf Vollständigkeit erhoben.

8.1.1 Authentisierung des E-ID-Systems

Wenn die Authentisierung des E-ID-Systems nicht verlässlich ist und nicht durch den E-ID-Inhaber geprüft wird oder werden kann, dann kann dies Risiken betreffend Missbrauch einer E-ID in sich bergen. Z.B. wenn sich der E-ID-Inhaber mit einem Passwort vermeintlich bei einem E-ID-System authentisieren lässt oder dort anmeldet. Das Passwort wird dann einem falschen Server übergeben, was die Möglichkeit schafft, dass sich jemand im Namen dieses E-ID-Inhabers bei einem E-ID-Dienst anmelden kann.

> Anmerkung: Der E-ID-Inhaber meldet sich z.B. bei einem E-ID-System an, um seine Daten einzusehen (Art. 15 Abs. 1 Bst. j BGEID).

MUST: Die Authentisierung des E-ID-Systems muss beschrieben werden und was dabei der E-ID-Inhaber zu beachten/prüfen hat. Dies soll in Form eines eCH-Standards festgehalten werden.

8.1.2 Ausgestaltung der Webseite des E-ID-Systems

Wenn die Webseite des E-ID-Systems nicht sorgfältig ausgestaltet ist, kann dies zu Missbrauch einer E-ID führen. Siehe z.B. XSS und XSRF Attacken und Gegenmassnahmen. Zu XSS und XSFR, siehe STUTTARD/PINTO und EXCESS XSS.

MUST: Es muss vorerst abgeklärt werden, ob dieser Aspekt unter die Bestimmung von Art. 15 Abs. 1 Bst a BGEID fällt und von Art. 15 Abs. 3 BGEID erfasst wird.

Falls nicht, dann:

MUST: Richtlinien zur Ausgestaltung der Webseite des E-ID-Systems müssen verfasst werden. Dies soll in Form eines eCH-Standards festgehalten werden.

8.1.3 Authentisieren des E-ID-Inhabers

Das Authentisieren des E-ID-Inhabers hängt vom Sicherheitsniveau ab. Dies kann über eine Verordnung definiert werden.

8.1.4 Verlässlichkeit der Zustimmung zur Weitergabe der Personaldaten

Die Personendaten für die Identifizierung resp. Bestimmung des E-ID-Inhabers dürfen nicht ohne dessen Zustimmung vom IdP an den E-ID-Dienst weitergeleitet werden (Art. 16 Abs. 1 Bst. c BGEID). Wie dies verlässlich zu erfolgen hat, geht daraus nicht hervor und darf nicht durch eine Verordnung näher beschrieben werden.

MUST: Verfassen einer technischen Richtlinie in Form eines eCH-„Best Practices“ in Zusammenarbeit mit dem EDÖB, wie dies verlässlich, d.h. u.a. fälschungssicher, zu erfolgen hat.

8.2 Zwischen E-ID-Dienst und E-ID-Inhaber

U.a. Folgendes sollte zwischen dem E-ID-Inhaber und dem E-ID-Dienst definiert werden:

- Die Authentisierung des E-ID-Dienstes gegenüber dem E-ID-Inhaber
- Die Authentisierung des E-ID-Inhabers bei dezentraler Authentisierung
- Die Möglichkeit eröffnen, dass der E-ID-Inhaber das E-ID-System des IdP authentisieren kann, wenn er vom E-ID-Dienst an das E-ID-System zwecks Authentisierung weitergeleitet wird.
- Ausgestaltung der Webseite des E-ID-Dienstes, z.B. Massnahmen gegen XSS und XSFR Attacken.

8.3 Zwischen E-ID-Dienst und IdP

8.3.1 Grundsätzliche Problematik

Behörden oder anderen Stellen, die öffentliche Aufgaben erfüllen, haben nun eine E-ID zu akzeptieren. Dies sofern sie eine elektronische Identifizierung beim Vollzug von Bundesrecht vornehmen und die E-ID die geforderte Sicherheit bietet (Art. 22 BGEID).

Jedoch ist für das Anmelden mit einer E-ID eine Vereinbarung zwischen dem E-ID-Dienst und dem IdP erforderlich.

Ersteres stellt eine Pflicht dar, der Inhalt der Vereinbarung jedoch eine gegenseitige Willenserklärung.

8.3.2 Inhalt der Vereinbarung

Zwar steht im BGEID (Art. 15 Abs. 1 Bst. l): Der IdP erarbeitet Muster für die Vereinbarungen mit Betreiberinnen von E-ID verwendenden Diensten und legt sie dem EDÖB vor.

> Der EDÖB prüft die Vereinbarung aber lediglich unter datenschutzrechtlichem Aspekt, nicht den Vertrag generell.

Doch sind die Kantone vermutlich nicht daran gebunden, welche einen E-ID-Dienst betreiben müssen. Aus dem BGEID ist eine Verpflichtung zum Abschluss einer Vereinbarung beliebiger damit verbundenen Pflichten nicht zu entnehmen. Da Pflichten der Kantone bei der Umsetzung und beim Vollzug von Bundesrecht in einem Gesetz festgehalten werden müssen, besteht keine solche Pflicht.

Deshalb wäre es ökonomisch, wenn die wesentlichen Punkte der Vereinbarung in Absprache mit denjenigen zu treffen sind, für welche eine Pflicht besteht, eine E-ID bei entsprechender Sicherheitsstufe zu akzeptieren.

Der Inhalt der Vereinbarung hängt u.a. auch von der eingesetzten Technologie und von der Sicherheitsstufe ab.

MUST: U.a. in Zusammenarbeit mit der EIDCOM, dem EDÖB, dem IdP und den Kantonen ist eine Modellvereinbarung zu erarbeiten; dies in Form eines eCH-„Best Practices“.

8.3.3 Beispiele

Es empfiehlt sich u.a. Folgendes pro Sicherheitsstufe und verwendeter Technologie zu definieren:

- Rechte, Haftung und Pflichten des IdP und des E-ID-Dienstes
- Sicherheit bei der Weitergabe der Personaldaten des E-ID-Inhabers vom IdP an den E-ID-Dienst
- Sicherheit und Prüfung der Authentisierungsbestätigung des IdP an den E-ID-Dienst(Synonyme für diese Bestätigung sind Token und Claim)
- Registrierung des E-ID-Dienstes beim IdP
- Technologie bei der gegenseitigen Authentisierung
- Wechselspiel Authentisierung – Autorisierung
- Wie schnell ein E-ID-Dienst den IdP zu informieren hat, wenn ein Verdacht besteht, dass ein Missbrauch einer E-ID vorliegt, und umgekehrt. Letzteres hängt auch davon ab, wie lange eine Verbindung zwischen einen E-ID-Dienst und einem E-ID-Inhaber ohne nochmalige Authentisierung eines E-ID-Inhabers bestehen darf.

8.4 Zwischen 2 IdP

8.4.1 Interoperabilität

Gemäss Art. 18 Abs. 1 BGEID haben die IdP die Interoperabilität sicherzustellen. Der Umfang an Interoperabilität lässt sich aus dem Wortlaut des Gesetzes nicht ableiten. Dies wäre eher möglich, wenn eine Architektur und die dazugehörigen Prozesse definiert wären.

Das Gesetz ermächtigt den Bund, Vorschriften betreffend Interoperabilität zwischen den E-ID Systemen verschiedener IdP zu erlassen (Art. 18 Abs. 3 BGEID). Doch sollte das Erlassen der Vorschriften in Zusammenarbeit mit den möglichen IdP erfolgen.

SHOULD: Die Vorschriften zur Interoperabilität der E-ID-Systeme sollen in Zusammenarbeit mit den davon betroffenen IdP erarbeitet werden; dies in Form eines eCH-„Best Practices“.

Die Interoperabilität zwischen einem Schweizer IdP und einem IdP aus der EU kann aber die Verordnung nicht erfassen. Es empfiehlt sich im Sinne der Ökonomie, eine zur EU kompatible Vorschrift betreffend Interoperabilität der Schweizer E-ID-Systeme untereinander zu erlassen.

SHOULD: Beim Erarbeiten der Vorschriften soll darauf geachtet werden, dass die Vorschriften mit der EU (eIDAS) möglichst kompatibel sind.

8.4.2 Akzeptanz

IdP akzeptieren ihre E-ID-Systeme gegenseitig (Art. 18 Abs. 1 BGEID). Der Umfang der Akzeptanz geht aus dem Wortlaut des Gesetzes nicht hervor. Was sie dabei zum Erreichen der Interoperabilität zu akzeptieren haben, bleibt unklar, da wie bereits erwähnt der Umfang der Interoperabilität unbestimmt ist.

Aus dem Bestreben nach Interoperabilität sollten sich die Rechte und Pflichten des jeweiligen IdP, insbesondere die Haftung bei Nichterfüllen der Pflichten, herauskristallisieren.

Einerseits müssten die Rechte und Pflichten der IdP untereinander im Gesetz festgehalten werden (Art. 164 BV). Folglich kann hierzu der Bund keine Vorschriften erlassen.

Andererseits stellt sich die Frage nach dem zulässigen Haftungsausschluss beim Akzept. Daraus können sich Haftungsrisiken für den IdP ergeben. Die Risiken resultieren aus der „Haftungsdifferenz“ zwischen:

- der Haftung im Aussenverhältnis (z.B. gegenüber dem E-ID-Dienst) und
- der Möglichkeiten beim Regress (z.B. gegenüber dem anderen IdP).

MAY: Der Bestanteil der gegenseitigen Akzeptanz kann erarbeitet werden.

8.4.3 Mögliche Alternativen

Es stellt sich je nach Geschäftsmodell die Frage, ob ein E-Dienst nicht nur mit einem IdP, sondern mit allen anerkannten IdP eine Vereinbarung trifft; dies auf Basis einer standardisierten Vereinbarung.

Somit wäre eine Interoperabilität zwischen den IdP nicht erforderlich, was gegebenenfalls Kosten reduzieren könnte.

9 Bestimmungen in Zusammenarbeit mit Technologiepartnern

In diesem Kapitel werden Inhalte aufgegriffen, zu welchen der Bund Vorschriften erlassen darf, aber dies in Zusammenarbeit mit Privaten und den Kantonen erfolgen sollte.

9.1 Sicherheitsniveau

9.1.1 Ausgestaltung des Sicherheitsniveaus

Die prozessuale und technologische Ausgestaltung des Sicherheitsniveaus hängt primär davon ab, was die im Gesetz aufgestellte Anforderung konkret bedeutet. Z.B. wie hoher Schutz gegen Identitätsmissbrauch und Identitätsveränderung erreicht werden kann. Daraus sollten objektive, wenn möglich auch quantifizierbare Anforderungen resultieren.

Die Anforderungen wiederum bestimmen die Ausprägung der zugrunde liegenden Technologie und Prozesse. Es kann durchaus möglich sein, dass gewisse Technologien für ein entsprechendes Sicherheitsniveau unzureichend sind.

Es empfiehlt sich, die Ausgestaltung in öffentlicher Zusammenarbeit mit Fachkräften aus der Privatwirtschaft zu erstellen, z.B. in Form eines eCH Standards, welcher dann in einer TAV entsprechend referenziert wird.

9.1.2 Anforderungen an den E-ID-Dienst

Ein Identitätsmissbrauch kann auch durch einen E-ID-Dienst verursacht werden. Folglich sollten sich die Sicherheitsniveaus auch durch den Betrieb eines E-ID-Dienstes unterscheiden. Der Betrieb des E-ID-Dienstes wird aber bei der Ausgestaltung des Sicherheitsniveaus in Artikel 4 BGEID nicht erwähnt. Folglich lässt sich dies nicht über die Verordnung regeln.

SHOULD: Die Sicherheitsvorkehrung für den Betrieb eines E-ID-Dienstes, wie die Ausgestaltung der Webseite, die Technologie für das Anmelden beim E-ID-Dienst und deren Ausprägung (engl. Profile) sollen pro Sicherheitsstufe beschrieben werden.

Cross-Site Request Forgery (CSRF) und Cross-Site Scripting (CSS) sind eine der gängigsten Angriffe für den Identitätsdiebstahl in der IT. Z.B. im RFC Standard OAUTH 2.0 wird empfohlen, sich gegen die CSRF Angriffe zu schützen, und dabei wird erläutert, was geschehen kann, wenn ein CSS-Angriff erfolgreich ist.

9.1.3 Höchstmöglicher Schutz

Durch Abänderung von Art. 1 Abs. 2 Bst. a der E-ID-Gesetzesvorlage hat der Nationalrat sich klar dazu bekannt, dass Sicherheit Priorität hat, indem er das Wort „einfach“ in Art. 1 Abs. 2 Bst. a in der Sommersession 2019 streichen liess, siehe Geschäft 18.049n Sommersession 2019. Folglich sind Einfachheit und Benutzerfreundlichkeit von untergeordneter Bedeutung. Diese Änderung wurde ohne Gegenvorschlag und somit ohne Beanstandung vom Ständerat akzeptiert. Siehe hierzu 18.049n, e-parl 05.06.2019, Sommersession.

Nun stellt sich die Frage, wie dem Willen des Parlaments bei der Realisierung der höchstmöglichen Sicherheit nach Art. 4 Abs. 1 Bst. c BGEID entsprochen wird. Wie aus Publikatio-

nen hervorgeht, ist offensichtlich, dass eine zentrale Authentisierung wie bei einem Single Sign-On Ansatz dies nicht erfüllen kann, siehe z.B. FORSTER/MUSTER.

Es empfiehlt sich, die Ausgestaltung der elektronischen Identifizierung für den höchstmöglichen Schutz in öffentlicher Zusammenarbeit mit Fachkräften aus der Privatwirtschaft und der Lehre zu erstellen, z.B. in Form eines eCH Standards, welcher fortwährend angepasst und dann in einer TAV entsprechend referenziert wird.

Anmerkung zu Querverweise auf Standards in Vorschriften: In Art. 5 bei VVK-EDI wird auf den eCH-Standard 0064 verwiesen, in TAV auf internationale Standards.

9.1.4 Jeweiliger Stand der Technik

Bei der Ausgestaltung der Sicherheitsstufen ist der jeweilige Stand der Technik zu berücksichtigen (Art. 4 Abs. 4 BGEID). Den jeweiligen Stand der Technik ohne das Hinzuziehen von Lehre und Technologiepartner zu erfassen, gestaltet sich schwierig.

9.1.5 Zu erwartende Schwierigkeiten bei der Umsetzung

Dieser Aspekt wurde bereits in früheren Kapiteln erwähnt, siehe hierzu z.B. Kapitel 7.3 „Wirtschaftlichkeit in der Umsetzung“.

9.2 Interoperabilität zwischen IdP und IdP

Siehe dazu Kapitel 8.4 „Zwischen 2 IdP“.

9.3 Wahl der Technologie

Das Gesetz und die darauf gestützten Verordnungen beachten den Grundsatz der Technologieneutralität (Art. 1 Abs. 3 BGEID). Zudem ist dem jeweiligen Stand der Technik beim Erlass der Verordnung zu den Sicherheitsstufen Rechnung zu tragen (Art. 4 Abs. 4 BGEID). Im Sinne der Wirtschaftlichkeit empfiehlt es sich, sich auf eine Auswahl an Technologien zu einigen, insbesondere unter denjenigen, welche eine E-ID für das elektronische Identifizieren zu akzeptieren haben und eine E-ID herausgeben (IdP). Anmerkung:

> Nicht nur bei Erlass einer Verordnung ist der jeweilige Stand der Technik zu berücksichtigen. Vielmehr wäre auch die Verordnung zwingend und automatisch anzupassen, sobald sich der Stand der Technik in relevantem Ausmass weiter entwickelt bzw. ändert. Darauf müsste aber schon in der Verordnung ausdrücklich hingewiesen werden – ausser man würde eine entsprechende Verordnung als «Sunset law» kreieren, d.h. sie gilt nur für z.B. drei Jahre und muss dann (erneut z.B. für zwei Jahre) bestätigt oder aber überarbeitet werden. Dies ist bislang das aber kein Begriff aus der Schweizer Rechtspraxis), vgl. dazu Auslaufklausel:
>
> https://de.wikipedia.org/wiki/Auslaufklausel_(Recht).
>
> Es stellt sich dabei folgende Frage: Falls die Verordnung nicht angepasst wird, und entsteht ein Schaden, weil die geltenden Verordnungsbestimmungen nicht den neueren Entwicklungen angepasst worden sind, wer haftet dann?

SHOULD: Man soll sich auf eine Auswahl einzusetzender Technologien einigen.

10 Schnittstelle zu anderen Vorschriften

10.1 ZertES

10.1.1 Identifizieren

Mit der Einführung des BGEID ist auch folgende Ergänzung beim ZertES angedacht (Art. 9 Abs. 1^{bis}):

> Wird der Identitätsnachweis durch eine E-ID des Sicherheitsniveaus substanziell nach dem BGEID vom 27. September 2019 erbracht, so muss die betreffende Person nicht persönlich erscheinen.

Hierzu stellt sich für eine nach ZertES anerkannten Anbieterin von Zertifizierungsdiensten folgende Frage bei der Ausstellung eines nach ZertES geregelten Zertifikats: Wie ist die Haftung im Innenverhältnis, d.h. im Verhältnis gegenüber dem IdP, und besteht daraus ein Haftungsrisiko? Dazu folgendes Beispiel:

> Die nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten stellt ein nach ZertES geregeltes Zertifikat vermeintlich für die Person A aus. Dies, weil, die Identifizierung von Person A beim IdP nicht ausreichend sorgfältig geschah oder die elektronische Identifizierung nicht ausreichend sicher war.
>
> In Wirklichkeit hat aber Person B den privaten Schlüssel des dazu passenden geregelten Zertifikats inne. Person B fügt nun Person C einen Schaden zu, weil sich C auf den Inhalt des nach ZertES geregelten Zertifikats verlassen hat.

Es empfiehlt sich, weiterhin am persönlichen Erscheinen festzuhalten.

10.1.2 Einbinden der E-ID-Nr. ins geregelte Zertifikat

Falls eine nach BGEID konforme Authentisierung auf Basis eines nach ZertES geregelten Zertifikats erfolgen soll, dann drängt sich wegen der Sicherheit auf, die E-ID-Nr. ins Zertifikat aufzunehmen. Nun stellt sich die Frage, ob in Art. 7 ZertES die Aufzählung abschliessend ist, welche Attribute ins geregelte Zertifikat aufgenommen werden können und müssen.

Es mag auch bei gewissen Geschäftsvorfällen sinnvoll sein, dass die E-ID-Nr. beim qualifizierten Zertifikat eingefügt wird.

SHOULD: Es soll abgeklärt werden, ob die Aufzählung der Attribute für das geregelte qualifizierte Zertifikat (Art. 7 und 8 ZertES) abschliessend ist.

10.2 UIDG

MAY: Die UID-Nr. kann in die (nach ZertES geregelten) Server Zertifikate des E-ID-Dienstes und E-ID-System aufgenommen werden.

10.3 eIDAS

Zur Schnittstelle mit eIDAS siehe Kapitel 8.4 „Zwischen 2 IdP“ und Kapitel 3.3 „eIDAS“.

11 Beispiele

In diesem Kapitel werden zur Illustration einige Beispiele zu einzelnen, d.h. folglich nicht zu allen Empfehlungen in den jeweiligen Kapiteln etwas detaillierter skizziert.

11.1 Authentisieren des E-ID-Systems und des E-ID-Dienstes

Das Authentisieren des E-ID-Systems wurde u.a. im Kapitel 8.1.1 „Authentisierung des E-ID-Systems“ thematisiert. Hier eine Auswahl dessen, was dabei festgelegt werden sollte.

- Serverzertifikat. U.a. wer stellt es aus, welchen Inhalt (z.B. die UID-Nr.) und welche Verlässlichkeit (z.B. ein nach ZertES geregeltes Zertifikat) weist es auf?
- Schutz der Kommunikation (z.B. TLS 1.x). und welche Cipher Suites. Eventuell eine Negativempfehlung für TLS 1.3 und für die Verschlüsselung AES im Galois Countermode (GCM). Wahl des Schlüsseleinigungsverfahrens.
- Was der E-ID-Inhaber dabei kontrollieren (können) muss.

11.2 Technologie für das Zusammenspiel unter den Parteien

Hier solle eine Auswahl der Technologien festgehalten werden, welche für den Aufbau der Kommunikation verwendet wird, wie OpenID Connect, Web Services. Dies kann unter Umständen auch vom Sicherheitsniveau abhängen.

11.3 Verlässlichkeit der Authentisierungsbestätigung

Zur Verlässlichkeit der Authentisierungsbestätigung könnte u.a. Folgendes festgelegt werden.

- Typ, wie JSON, SAML (Eventuell abhängig vom Sicherheitsniveau)
- Verlässlichkeit des Schutzes (Signatur, Art der Signatur)
- Struktur, z.B. bei SAML das Schema, bei JSON und SAML Restriktionen beim Zeichenformat

11.4 Ausgestaltung der Webseite

Hier könnte z.B. zur Verhinderung von Cross-Site Attacken festgelegt werden,

- worauf die Eingaben vom Client zu prüfen sind und was akzeptiert oder nicht akzeptiert werden darf.
- was als Output an den Client gesendet werden darf.
- wie lange ein am E-ID-Dienst angemeldeter E-ID-Inhaber als authentisiert gilt.

12 Weiteres Vorgehen

In diesem Dokument ist eine Reihe von zukünftigen Arbeiten aufgeführt und deren Umsetzung empfohlen. Diese Aufgaben sind zu priorisieren. Deren Erledigung erfordert zum Teil zwingend das Mitwirken wichtiger Akteure zu diesem Thema, wie

- IdP (Anbieter von elektronischen Identitätsdienstleistungen),
- Anbieter von E-ID-Diensten, insbesondere Vertreter kantonaler Ämter, welche eine E-ID zu akzeptieren haben,
- Mitarbeiter der Bundesverwaltung, welche die Gesetzesvorlage ans Parlament ausgearbeitet haben und sich für die Verordnung verantwortlich zeichnen,
- Vertreter der Kantone.

Weiter soll eruiert werden, welche eCH-Standards angepasst und ob neue Standards/“Best Practices“ geschaffen werden sollen.

Anmerkung zum Status eines eCH-Standards: Gemäss einer öffentlich-rechtlichen Vereinbarung vom 20. Dezember 2019 zwischen Bund und Kantonen (ÖRv, Kapitel 1.4):

> [1] Bei der Erarbeitung von E-Government-Leistungen oder Teilen davon orientieren sich die Gemeinwesen an internationalen oder nationalen Standards.
>
> [2] Als nationale Standards gelten grundsätzlich diejenigen des Vereins eCH. Die Gemeinwesen erklären diese in der Regel für verbindlich. Dies gilt insbesondere bei Beschaffungen und Lösungsentwicklungen.
>
> [3] Die Gemeinwesen wirken im Rahmen ihrer Möglichkeiten bei der Erarbeitung von Standards des Vereins eCH mit.

Beispiel für ein erfolgreiches Zusammenspiel bei der Erarbeitung von Standards zwischen Bund und Kantonen (ohne gesetzliche Grundlage) sind die eCH-Standards zur Unternehmensidentifikation (UID) eCH-0097 und eCH-0098.

13 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtig-

keit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

14 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

15 Referenzen & Bibliographie

15.1 Erlasse

BGEID:	Bundesgesetzüber über elektronische Identifizierungsdienste vom 27. September 2019
BV	Schweizerische Bundesverfassung vom 18. April 1999, SR 101
eIDAS	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
OR	Schweizerisches Obligationenrecht vom 30. März 1911, SR 220
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032.1
UIDG	Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010, SR 431.03

VVK-EDI	Verordnung des EDI über die technischen und grafischen Anforderungen an die Versichertenkarte für die obligatorische Krankenpflegeversicherung (SR 832.105.1)
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032
ZertES	Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.03)

15.2 Rechtliches Hintergrundmaterial

18.049n, e-parl 05.06.2019 11:15, Bundesgesetz über elektronische Identifizierungsdienste Sommer- und Herbstsession 2019

ÖRv, Öffentlich-rechtliche Rahmenvereinbarung über die E-Government-Zusammenarbeit in der Schweiz 2020 vom 20. Dezember 2019, BBL 8729 ff.

15.3 Fachliteratur

CLAIMS	Dominick Baier et. al, A guide to Claims-Based Identity Access Control, Microsoft, 2nd Edition, 2011. Kann vom Internet heruntergeladen werden.
EXCESS XSS	Excess XSS, A comprehensive tutorial on cross-site scripting, Created by Jakob Kallin and Irene Lobo Valbuena, https://excess-xss.com/
HÄFELIN/HALLER/KELLER	Ulrich Häfelin/Walter Haller/Helen Keller, Schweizerisches Bundesstaatsrecht, 8. Auflage, Schulthess Verlag, 2012.
HOLLIGER	Eugénie Holliger-Hagmann, Produktesicherheitsgesetz PrSG, Schulthess Verlag 2010
LUTERBACHER	Thierry Luterbacher, Fischer Willi (Hrsg.), Haftpflichtkommentar, Dike Verlag, 2016
STUTTARD/PINTO	Darfydd Stuttard, Marcus Pinto, Hacker's Handbook, 2nd edition, Wiley, 2011
ZALEWSKI	Michal Zalewski, Tangled Web, dpunkt.verlag, 2013

15.4 Wissenschaftliche Publikationen

BREAK SAML	Juray Somorovsky, Andreas Mayer at al, On Breaking SAML: Be Whoever You Want to be, https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final91.pdf
FORSTER/MUSTER	Florian Forster, Daniel Muster, Vergleich von online Authentisierungen im eGov Bereich, V.1.1, 13. März 2020, http://www.it-rm.ch/e-id-gesetzesvorlage.html Advanced Encryption Standard

MLADENOW-MAINKA Vladislav Mladenov, Christian Mainka, OpenID Connect Security Consideration, Ruhr Universität Bochum, 2017, https://www.nds.ruhr-uni-bochum.de/media/ei/veroeffentlichungen/2017/01/13/OIDCSecurity_1.pdf

15.5 Standards

15.5.1 IETF Standards (www.ietf.org)

RFC 4346	TLS v.1.1
RFC 5246	TLS v. 1.2
RFC 5849	OAUTH The OAuth 1.0 Protocol
RFC 6749	OAUTH The OAuth 2.0 Authorization Framework
RFC 8446	TLS v. 1.3

15.5.2 eCH (www.ech.ch)

eCH-0048	PKI-Zertifikatsklassen
eCH-0064	Spezifikationen für das System Versichertenkarte
eCH-0097	Datenstandard Unternehmensidentifikation
eCH-0098	Datenstandard Unternehmensdaten
eCH-0219	IAM Glossar
eCH-0220	Bewahrung der Gültigkeit elektronischer Signaturen auf Dokumenten
eCH-0225	Identity Federation - Implementierung mit OIDC

15.5.3 W3C (www.w3c.org)

SOAP	Simple Object Access Protocol v. 1.2

15.5.4 OASIS (www.oasis.org)

SAML	Security Assertion Markup Language (SAML) V2.0

15.5.5 OpenID Foundation (https://openid.net/foundation)

OpenID Connect	OpenID Connect Core 1.0 incorporating errata set 1

15.5.6 NIST (www.nist.gov)

AES	Advanced Encryption Standard, FIPS) - 197
GCM	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D

Anhang A – Mitarbeit & Überprüfung

Dr. iur Esther Hefti, Staatskanzlei des Kantons Zürich

Anhang B – Glossar

Authentisieren	Synonym für elektronische Identifizierung. Zum Begriff Authentisieren, siehe eCH-0219
Cross-Site Request Forgery	Siehe XSRF
Cross-Site Scripting	Siehe dazu XSS. Den Browser dazu veranlassen
Elektronische Identifizierung	Synonym für Authentisieren
IdP	Identity Provider = Anbieterin von elektronischen Identitätsdienstleistungen
XSRF	Den Browser dazu veranlassen, einen Befehl (http-Request) zu senden, welcher vom User nicht gewollt ist, und Daten auf dem Server in einer Art und Weise zu ändern, welche vom User nicht beabsichtigt ist, z.B. unbeabsichtigter Geldtransfer. Siehe Cross-Site Request Forgery (CSRF), siehe dazu STUTTARD/PINTO
XSS	Synonym für Cross-Site Scripting. XSS ist eine Attacke, Programme in einer geladenen HTML-Webseite auszuführen zu lassen, welche vom Hersteller der Webseite nicht vorgesehen ist. Dabei wird u.a. beabsichtigt sicherheitsrelevante Informationen wie Cookies zu stehlen. Siehe dazu https://excess-xss.com/ und STUTTARD/PINTO

Anhang C – Abkürzungen

Abs.	Absatz
AES	Advanced Encryption Standard
Art.	Artikel
BBl	Bundesblatt
BGEID	siehe Kapitel 15.1 „Erlasse“
Bst.	Buchstabe
BV	siehe Kapitel 15.1 „Erlasse“
CSRF	Cross-Site Request Forgery
CSS	1) Cascading Style Sheets Language 2) Cross-Site Scripting
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
E-ID	Elektronische Identität
eIDAS	siehe Kapitel 15.1 „Erlasse“

EIDCOM	Eidgenössische E-ID-Kommission
ff.	folgende
GCM	Galois Counter Mode, siehe Kapitel 15.5.6 „NIST (www.nist.gov)“
IAM	Identity and Access Management
IdP	Identity Provider
JSON	JavaScript Object Notation
OAUTH	Open Authorization, siehe Kapitel 15.5.1 „IETF Standards (www.ietf.org)“
OIDC	OpenID Connect
OR	siehe Kapitel 15.1 „Erlasse“
ÖRv	Siehe Kapitel 15.2 „Rechtliches Hintergrundmaterial“
resp.	respektive
Rz	Randziffer
SAML	Security Assertion Markup Language (SAML) v2.0
SOAP	Service Oriented Application Protocol oder Simple Object Access Protocol
SR	Systematische Rechtssammlung
TAV	Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032.1
TAV	siehe Kapitel 15.1 „Erlasse“
TLS	Transport Layer Security
u.a.	unter anderem
UID	Unternehmensidentifikation
UIDG	siehe Kapitel 15.1 „Erlasse“
VZertES	siehe Kapitel 15.1 „Erlasse“
W3C	World Wide Web Consortium
XSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting
z.B.	zum Beispiel
ZertES	siehe Kapitel 15.1 „Erlasse“