



Bern, 30. Juni 2021

E-Signatur für verwaltungsinterne Dokumente

Bericht in Erfüllung des Postulats
18.3502 Dobler vom 12. Juni 2018

Inhaltsverzeichnis

1	Parlamentarischer Auftrag.....	3
1.1	Postulat «E-Signatur für verwaltungsinterne Dokumente»	3
1.2	Vorgeschichte	3
2	Erfordernis einer Signatur – Rechtliche Vorgaben.....	4
2.1	Einleitung.....	4
2.2	Definition der elektronischen Signatur.....	4
2.3	Die bundesverwaltungsintern verwendeten elektronischen Zertifikate	5
2.4	Einsatzbereiche der eigenhändigen Unterschrift	6
2.4.1	Elektronische Formen	6
2.4.2	Schriftlichkeit.....	7
2.4.3	Formvorschriften für Verträge	7
2.4.4	Exkurs: Verträge bei Beschaffungen des Bundes	9
2.4.5	Exkurs: Verfügungen und Rechnungen mit Verfügungscharakter	11
2.4.6	Exkurs: Bundesratsgeschäfte	12
2.4.7	Exkurs: Personalwesen und Personensicherheitsüberprüfungen	13
2.4.8	Exkurs: Legalisationen.....	16
3	Technische Analyse / Rahmenbedingungen.....	17
3.1	Elektronische Geschäftsverwaltung in der Bundesverwaltung.....	17
3.2	Elektronische Bestätigungen in Acta Nova	17
3.3	Elektronische Signatur in Acta Nova.....	17
4	Zusammenfassung	18
4.1	Mehrwert der elektronischen Bestätigung im Vergleich zur elektronischen Signatur..	18
4.2	Rechtliche «Hindernisse» oder anderer Handlungsbedarf	18
5	Schlussfolgerungen	19

E-Signatur für verwaltungsinterne Dokumente

1 Parlamentarischer Auftrag

1.1 Postulat «E-Signatur für verwaltungsinterne Dokumente»

Am 12. Juni 2018 reichte Nationalrat Marcel Dobler das Postulat 18.3502 «E-Signatur für verwaltungsinterne Dokumente» mit folgendem Wortlaut ein:

«Der Bundesrat wird beauftragt, vertiefte Abklärungen für die standardmässige Einführung der digitalen Signatur bei rechtlich zwingendem Erfordernis einer Unterschrift auf verwaltungsinternen Dokumenten zu treffen und diese in einem Bericht zu veröffentlichen.»

Das Postulat wird wie folgt begründet: «Die Motion 18.3008, *«Bundesverwaltungsinterne Dokumente standardmässig digital signieren»*, forderte, so rasch wie möglich die rechtlichen Grundlagen zu schaffen, wonach alle bundesverwaltungsinternen Dokumente, wo ein rechtlich zwingendes Erfordernis für eine Signatur besteht, standardmässig digital anstatt handschriftlich zu signieren sind.

In allen übrigen Fällen soll die Bundesverwaltung die Möglichkeiten der prozessgesteuerten Dokumentation der Bestätigungen, welche insbesondere das neue GEVER-Standardprodukt Acta Nova bietet, nutzen. Der Bundesrat konstatierte in seiner Antwort auf diese Motion, dass er zwar beabsichtigt, bundesverwaltungsintern die Möglichkeiten der prozessgesteuerten Dokumentation der Bestätigungen, die insbesondere das neue GEVER-Standardprodukt Acta Nova bietet, zu nutzen.

Der Bundesrat vermerkte aber auch, dass es für die flächendeckende Einführung der E-Signatur weiterführender Abklärungen bedürfen würde. Diese vertieften Abklärungen sollen nun aufgrund des vorliegenden Postulates erfolgen. Denn die E-Signatur hilft bei der Digitalisierung der Bundesverwaltung, eliminiert den bisherigen Medienbruch, leistet einen entscheidenden Beitrag zur Akzeptanz der digitalen Signatur und steigert die Kosteneffizienz der Bundesverwaltung.

Die Rechtmässigkeit¹ eines signierten Dokumentes kann jederzeit mit dem Validator.ch-Service der Bundesverwaltung umfassend und abschliessend überprüft werden. Die Erstellung einer digitalen Signatur wie auch die Prüfung mit dem Validator ist einfach und erfordert kein technisches Verständnis.»

Am 29. August 2018 beantragte der Bundesrat die Annahme des Postulats. Der Nationalrat folgte diesem Antrag und nahm das Postulat am 28. September 2018 an.

1.2 Vorgeschichte

Mit der Motion 18.3008 Dobler vom 26. Februar 2018 wurde der Bundesrat eingeladen, so rasch wie möglich die rechtlichen Grundlagen für die elektronische Signatur von bundesverwaltungsinternen Dokumenten zu schaffen.

Der Bundesrat beantragte am 1. Juni 2018 die Ablehnung der Motion. Er begründete dies damit, dass bundesverwaltungsinterne Dokumente, die der Zustimmung bedürfen, mit der elektronischen Geschäftsverwaltung schon heute elektronisch signiert oder mit «Genehmigung» weitergeleitet oder bestätigt werden können. Die technischen Voraussetzungen dafür würden bereits bestehen und ab 2020 mit der Einführung einer Standardlösung für die elektronische Geschäftsführung (GEVER) für rund 30 000 Arbeitsplätze in der zentralen und eines Teils der dezentralen Bundesverwaltung gegeben sein.

Der Motionär reichte am 12. Juni 2018 das oben erwähnte Postulat 18.3502 ein und zog die Motion 18.3008 in der Folge am 10. September 2018 zurück. Abgesehen von den Auslandsvertretungen des EDA ist ab August 2021 Acta Nova als elektronisches Geschäftsverwaltungssystem (GEVER) in der gesamten zentralen Bundesverwaltung eingeführt.

¹ Anmerkung: Der Validator bestätigt, dass die elektronische(n) Signatur(en) des Dokuments gültig bzw. technisch valide sind. Der Validator sagt nichts über die inhaltliche Rechtmässigkeit des Dokuments aus. Bei einem elektronisch signierten Strafregistrauszug wird z.B. vom Validator geprüft, ob der Strafregistrauszug qualifiziert signiert und mit einem gültigen Zeitstempel versehen ist, und ob er mit einem vom Verantwortlichen des Strafregisters für diesen Zweck vorgesehenen Zertifikat signiert wurde. Bei einem qualifiziert signierten Dokument kann der Validator bestätigen, dass die elektronische Unterschrift den Anforderungen von Art. 14 Abs. 2^{bis} des Obligationenrechts (eigenhändige Unterschrift) entspricht.

E-Signatur für verwaltungsinterne Dokumente

2 Erfordernis einer Signatur – Rechtliche Vorgaben

2.1 Einleitung

Aus der Vorgeschichte und dem im Postulat formulierten Auftrag wird deutlich, dass einerseits zu klären ist, für welche *bundesverwaltungsinternen* Dokumente eine eigenhändige (handschriftliche) Unterschrift überhaupt nötig bzw. *rechtlich zwingend* ist. Andererseits, ob in diesen Fällen die handschriftliche Unterschrift durch eine elektronische Signatur (im Postulat als E-Signatur bezeichnet) *ersetzt* werden kann und ggf. welche Art bzw. Qualität von elektronischer Signatur dafür notwendig ist.

In der Motion 18.3008 «Bundesverwaltungsinterne Dokumente standardmässig digital signieren» wurde von bundesverwaltungsinternen und im Postulat 18.3502 «E-Signatur für verwaltungsinterne Dokumente» von verwaltungsinternen Dokumenten gesprochen.

In diesem Bericht wird primär auf interne Dokumente der zentralen Bundesverwaltung (kurz: bundesverwaltungsinterne Dokumente) eingegangen, wenn auch an vielen Stellen auf die Sachlage bei Dokumenten mit Adressaten ausserhalb der zentralen Bundesverwaltung hingewiesen wird.

Der Bundeskanzler ist zuständig für die Festlegung der Standarddienste mit Bezugswang für die Verwaltungseinheiten (VE) im Geltungsbereich der Verordnung über die digitale Transformation und die Informatik (VDTI)². Die Standarddienste erbringen Leistungen zentral, die vielfach verwendet werden, und gleiche oder ähnliche Bedürfnisse befriedigen. Solche Standarddienste sind z. B. die Geschäftsverwaltung (GEVER) und der Standarddienst IAM, der die Signaturdienste beinhaltet.

2.2 Definition der elektronischen Signatur

Während es nur eine Art der handschriftlichen Unterschrift gibt, gibt es bei den elektronischen Signaturen verschiedene Arten bzw. Abstufungen. Diese werden in Artikel 2 des Bundesgesetzes über die elektronische Signatur (ZertES)³ beschrieben.

Dabei lassen sich die folgenden vier elektronischen Signaturen und das geregelte elektronische Siegel unterscheiden (wobei das geregelte elektronische Siegel in technischer Hinsicht auch eine elektronische Signatur ist, aber mangels einer direkten Zuordnung zu einer natürlichen Person nicht im Rechtsinn als Signatur bezeichnet wird):

- **(einfache) elektronische⁴ Signatur:** Diese Daten sind *keiner Person* zugeordnet und ermöglichen daher keine Identifizierung von Personen.

«Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen» (Art. 2 Bst. a ZertES)

- **fortgeschrittene elektronische Signatur (Art. 2 Bst. b ZertES):** Dies ist eine elektronische Signatur, die folgende Anforderungen erfüllt: 1. sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet, 2. sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers, 3. sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann, 4. sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Alle Mitarbeitenden der zentralen Bundesverwaltung verfügen über ein fortgeschrittenes Zertifikat auf ihrer Smartcard, mit dem eine fortgeschrittene elektronische Signatur auf einem Dokument angebracht werden kann.

² SR 172.010.58

³ SR 943.03

⁴ Das vorliegende Postulat verlangt vertiefte Abklärungen für die standardmässige Einführung der *digitalen* Signatur, während das ZertES den Begriff der *elektronischen* Signatur verwendet. Im vorliegenden Bericht wird der gesetzliche Begriff der elektronischen Signatur verwendet, davon ausgehend, dass die Begriffe *digital* und *elektronisch* synonym verwendet werden können.

E-Signatur für verwaltungsinterne Dokumente

- **geregelte elektronische Signatur (Art. 2 Bst. c ZertES):** eine fortgeschrittene elektronische Signatur, die unter Verwendung *einer sicheren Signaturerstellungseinheit* nach Artikel 6 ZertES erstellt wurde und auf einem geregelten, auf eine natürliche Person ausgestellten und zum Zeitpunkt der Erzeugung der elektronischen Signatur gültigen Zertifikat beruht.

Die Swiss Government PKI (SGPKI) gibt derzeit keine geregelten persönlichen Signaturen aus. (Das Signaturzertifikat Klasse B auf der Smartcard der Mitarbeitenden des Bundes erlaubt nur die Erstellung von fortgeschrittenen persönlichen elektronischen Signaturen und nicht von nach ZertES geregelten persönlichen elektronischen Signaturen).

- **qualifizierte elektronische Signatur (Art. 2 Bst. e ZertES):** Ein qualifiziertes Zertifikat darf nur auf eine natürliche Person ausgestellt werden und muss einen Eintrag enthalten, wonach es nur für die elektronische Signatur bestimmt ist (Art. 8 Abs. 1 und 2 ZertES). Zudem ist der Hinweis ins Zertifikat aufzunehmen, dass es sich um ein qualifiziertes Zertifikat handelt (Art. 8 Abs. 3 ZertES).

Die qualifizierte elektronische Signatur hat im Grundsatz dieselben Eigenschaften wie die *fortgeschrittene elektronische Signatur* nach Artikel 2 Buchstabe b ZertES, muss jedoch unter Verwendung einer sicheren Signaturerstellungseinheit nach Artikel 6 ZertES erstellt werden und beruht auf einem *qualifizierten Zertifikat*⁵.

Diese Voraussetzungen werden in der Bundesverwaltung nur von den qualifizierten Signaturzertifikaten (gemäss BIT «Zertifikat der Klasse A – qualifiziert») für eine natürliche Person eingehalten.

- **geregeltes elektronisches Siegel (Art. 2 Bst. d ZertES):** Das entsprechende Zertifikat wird nicht auf den Namen einer Person, sondern auf den Namen einer Organisation (Behörde, Unternehmen usw.) ausgestellt. Das geregelte elektronische Siegel (beim Bundesamt für Informatik [BIT] als geregeltes Behördenzertifikat bezeichnet und auf Smartcard wie auch serverbasiert erhältlich) ist dafür gedacht, die Herkunft und die Integrität eines Dokumentes gegenüber Dritten zu bestätigen, und kann so auch von Einheiten der Bundesverwaltung dazu verwendet werden, ausgehende Dokumente (u. a. auch Verfügungen) zu siegeln.

Dieses hat im Grundsatz⁶ dieselben Eigenschaften wie die *fortgeschrittene elektronische Signatur* (Art. 2 Bst. b ZertES), muss jedoch unter Verwendung einer sicheren Siegelerstellungseinheit (Art. 6 ZertES) erstellt werden und beruht auf einem geregelten, auf eine UID-Einheit nach Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG)⁷ ausgestellten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat⁸. Zudem ist der Hinweis ins Zertifikat aufzunehmen, dass es sich um ein geregeltes Zertifikat handelt (Art. 7 Abs. 2 Bst. b ZertES).

2.3 Die bundesverwaltungsintern verwendeten elektronischen Zertifikate

Bundesverwaltungsintern wird – sofern elektronisch gearbeitet wird und überhaupt elektronische Signaturen zum Einsatz kommen – mehrheitlich die fortgeschrittene elektronische Signatur nach Artikel 2 Buchstabe b ZertES genutzt. Alle Mitarbeitenden der Bundesverwaltung können diese auf ihrer Smartcard nutzen. Die Smartcard beinhaltet folgende «Zertifikate der Klasse B»:

- **Fortgeschrittenes Signaturzertifikat** zum Signieren von Dokumenten (primär PDF) und E-Mail. Dazu sind eine Signaturanwendung wie der noch in der ganzen Bundesverwaltung installierte Open eGov LocalSigner oder die neuen serverbasierten Signatordienste und (für E-Mail) Outlook notwendig.

⁵ Ein qualifiziertes Zertifikat ist nach Art. 2 Bst. h ZertES ein geregeltes Zertifikat nach Buchstabe g, welches die Anforderungen nach Art. 8 ZertES erfüllt. (vgl. dazu die in Fussnote 3 genannten Zertifikatstyp-Informationen des BIT).

⁶ Die im ZertES aufgeführten Anforderungen an die Identifizierung der Inhaberin des entsprechenden geregelten Zertifikats gehen aber weit über diejenigen für ein fortgeschrittenes Zertifikat hinaus.

⁷ SR 431.03

⁸ Die in der zentralen Bundesverwaltung ausgegebenen Zertifikate für elektronische Siegel werden in der Bundesverwaltung als Klasse A Signaturzertifikat für (nicht ganz zutreffend) eine juristische Person oder als geregeltes Behördenzertifikat bezeichnet (vgl. dazu die Informationen des BIT zu den Zertifikatstypen, www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki/zertifikatstypen/klasse-a/Geregelte-Behoerdenzertifikate.html).

E-Signatur für verwaltungsinterne Dokumente

- *Authentifizierungszertifikat*, das die Person identifiziert und deren Zugriff zum Netz der Bundesverwaltung und zu den darin befindlichen Infrastrukturen und (Fach-) Anwendungen mit einer 2-Faktor-Authentifizierung erlaubt bzw. steuert.
- *Verschlüsselungszertifikat* zur Verschlüsselung von Dokumenten und E-Mails.

Die vergleichsweise kleine Anzahl von unterschiftsberechtigten Mitarbeitenden der Personaldienste und die unterschiftsberechtigten Vorgesetzten aller Verwaltungseinheiten (VE) der Bundesverwaltung können zusätzlich ein qualifiziertes Signaturzertifikat (Klasse A) beantragen. Technisch bedarf es dazu entweder einer zweiten Smartcard⁹ in einem zusätzlichen Kartenleser (meist ein USB-Stick) oder ein serverbasiertes qualifiziertes Signaturzertifikat (Klasse A) für natürliche Personen, auf das die entsprechend Unterschiftsberechtigten über ihr Authentifizierungs-Zertifikat zugreifen. Zum Anbringen einer qualifizierten Signatur auf einem Dokument (PDF) bedarf es im letzteren Fall der entsprechenden Anwendungen der Signaturdienste.

Das fortgeschrittene elektronische Signaturzertifikat (Klasse B) der Mitarbeitenden der Bundesverwaltung verfügt über eine sehr hohe Qualität, da sich einerseits der zugehörige Signaturschlüssel auf der Smartcard befindet (und so nicht kopiert werden kann) und andererseits sowohl das Signaturzertifikat als auch jeweils das Verschlüsselungs- und Authentisierungszertifikat nur gegen eine strenge Identifikation mit Pass oder Identitätskarte an die Mitarbeitenden ausgegeben wird. Damit erzeugte Unterschriften verfügen damit über einen *sehr hohen Beweiswert*, obwohl mit ihnen nicht das Formerfordernis der einfachen Schriftlichkeit nach dem Obligationenrecht (OR, vgl. Ziff. 2.4.2) erfüllt werden kann.

2.4 Einsatzbereiche der eigenhändigen Unterschrift

2.4.1 Elektronische Formen

Im Rahmen der Klärung der Frage, welche bundesverwaltungsinternen Dokumente in Papierform *zwingend eigenhändig* und damit in elektronischer Form auch *zwingend qualifiziert* unterschrieben werden müssen, hat sich gezeigt, dass es diesbezüglich nur vereinzelt rechtliche Vorgaben gibt. Es ist daher davon auszugehen, dass bei Dokumenten, die nur bundesverwaltungsintern zirkulieren, nur in seltenen Fällen qualifizierte elektronische Signaturen auf Dokumenten (PDF) notwendig sind.

Dies bedeutet, dass in den allermeisten Fällen bei bundesverwaltungsinternen Dokumenten, die im GEVER-System oder in ähnlichen Fachanwendungen (z. B. SAP-ERP im Beschaffungs-, Finanz- und Personalbereich) erstellt und bearbeitet werden, anstelle einer elektronischen Signatur des Dokuments mit den *sogenannten GEVER-Bestätigungsfunktionen zum Visieren und Genehmigen* gearbeitet werden kann. Da die visierenden und genehmigenden Personen im GEVER-System über ihr Authentifizierungszertifikat auf der Smartcard (2-Faktor Authentifizierung mit Zertifikat der Klasse B¹⁰) angemeldet sind, sind die als verantwortlich zeichnenden Personen und der Zeitpunkt jederzeit mit Sicherheit über die Metadaten von GEVER-, E-Mail- oder Fachapplikationen nachvollziehbar.

Auch das SAP ERP ist ein revisionssicheres System, bei dem für die internen Dokumente eine elektronische Signatur nicht benötigt wird, da die entsprechenden Freigaben in den Workflows analog zum GEVER-System im System selbst protokolliert werden.

Eigenhändige Unterschriften oder elektronische Signaturen sind nur in denjenigen bundesverwaltungsinternen Fällen notwendig, in denen es sich um *finale Dokumente* handelt. Dies betrifft insbesondere die Fälle, in denen a) z. B. *Vereinbarungen* zwischen zwei oder mehreren Parteien abgelegt werden sollen oder b) Dokumente *ausserhalb des GEVER-Systems* gehalten werden oder c) Dokumente das

⁹ Wegen der technisch hohen Anforderungen an ein qualifiziertes Signaturzertifikat (Klasse A) kann der entsprechende Signaturschlüssel nicht auf der Smartcard des Bundes mit Zertifikaten der Klasse B gespeichert werden.

¹⁰ Bei der Zwei-Faktor-Authentifizierung einer Person werden Wissen und Besitz kombiniert: Wissen: «etwas, was Sie als Person kennen» = das Windows Passwort oder der PIN; Besitz: «etwas, was Sie als Person haben» = die Smartcard.

E-Signatur für verwaltungsinterne Dokumente

GEVER-System z. B. für die Archivierung *verlassen*. In den allermeisten Fällen reicht jedoch eine fortgeschrittene elektronische Signatur mit dem fortgeschrittenen Signaturzertifikat (Klasse B) aus, ausser die schriftliche Form ist im konkreten Fall als Gültigkeitsvoraussetzung ausdrücklich vorgesehen, wie das z. B. gemäss Artikel 13 des Bundespersonalgesetzes (BPG)¹¹ für Arbeitsverträge der Fall ist.

Eigenhändige Unterschriften oder qualifizierte elektronische Signaturen sind ebenso beim Erlass von Verfügungen relevant (siehe Ziff. 2.4.5.1 Verfügungen). Deren Adressaten befinden sich jedoch grösstenteils ausserhalb der Bundesverwaltung. In seltenen Fällen richten sich Verfügungen an bundesverwaltungsinterne Adressaten (z. B. Kündigung durch den Arbeitgeber im Personalwesen). Die Eröffnung qualifiziert elektronisch signierter Verfügungen wird zusätzlich durch die Vorschrift eingeschränkt, dass die Adressaten ausdrücklich ihr Einverständnis zur Eröffnung in elektronischer Form erteilen müssen.

Fazit

Im Bundesverwaltungsrecht gibt es nur wenige Vorschriften, die – neben den Verfügungen – explizit die *schriftliche Form* und damit eine eigenhändige Unterschrift und in elektronischer Form entsprechend eine qualifizierte elektronische Signatur (anstelle einer fortgeschrittenen Signatur) verlangen. Es ist im Einzelfall auszulegen, wie die Begriffe «Schriftform», «schriftliche Form» und «(mit) Unterschrift» im Bundesverwaltungsrecht jeweils zu verstehen sind.

2.4.2 Schriftlichkeit

Die Schriftlichkeit von *bundesverwaltungsinternen Dokumenten* stellt sicher, dass Entscheidungsprozesse der Verwaltung *nachvollziehbar* und transparent sind. Dies lässt sich auch aus der Bundesverfassung (BV)¹² ableiten: Diese hält fest, dass alle Menschen vor dem Gesetz gleich sind (Art. 8 BV) und Anspruch darauf haben, von den staatlichen Organen ohne Willkür und nach Treu und Glauben behandelt zu werden (Art. 9 BV).

Damit diese Rechte bei Bedarf auch durchgesetzt werden können, ist es nötig, dass das Verwaltungshandeln klar geregelt und dokumentiert ist. Konkret bedeutet dies, dass bundesverwaltungsinterne Geschäftsprozesse abgebildet und nachvollziehbar sein müssen; insbesondere wenn es darum geht, wer wann wie entschieden hat und wer in den Entscheidungsprozess einbezogen war.

Diese Vorgabe kann bundesverwaltungsintern im elektronischen Bereich auch ohne eigenhändige Unterschrift oder einer gleichwertigen qualifizierten elektronischen Signatur eingehalten werden, beispielsweise mittels *elektronischer Geschäftsverwaltung*. Ausschlaggebend ist somit die dauerhafte Aufzeichnung mittels Schriftzeichen auf einem Erklärungsträger (sog. «Verurkundung») und nicht die «Schriftlichkeit» im technischen Sinne, wonach der Text mit einer eigenhändigen Unterschrift zu versehen ist.

Fazit

Entsprechend sind die VE nach Artikel 22 Absatz 1 der Verwaltungsorganisationsverordnung (RVOV)¹³ verpflichtet, den Nachweis über die eigene Geschäftstätigkeit aufgrund einer systematischen Geschäftsverwaltung zu führen. Daher setzen die VE elektronische Geschäftsverwaltungssysteme nach der GEVER-Verordnung¹⁴ ein (Art. 22 Abs. 2 RVOV). Im Finanz- und Ressourcenbereich wird Nachvollziehbarkeit und Revisionstauglichkeit analog mit dem SAP-ERP-System sichergestellt.

2.4.3 Formvorschriften für Verträge

Nach Artikel 1 Obligationenrecht (OR; SR 220) ist jegliche «übereinstimmende gegenseitige Willensäusserung der Parteien» rechtsverbindlich und Verträge bedürfen gemäss Artikel 11 Absatz 1 OR zu ihrer Gültigkeit nur dann einer besonderen Form, wenn das Gesetz eine solche vorschreibt¹⁵ (sog.

¹¹ SR 172.220.1

¹² SR 101

¹³ SR 172.010.1

¹⁴ SR 172.010.441

¹⁵ Überdies können die Vertragsparteien auch untereinander eine bestimmte Form vereinbaren (vgl. Art. 16 OR).

E-Signatur für verwaltungsinterne Dokumente

Grundsatz der Formfreiheit). So sieht das Gesetz für gewisse Rechtsgeschäfte die Form der *einfachen Schriftlichkeit* im Sinne von Artikel 12 ff. OR vor. Die einfache Schriftlichkeit verlangt, dass der Vertrag von allen Parteien eigenhändig (vgl. Art. 14 Abs. 1 OR) oder mit einer «qualifizierten elektronischen Signatur» nach Artikel 2 Buchstabe e ZertES elektronisch (vgl. Art. 14 Abs. 2^{bis} OR) signiert wird. Nur mit einer qualifizierten elektronischen Signatur kann somit das Formerfordernis der *einfachen Schriftlichkeit* bei der elektronischen Kommunikation erfüllt werden.¹⁶

Daraus folgt jedoch nicht, dass schriftlich festgehaltene Verträge, die nicht eigenhändig oder mit einer qualifizierten elektronischen Signatur unterzeichnet sind, nicht rechtsverbindlich sind. In Abwesenheit gesetzlicher oder vertraglich vorbehaltener Formerfordernisse, sind sie nach dem Grundsatz der Formfreiheit also rechtsverbindlich. In diesen Fällen ist auch ein Vertrag, der nur mit einer fortgeschrittenen elektronischen Signatur nach Artikel 2 Buchstabe b ZertES unterzeichnet ist, *rechtsverbindlich*.

Die verschiedenen elektronischen Unterschriftenformen unterscheiden sich jedoch in ihrer *Qualität* und damit auch in ihrer *Beweiskraft*. Bis anhin fehlt eine einschlägige Rechtsprechung zur Frage, welche Beweiskraft einer fortgeschrittenen elektronischen Signatur zukommt. Die Frage nach der Gültigkeit einer fortgeschrittenen Signatur lässt sich nicht im Allgemeinen beantworten, sondern muss im Einzelfall geprüft und beurteilt werden. Dabei ist auch den Anforderungen der Vertragspartner an die Beweiskraft der Dokumente Rechnung zu tragen. Weiter muss die Sicherheit der Signaturverfahren, der Aufbewahrung des Signaturschlüssels und der Identifikationsprozesse bei der Ausgabe eines Zertifikates unterhalb des Niveaus qualifizierter und geregelter elektronischer Signaturen im Einzelfall geprüft werden.

Angesichts fehlender Kontrollmöglichkeiten der Authentizität handschriftlicher Signaturen sowie der einfachen Manipulierbarkeit von Papierdokumenten (insbesondere bei mehrseitigen Dokumenten) darf jedoch angenommen werden, dass eine *fortgeschrittene* elektronische Signatur nach Artikel 2 Buchstabe b ZertES durchaus eine mit der handschriftlichen Unterschrift mindestens gleichwertige Beweiskraft für die Integrität und Authentizität eines Dokumentes bieten kann. Die schwächere Beweiskraft einer fortgeschrittenen Signatur im Vergleich zu einer qualifizierten elektronischen Signatur dürfte in der Praxis kaum zu Problemen führen: Streitigkeiten mit Lieferanten sind in der Regel auf Differenzen bei der Auslegung von Vertragsbestimmungen oder bei der Bewertung der Lieferqualität zurückzuführen. Selten bis nie wird die Authentizität oder Integrität des Vertragstextes selbst bestritten.

Fazit

Rein bundesinterne Dokumente, aber auch Verträge mit externen Parteien, können somit – sofern nicht in eher seltenen Fällen von deren Inhalt her oder generell vom Geschäftsprozess her ausdrücklich gesetzlich die Schriftform verlangt wird – von allen bundesinternen Parteien auch mit dem fortgeschrittenen Signaturzertifikat der Klasse B elektronisch signiert werden. Die hohe Qualität dieses Zertifikates (Signaturschlüssel auf Smartcard und glaubwürdiger Identifikationsprozess) ist den Mitarbeitenden bekannt und die damit erzeugten *fortgeschrittenen* Signaturen genießen zumindest bundesverwaltungsintern hohes (gegenseitiges) Vertrauen.

Gegenüber externen Parteien stellt sich das Ganze dagegen nicht so einfach dar. Die fortgeschrittene Signatur der Bundesverwaltung, wie auch die fortgeschrittenen Signaturen aus der Privatwirtschaft sind nicht vom ZertES und dem darunterliegenden Normenwerk in allen qualitativen Aspekten (Sicherheit, Schlüsselaufbewahrung, Identifikationsprozess usw.) definiert. Dies im Gegensatz zu einer qualifizierten Signatur. Für beide Parteien ist es deshalb schwierig zu beurteilen, ob sie einem beidseitig fortgeschritten signierten Dokument vertrauen können.

¹⁶ Botschaft vom 15. Januar 2014 zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES), BBl 2014 1001, S. 1014.

E-Signatur für verwaltungsinterne Dokumente

2.4.4 Exkurs: Verträge bei Beschaffungen des Bundes

Gemäss Artikel 11 Absatz 1 der Verordnung über das öffentliche Beschaffungswesen (VöB)¹⁷ sind alle Beschaffungsverträge der Bundesverwaltung, die im Geltungsbereich des Bundesgesetzes über das öffentliche Beschaffungswesen (BöB)¹⁸ liegen, «in Schriftform» abzuschliessen.

Der Begriff der Schriftform in Art. 11 VöB ist nicht gleichbedeutend mit dem Begriff der Schriftlichkeit gemäss OR.¹⁹ Ein Beschaffungsvertrag kann somit schriftlich oder in einer anderen Form, die den Nachweis durch Text ermöglicht, abgeschlossen werden. Mündlich oder konkludent geschlossene Beschaffungsverträge erfüllen diese Erfordernisse hingegen nicht. Im Rahmen der Umsetzung dieser Bestimmung in der Praxis erarbeitet die Beschaffungskonferenz des Bundes derzeit Empfehlungen zum digitalen Vertragsabschluss im öffentlichen Beschaffungswesen.

Qualifizierte Zertifikate in der Bundesverwaltung

Die Mitarbeitenden der Bundesverwaltung verfügen über ein nicht qualifiziertes, fortgeschrittenes Signaturzertifikat (Klasse B) von der Swiss Government PKI (SGPKI) des Bundesamts für Informatik und Telekommunikation (BIT). Ein qualifiziertes Signaturzertifikat (Klasse A) kann aber bei der SGPKI jederzeit beschafft werden. Dabei ist der aktuelle Identifikationsprozess, bei dem die Antragstellenden für ein solches Zertifikat persönlich und mit einer amtlichen Ausweisschrift bei der SGPKI vorsprechen müssen, relativ aufwändig. Mit aus diesem Grund sind bisher nur einige hundert Mitarbeitende mit einem qualifizierten Signaturzertifikat ausgerüstet.

Der Identifikationsprozess dürfte sich mittelfristig jedoch vereinfachen, da auf Ebene der Europäischen Union (EU) Arbeiten für eine Standardisierung von Identifikationsprozessen via Video im Gange sind. Diese sollen in Form der europäischen Norm ETSI TS 119 461 Teil auch der schweizerischen Signaturgesetzgebung (ZertES) werden. Der Bunderrat hat in der Interpellation 20.4274 Bellaïche darauf hingewiesen, dass mit Artikel 7 Absatz 1 VZertES²⁰ eine rechtliche Grundlage für eine allgemeine Identifikation via Video besteht.

Für die Umsetzung dieser Bestimmung wird vorausgesetzt, dass eine akkreditierte Stelle prüft und beurteilt, ob die von den anerkannten Anbieterinnen von Zertifizierungsdiensten verwendeten Methoden zur Identifizierung auf Distanz den Regeln entsprechen. Auch die Swiss Government PKI (SGPKI) in der Bundesverwaltung kann so in absehbarer Zeit auf dieser Basis Videoidentifikationsprozesse aufbauen, um die Ausgabe von qualifizierten Zertifikaten zu vereinfachen und zu beschleunigen.

Qualifizierte Zertifikate bei Lieferanten

Die meisten Lieferanten der Bundesverwaltung verfügen heute nicht über eine qualifizierte elektronische Signatur. Dies liegt aber hauptsächlich daran, dass sie kaum Gelegenheit haben, eine solche zu benutzen. Die Beschaffung einer qualifizierten Signatur ist zwar schwieriger geworden - insbesondere seit dem der Verkauf der SuisseID von der Post Ende 2020 eingestellt wurde - bleibt aber für Personen, die in der Schweiz wohnhaft sind, trotzdem bei mindestens zwei anerkannten Anbieterinnen möglich. Die Identitätsprüfung (persönliches Vorsprechen mit Pass oder Identitätskarte) kann dabei bei ausgewählten Swisscom Shops, bei Poststellen oder vor einer Urkundsperson (Notariat) erfolgen.

Lieferanten der Bundesverwaltung im europäischen Ausland haben es insofern schwer, dass ein dort ausgegebenes qualifiziertes Zertifikat gemäss EU-Recht in der Schweiz rechtlich als ein fortgeschrittenes gilt. Für eine Vertragsunterschrift bietet es jedoch die gewünschte Sicherheit, v. a. bei der Identifikation der Person. Die Lieferanten sind nicht verpflichtet, elektronische Zertifikate anzuschaffen. Die Geschäftsprozesse sind bereits heute so ausgestaltet, dass verschiedene Möglichkeiten bestehen. So haben beispielsweise Verwaltungseinheiten des Bundes den Vertragsschluss in einer der folgenden Vorgehensweisen ausgestaltet:

¹⁷ SR 172.056.11

¹⁸ SR 172.056.1

¹⁹ Siehe Erläuterungen zur Verordnung über das öffentliche Beschaffungswesen (VöB) vom 12. Februar 2020, Art. 11, S. 10.

²⁰ SR 943.032

E-Signatur für verwaltungsinterne Dokumente

Vorgehensweise 1:

1. Der Vertragsentwurf wird dem Lieferanten per E-Mail unsigniert zugesendet;
2. Der Lieferant sendet den Vertrag entweder qualifiziert elektronisch signiert per E-Mail oder Secure Mail ein, oder er druckt den Vertrag aus, unterschreibt von Hand und sendet den Vertrag per Post ein.
3. Je nachdem, ob der unterzeichnete Vertrag elektronisch oder auf Papier eingegangen ist, sendet die Auftraggeberin den Vertrag ihrerseits elektronisch signiert per E-Mail oder Secure Mail oder von Hand unterschrieben per Post zu.

Die Wahl liegt bei dieser Vorgehensweise bei den Lieferanten, ob ein Vertrag elektronisch geschlossen wird oder herkömmlich auf Papier.

Vorgehensweise 2;

1. wie oben
2. wie oben
3. Nach Eintreffen bei der Verwaltung wird der Vertrag (wenn auf Papier) eingescannt. Die eingescannte elektronische Version, oder die eingegangene elektronisch signierte Version werden danach qualifiziert von der Verwaltung signiert und per E-Mail oder Secure Mail dem Lieferanten geschickt.

Bei dieser Vorgehensweise werden die Verträge seitens der Verwaltung nur elektronisch unterschrieben und der ganze Geschäftsprozess elektronisch abgewickelt.

Es bestehen auch weitere Vorgehensmöglichkeiten. Wie erwähnt, beabsichtigt die Beschaffungskonferenz des Bundes BKB deshalb, Empfehlungen zum digitalen Vertragsabschluss im öffentlichen Beschaffungswesen abzugeben. Es wird auf diese verwiesen.

Validierung elektronischer Unterschriften

Werden bei den Vertragsschlüssen die Dokumente mit qualifizierten elektronischen Signaturen oder auch mit fortgeschrittenen elektronischen Signaturen mit dem Signaturzertifikat Klasse B der Mitarbeitenden signiert, können diese Signaturen mit dem Validator der Bundesverwaltung ([validator.ch](https://www.bk.admin.ch/validador)) überprüft werden. Nicht mit dem Validator überprüft werden können fortgeschrittene Zertifikate anderer anerkannter Schweizer und EU-Anbieter und qualifizierte Zertifikate von EU und sonstigen ausländischen Anbietern. Für die entsprechenden Zertifikate kann jedoch eine beschränkte Überprüfung mittels des Adobe Acrobat Readers vorgenommen werden. Dafür müssen in der Konfiguration dieses Programms sowohl die sog. AATL (Adobe Approved Trustlist) wie auch die EUTL (EU Approved Trustlist) aktiviert sein.

Internationale Anerkennung von schweizerischen Zertifikaten

Im Kontext von Beschaffungsverträgen mit ausländischen Unternehmen ist die Frage der gegenseitigen Anerkennung von qualifizierten Zertifikaten und geregelten Siegeln gemäss ZertES zurzeit nicht geregelt. Die Schweiz hat mit der Revision ihres Signaturgesetzes (ZertES) eine Regelung eingeführt, die rechtlich, technisch und organisatorisch konform zur entsprechenden Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) der EU ist. Da die privatwirtschaftlichen Anbieterinnen von Signaturlösungen meist wahlweise die Erstellung von ZertES konformen, wie auch die Erstellung von EU-konformen geregelten und qualifizierten Signaturen erlauben, könnte eine Lösung auch darin bestehen, dass die Schweiz einseitig Signaturen gemäss der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) der EU anerkennt.

Massnahme 1

Das EJPD (BJ) wird beauftragt, unter Einbezug von WBF (SECO), EDA (DV und StS), EFD (EZV) und UVEK (BAKOM) zu prüfen, wie die einseitige oder gegenseitige Anerkennung der geregelten und qualifizierten Zertifikate mit der EU und mit anderen für die Schweiz wichtigen Staaten vorangetrieben werden kann, und den Bundesrat bis Ende 2021 über das Ergebnis zu informieren.

E-Signatur für verwaltungsinterne Dokumente

2.4.5 Exkurs: Verfügungen und Rechnungen mit Verfügungscharakter

2.4.5.1 Verfügungen

Für Verfügungen sieht Artikel 34 Absatz 1 des Verwaltungsverfahrensgesetzes (VwVG)²¹ zwar den *Grundsatz der Schriftlichkeit* vor. Dabei ist aber umstritten, ob das *Erfordernis der Schriftlichkeit* auch eine in jedem Fall gültige Verpflichtung zur (handschriftlichen) Unterzeichnung durch Mitarbeitende der verfügenden Behörde beinhaltet.²² Viele Verfügungen, wie z. B. Veranlagungen von Zoll und Steuerbehörden, werden gar ohne jegliche Unterschrift erlassen.

Gemäss Artikel 34 Absatz 1^{bis} VwVG können Verfügungen nur mit dem Einverständnis der Partei elektronisch eröffnet werden, wobei auf Gesetzesstufe nicht ausschliesslich eine qualifizierte – der handschriftlichen Unterschrift gleichgestellte – elektronische Signatur verlangt wird. Vielmehr bleibt die Bestimmung der Art der elektronischen Signatur dem Verordnungsgeber überlassen. So hat der Bundesrat in der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV)²³ in Artikel 9 Absatz 4 festgelegt, dass elektronisch zu eröffnende Verfügungen im Grundsatz mit qualifizierten elektronischen Signaturen zu versehen sind. Dabei beschränkt der Bundesrat in Artikel 9 Absatz 5 VeÜ-VwV den Einsatz von geregelten elektronischen Siegeln nach Artikel 2 Buchstabe d ZertES auf

- (a) die Erstellung von elektronischen Kopien von handunterzeichneten Verfügungen in Papierform;
- (b) Verfügungen, die in einem automatisierten Verfahren erlassen werden und aufgrund ihrer grossen Anzahl nicht einzeln von einer Vertretung der Behörde unterzeichnet werden (Massenverfügungen);
- (c) E-Rechnungen mit Verfügungscharakter; auf diesen Rechnungen kann das geregelte elektronische Siegel im Auftrag der zuständigen Behörde von den für den elektronischen Rechnungsaustausch üblichen Dienstleistern angebracht werden.

Der bestehende rechtliche Rahmen und dessen risikoscheue Auslegung (insb. von Art. 9 Abs. 5 Bst. b VeÜ-VwV) seitens der Verwaltungseinheiten führt dazu, dass die in der Anwendung effizienten und kostengünstigen geregelten elektronischen Siegel gerade bei den zahlreichen, einfachen Bewilligungsprozessen nur selten als einsetzbar eingestuft werden. Dies obwohl heute der grösste Teil der Verfügungen der Bundesverwaltung in automatisierten Verfahren (GEVER oder spezielle Fachanwendungen) erlassen wird, in denen die Mitarbeitenden ohnehin mittels des Authentifizierungszertifikates (Klasse B) identifiziert sind. Würde anstelle eines qualifizierten Signaturzertifikates für eine natürliche Person ein geregeltes *Siegel*zertifikat eingesetzt, wäre dies bezüglich Nachvollziehbarkeit und Transparenz mit der aktuellen Lösung gleichwertig, jedoch deutlich effizienter.

Massnahme 2a

Das EJPD (BJ) wird beauftragt, unter Einbezug der BK (DTI) bis Ende 2021 zu prüfen, ob und wie geregelte elektronische Siegel generell beim Erlass von Verfügungen ohne Unterschrift eingesetzt werden können, und ggf. dem Bundesrat einen Entwurf zur Änderung der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV, SR 172.021.2, Art. 9 Abs. 4 und 5) vorzulegen

2.4.5.2 Rechnungen mit Verfügungscharakter

Die Eidgenössische Finanzverwaltung (EFV) ist als Fachamt Finanzen zuständig für die Supportprozesse Finanzen Bund. Sie ist bestrebt, die bundesweiten Finanzprozesse vollständig und integriert digital abzuwickeln. In dieser Hinsicht ist die Bundesverwaltung bereits sehr weit fortgeschritten. Einer der wenigen Bereiche, in dem noch viel Optimierungspotential (mehrere hunderttausend Rechnungen

²¹ SR 172.021

²² vgl. Kneubühler/Pedretti in Auer et al. vgl. Kneubühler/Pedretti in Auer et al., VwVG Kommentar, Artikel 34, Rz. 9f.

²³ SR 172.021.2

E-Signatur für verwaltungsinterne Dokumente

jährlich) besteht, ist der (elektronische) Versand von Rechnungen, welche zusätzlich eine Rechtsmittelbelehrung aufweisen («Rechnungen mit Verfügungscharakter»).

In der Revision der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV) per 2017 wurden die Grundlagen geschaffen, dass die Rechnungen mit Verfügungscharakter elektronisch signiert mit einem geregelten elektronischen Siegel über die gängigen Plattformen für elektronische Rechnungsstellung (Postfinance, SIX) zugestellt werden können.

In der Zwischenzeit hat sich die Zustellung von Rechnungen per E-Mail im PDF-Format ebenfalls etabliert, weil dies sehr einfach und kostengünstig ist. Dazu beigetragen hat, dass die MWST auf die Pflicht zur Signatur verzichtet und die entsprechende Verordnung des EFD über elektronische Daten und Informationen (EIDI-V)²⁴ per Ende 2019 ausser Kraft gesetzt hat. Dies ermöglicht nun den rechtskonformen Austausch auch von unsignierten PDF-Rechnungen.

Bei den Rechnungen der Lieferanten des Bundes hat sich gezeigt, dass die Eingabe von unsignierten Rechnungen via E-Mail insbesondere für kleinere Unternehmen weniger aufwändig und kostengünstiger ist, weil sie sich nicht bei einer Plattform für elektronische Rechnungsstellung (kostenpflichtig) registrieren müssen. So hat die EFV ihrerseits für den Empfang von Rechnungen im PDF-Format eine zentrale E-Mail-Adresse für ihre Lieferanten aufgesetzt. Dies entspricht den Erwartungen der Lieferanten und wird von diesen rege genutzt. Die EFV hat zudem bereits bundesweit für alle Verwaltungseinheiten die technischen Möglichkeiten geschaffen, dass Rechnungen im PDF-Format an eine E-Mail-Adresse zugestellt werden können.

Die EFV beantragt deshalb, dass mit der unter Ziffer 2.4.5.1 bereits angedachten Revision der VeÜ-VwV zusätzlich geprüft wird, ob die Grundlagen geschaffen werden können, dass neu auch Rechnungen mit Verfügungscharakter dem Empfänger als signiertes oder als gesiegeltes PDF auch über andere Kanäle zugestellt werden können. Eine solche Anpassung entspricht einem grossen Bedürfnis der Kunden der Bundesverwaltung, fördert die digitale Weiterentwicklung und Transformation der Dienstleistungen der Bundesverwaltung und entspricht damit dem grundlegenden Anliegen Postulats Dobler, den Geschäftsverkehr möglichst elektronisch abwickeln zu können.

Massnahme 2b

Das EJPD (BJ) wird beauftragt, unter Einbezug der BK (DTI) bis Ende 2021 zu prüfen, ob und wie die Zustellung von Rechnungen mit Verfügungscharakter, gegenüber der heutigen Regelung in der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV, SR 172.021.2, Art. 9 Abs. 2^{bis} und 3) vereinfacht werden kann, und ggf. einen entsprechenden Entwurf vorzulegen

2.4.6 Exkurs: Bundesratsgeschäfte

Der Bundesrat ist nach Artikel 174 der Bundesverfassung die oberste leitende und vollziehende Behörde des Bundes. Die Bundesverwaltung untersteht dem Bundesrat gemäss Artikel 2 Absatz 1 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG)²⁵. Somit leitet der Bundesrat die Bundesverwaltung, gehört ihr aber selber nicht an. Auch wenn der Bundesrat als *Kollegialbehörde* nicht Gegenstand des vorliegenden Berichts ist, sei dennoch kurz auf die Schriftlichkeit seines *Entscheidfindungsprozesses* hingewiesen. Der Bundesrat hat bereits im Jahr 2019 entschieden, seine Entscheidungsprozesse *digital* durchzuführen.

²⁴ SR 641.201.511

²⁵ SR 172.010

E-Signatur für verwaltungsinterne Dokumente

Artikel 3 Absatz 1 der Verwaltungsorganisationsverordnung (RVOV) hält fest, dass der Bundesrat seine Beschlüsse in der Regel gestützt auf schriftliche Anträge und nach abgeschlossenem *Mitberichtsverfahren* fällt. Daraus ergibt sich, dass auch die den Entscheidungsprozess beschliessenden Dokumente – die *Bundesratsbeschlüsse* – unterzeichnet werden müssen.

Der Entscheidungsprozess des Bundesrates ist unterteilt in das schriftliche Mitberichtsverfahren nach Artikel 15 RVOG und der darauf anschliessenden mündlichen Bundesratssitzung (vgl. Art. 21 RVOG). Das Mitberichtsverfahren *beginnt* mit der Unterzeichnung des Antrags²⁶ durch das federführende Departement (Art. 5 Abs. 1^{bis} RVOV). Die RVOV äussert sich *nicht* zur *Form* der Unterzeichnung des Antrags. Dasselbe muss analog auch für Mitberichte, Stellungnahmen sowie die Beschlüsse des Bundesrates gelten.

Artikel 5 Absatz 1^{bis} RVOV wurde mit der Verordnung vom 24. Mai 2006 über das Öffentlichkeitsprinzip der Verwaltung (VBGÖ)²⁷ in die RVOV eingefügt. Bei der neuen Bestimmung ging es darum, den Zeitpunkt des *Beginns des Mitberichtsverfahrens* genau festzulegen, da die amtlichen Dokumente des Mitberichtsverfahrens vom Zugangsrecht des Öffentlichkeitsgesetzes (BGÖ)²⁸ ausgenommen sind. Für die Bestimmung des Zeitpunkts der Eröffnung des Mitberichtsverfahrens ist es *unerheblich*, ob der Antrag handschriftlich oder elektronisch unterzeichnet wurde. In den Materialien finden sich daher auch keine Hinweise, dass die Unterzeichnung *nur handschriftlich* erfolgen kann.

Auch wenn der Bundesrat bei der Schaffung von Artikel 5 Absatz 1^{bis} RVOV nicht die elektronische Unterzeichnung im Fokus hatte, lässt die offene Formulierung der Bestimmung auch die elektronische Signatur zu. Dieser Idee folgend hat der Bundesrat am 30. Januar 2019 beschlossen, dass die *handschriftliche Unterschrift und die elektronische Signatur* im Sinne des ZertES auf den Unterlagen im Zusammenhang mit der Vorbereitung (Mitberichtsverfahren) und der Durchführung von Bundesratssitzungen wie Anträge, Mitberichte sowie Bundesratsbeschlüsse *gleichgestellt* sind. Für das Mitberichtsverfahren, deren Stellungnahmen sowie die Beschlüsse des Bundesrates ist die elektronische Signatur mit einem fortgeschrittenen Klasse-B-Signaturzertifikat ausreichend.

2.4.7 Exkurs: Personalwesen und Personensicherheitsüberprüfungen

2.4.7.1 Personalwesen allgemein

Im Personalwesen ist zwischen Verträgen als zweiseitig verpflichtende Rechtsgeschäfte und den Kündigungen als einseitige Rechtsgeschäfte zu unterscheiden. Gemeinsam ist ihnen, dass sie nach Artikel 13 des Bundespersonalgesetzes (BPG)²⁹ zu Ihrer *Gültigkeit* der *schriftlichen Form* (hier im Sinne der einfachen Schriftlichkeit des Obligationenrechts) bedürfen. Diese beinhaltet in der elektronischen Form - wie oben ausgeführt (Ziff. 2.2) - eine mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronischen Signatur gemäss ZertES (Art. 14 Abs. 2^{bis} OR), womit auch hier das *Prinzip der Gleichwertigkeit der Formen* Anwendung findet. Ein neuer Arbeitsvertrag zwischen der Bundesverwaltung als Arbeitgeberin und einer anzustellenden Person, ist jedoch *nicht* ein rein bundesverwaltungsinternes Dokument im Sinne des vorliegenden Postulats.

Demgegenüber ist die Kündigung des Arbeitsverhältnisses ein einseitiges Rechtsgeschäft. Die von der Verwaltung als Arbeitgeberin ausgehende Kündigung muss schriftlich erfolgen (Art 34 Abs. 1 VwVG) und darf in nur mit dem Einverständnis der Partei und elektronisch qualifiziert signiert eröffnet werden (Art. 34 Abs. 1^{bis} VwVG). Die elektronische Kündigung durch den Arbeitnehmer ist ebenfalls nur möglich, wenn dieser über ein qualifiziertes Zertifikat verfügt.

Bei einer Analyse der Geschäftsfälle des Eidgenössischen Personalamtes (EPA) wurde vom *Standarddienst Signaturdienste Bund* (vgl. Ziff. 2.1) im Dezember 2020 vor diesem Hintergrund geprüft, ob alle

²⁶ Aus der Systematik von RVOG und RVOV ergibt sich, dass das Mitberichtsverfahren zu Aussprachepapieren (Art. 17 RVOG, Art. 3 Abs. 4 RVOV) und zu Informationsnotizen (Art. 12 a RVOG, Art. 3 Abs. 5 RVOV) ebenfalls mit der Unterzeichnung beginnt (Art. 3 RVOV).

²⁷ SR 152.31

²⁸ SR 152.3

²⁹ SR 172.220.1

E-Signatur für verwaltungsinterne Dokumente

Mitarbeitenden der zentralen Bundesverwaltung mit einem qualifizierten Signaturzertifikat (Klasse A) auszurüsten seien, oder ob es ausreichend sei, nur die unterschriftsberechtigten Mitarbeitenden mit einem qualifizierten Signaturzertifikat (Klasse A) auszurüsten.

Die Analyse ergab, dass der Abschluss des Arbeitsvertrages kaum beiderseitig mit einer qualifizierten elektronischen Signatur erfolgen kann, da neu eintretende Mitarbeitende nur in Ausnahmefällen über ein qualifiziertes Signaturzertifikat aus dem Markt verfügen. Nur die Anpassung von bestehenden Arbeitsverträgen oder die einvernehmliche Auflösung (da zweiseitig verpflichtendes Rechtsgeschäft) könnten beiderseitig qualifiziert signiert werden, sofern alle Mitarbeitenden nach dem Eintritt ein qualifiziertes Signaturzertifikat erhalten würden. Auch das Arbeitszeugnis bedarf einer qualifizierten Signatur, damit die Gültigkeit mit dem Validator.ch-Service umfassend und abschliessend durch einen potenziellen Arbeitgeber ausserhalb der zentralen Bundesverwaltung überprüft werden kann.

Ganz allgemein gilt, dass Verfahren im Personalwesen, auf die das Bundesgesetz über das Verwaltungsverfahren (VwVG) Anwendung findet, nur dann vollständig digital abgewickelt werden können, wenn nicht nur allfällige Unterschriften elektronisch angebracht, sondern auch die Übermittlung elektronisch abgewickelt werden kann. Geregelt wird dies in der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV). Artikel 34 Absatz 1^{bis} VwVG und Artikel 8 der VeÜ-VwV halten fest, dass die Behörde einer Partei eine Verfügung nur dann auf elektronischem Weg eröffnen darf, wenn «die Partei dieser Art der Mitteilung im Rahmen des konkreten Verfahrens ausdrücklich zugestimmt hat». Die Verfügungen sind gemäss Artikel 9 Absatz 4 VeÜ-VwV qualifiziert zu signieren.

In allen anderen vom EPA beschriebenen, viel häufigeren Geschäftsfällen (u. a. Ziel- und Ausbildungsvereinbarungen, Personalbeurteilungen) sind die folgenden Abschlussarten auf elektronischem Weg dagegen ausreichend, da es nur um den Nachweis/Beweis geht:

- eine E-Mail allenfalls mit Bestätigung durch den Empfänger (ggf. mit Klasse B E-Mailsignatur und allenfalls Verschlüsselung);
- Visum in den Metadaten eines Workflows (z. B. ActaNova);
- fortgeschrittene Signatur (Klasse B) auf einem PDF mit der Smartcard des Bundes.

Fazit

Um im Personalwesen die im Verhältnis geringe Zahl von Geschäftsfällen elektronisch abwickeln zu können, die – wegen des Schriftlichkeitserfordernisses – eine zweiseitige qualifizierte elektronische Signatur erfordern, müsste ein unverhältnismässiger Aufwand betrieben werden, indem alle Mitarbeitenden der zentralen Bundesverwaltung mit einer qualifizierten elektronischen Signatur auszurüsten wären. Entsprechende Massnahmen sind zurzeit nicht sinnvoll. Die überwiegende Zahl der täglichen Geschäftsfälle im Personalwesen erfordert keine qualifizierte Signatur und kann – wo eine Unterschrift notwendig ist – auf Basis des fortgeschrittenen Signaturzertifikates (Klasse B) abgewickelt werden.

2.4.7.2 Personensicherheitsprüfungen

Geschäftsfälle von relativ grossem Volumen sind die *Personensicherheitsprüfungen* (PSP) der Bundeskanzlei und v. a. des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS). Diese sind in der Verordnung über die Personensicherheitsprüfungen vom 4. März 2011 (PSPV)³⁰ geregelt.

Artikel 19 Absatz 3 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (BWIS)³¹ sieht vor, dass es zur Durchführung einer PSP einer Einwilligung der zu prüfenden Person bedarf. In Artikel 14 Absatz 5 der Verordnung über die Personensicherheitsprüfungen vom 4. März 2011 (PSPV) ist deshalb festgehalten, dass die zu prüfende Person das Prüfformular zu unterzeichnen hat, sofern sie in die PSP einwilligen möchte.

³⁰ SR 120.4

³¹ SR 120

E-Signatur für verwaltungsinterne Dokumente

Bisher wurde das Prüfformular von der zu prüfenden Person handschriftlich unterschrieben. Seit dem 1.1.2021 akzeptiert die Fachstelle PSP der Bundeskanzlei neu bei *Wiederholungen* der Prüfung auch eine fortgeschrittene elektronische Signatur mit dem Signaturzertifikat Klasse B der Mitarbeitenden des Bundes. Bei Erstanstellung ist weiterhin eine handschriftliche Unterzeichnung notwendig, da die zu prüfende Person in den allermeisten Fällen noch nicht über ein qualifiziertes Signaturzertifikat verfügt.

Die Fachstelle PSP des VBS dagegen erachtet eine fortgeschrittene Signatur als rechtlich ungenügend und verlangt in jedem Fall eine handschriftliche Unterzeichnung respektive, bei elektronischer Einreichung des Prüfformulars, eine qualifizierte elektronische Signatur. Diese unterschiedliche Haltung bedarf einer Klärung. Das VBS stützt seine Meinung darauf, dass eine Eingabe an die Behörde gemäss Artikel 6 der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV) zwar ohne qualifizierte elektronische Unterschrift (d. h. auch ohne Unterschrift) möglich wäre, falls die Identität der absendenden Person und die Integrität der Übermittlung mit anderen Mitteln sichergestellt werden.

Von dieser Regel sind im Folgesatz jedoch die Fälle ausdrücklich ausgenommen, wo das Bundesrecht ausdrücklich eine Unterschrift verlangt, was bei der PSPV der Fall ist. Die Frage ist jedoch, ob nur eine qualifizierte elektronische Signatur oder ob auch eine fortgeschrittene Signatur mit dem Signaturzertifikat Klasse B der Mitarbeitenden des Bundes als gültige Unterschrift, die das Einverständnis der betroffenen Person dokumentieren soll, betrachtet werden darf.

Nach geltendem Recht³² gilt das Resultat einer durchgeführten Personensicherheitsprüfung und damit die Sicherheitserklärung ohne (Art. 22 Abs. 1 Bst. a PSPV) oder mit Auflagen (Art. 22 Abs. 1 Bst. b PSPV), eine Risiko- oder Feststellungserklärung als *Verfügung* (Art. 22 Abs. 1 Bst. c und d PSPV). Diese Verfügungen werden *schriftlich* eröffnet (Art. 22 Abs. 2 bis 4 PSPV). Da eine personensicherheitsgeprüfte Person noch gar nicht angestellt ist, ist die Personensicherheitsprüfung *kein bundesverwaltungsinternes* Verfahren im Sinne des vorliegenden Postulats und die Personensicherheitserklärung muss ihrer Eigenschaft als Verfügung entsprechend weiterhin eigenhändig (handschriftlich) unterzeichnet werden bzw. kann – unter Vorbehalt des Einverständnisses der geprüften Person – auch qualifiziert elektronisch signiert und übergeben werden (Art. 34 Abs. 1^{bis} VwVG und Art. 9 Abs. 4 VeÜ-VwV). Wiederholungen der Personensicherheitsprüfungen nach Artikel 18 PSPV sind demgegenüber an die Funktion geknüpft, womit das Verfahren als *bundesverwaltungsintern* im Sinne des vorliegenden Postulats betrachtet werden kann.

Fazit

Der Geschäftsprozess im Zusammenhang mit der *Wiederholungsprüfung von bundesinternen Personen* könnte rein elektronisch abgewickelt werden, sofern die rechtlichen Voraussetzungen in der PSPV geschaffen werden, damit sowohl a) das von der betroffenen Person zu signierende Prüfformular auch ohne qualifizierte elektronische Signatur eingereicht, wie auch b) die entsprechenden Verfügungen am Ende des Prozesses ohne ausdrückliches Einverständnis der betroffenen Person verschlüsselt per E-Mail elektronisch übermittelt werden können.

Vom Gesamtvolumen der Personensicherheitsprüfungen, das überwiegend vom VBS hauptsächlich mit bundesexternen Personen abgewickelt wird, stellen diese Fälle der Bundeskanzlei jedoch lediglich einen sehr kleinen Teil dar. Der grösste Teil der Personensicherheitsprüfungen lässt sich derzeit somit kaum in einem durchgängigen elektronischen Geschäftsprozess abwickeln, da die allermeisten der zu prüfenden Personen über keinerlei elektronische Signaturzertifikate oder gleichwertige elektronische Identifikationsmittel verfügen.

Das Beispiel zeigt aber auch, dass die Verwaltungseinheiten im Anwendungsbereich elektronischer Signaturen zu verschiedenen Auslegungen des geltenden Rechts kommen. In diesen Fällen sollten

³² Mit dem am 18. Dezember 2020 vom Parlament verabschiedeten Informationssicherheitsgesetz sollen das Ergebnis der Personensicherheitsbeurteilung (*Erklärungen*) dereinst einen *Realakt* nach Artikel 25a VwVG darstellen und es kann dagegen Beschwerde beim Bundesverwaltungsgericht geführt werden (Art. 44 Abs. 3 ISG), weil die Erklärungen der Fachstellen PSP «nur» empfehlenden Charakter haben (Art. 41 Abs. 1 ISG). Auch nach geltendem Recht ist die entscheidende Instanz nicht an die Verfügung der Prüfbehörde gebunden (Art. 23 Abs. 1 PSPV).

E-Signatur für verwaltungsinterne Dokumente

interne Gutachten erstellt werden, die Hindernisse für eine rasche digitale Transformation zu beseitigen versuchen, sei dies durch Auslegung, sei dies durch Vorschläge von raschen Anpassungen auf Verordnungsebene.

Massnahme 3

Das VBS (GS-VBS) wird beauftragt, in Zusammenarbeit mit der BK (Fachstelle PSP) sicherzustellen, dass im Rahmen der laufenden Arbeiten zur Erarbeitung des Ausführungsrechts zum Informationssicherheitsgesetz die formelle Gültigkeitsanforderung der Unterschrift für die Einwilligung der zu prüfenden Person zur Durchführung einer PSP zumindest für Wiederholungsprüfungen aus der Verordnung gestrichen wird. Die Einwilligung hat jedoch weiterhin schriftlich zu erfolgen und muss nachvollziehbar sein.

2.4.8 Exkurs: Legalisationen

Die «Legalisation» eines Schriftstückes bezweckt die Gleichstellung einer öffentlichen Urkunde eines anderen Staates. Dazu ist oft eine «Beglaubigung» der Echtheit der Urkunde durch eine Behörde des Staates, aus dem die Urkunde stammt, notwendig.

In der Schweiz ist die Bundeskanzlei (BK) für die Beglaubigung der Unterschriften von Verwaltungseinheiten der Bundesverwaltung, einschliesslich der schweizerischen Botschaften und Konsulate sowie der kantonalen Staatskanzleien und der Organisationen, die öffentliche Aufgaben im Interesse des ganzen Landes wahrnehmen, zuständig. Dieses formalisierte Verfahren der Legalisation wurde gestützt auf das Haager Übereinkommens vom 5. Oktober 1961 zur Befreiung ausländischer öffentlicher Urkunden von der Beglaubigung³³ für gewisse Staaten durch das etwas einfachere Apostillev erfahren ersetzt. Die BK ist zuständig für die Ausstellung der Apostille nach Artikel 3 des Haager Übereinkommens, soweit Verwaltungseinheiten der Bundesverwaltung betroffen sind.

Sowohl die Beglaubigung wie auch die Ausstellung einer Apostille setzt voraus, dass die Bundeskanzlei über Kopien der zu beglaubigenden oder - im Hinblick auf die Anbringung einer Apostille – zu überprüfenden Unterschrift verfügt. Die laufende Aktualisierung der Sammlung der Unterschriftsmuster und der manuelle Vergleich von Unterschriften ist aufwändig.

Die Beglaubigung und die Anbringung einer Apostille sind in der Schweiz rein analoge Verfahren. Der aktuelle internationale Rechtsrahmen sieht aber bereits seit bald 15 Jahren die Digitalisierung der Apostille vor, beispielsweise in Form einer Digitalisierung der zugrundeliegenden Urkunde und einer Signierung derselben mit einer e-Apostille.³⁴ Die e-Apostille wurde bereits in über 40 Ländern umgesetzt, nicht aber in der Schweiz.

Die Überprüfung digitaler Signaturen der Bundesverwaltung ist hingegen schon heute möglich. Unter der Adresse [validator.ch](https://www.validator.ch) besteht ein Service der Service der Bundesverwaltung, über den elektronische Signaturen auf Dokumenten von schweizerischen Behörden jederzeit und aller Welt aus überprüft werden können. Je nach Dokumenttyp werden dabei die Integrität der signierten Datei, die Signaturprüfung, der Stand eines allfälligen Widerrufs (Revozierungsstatus) des signierenden Zertifikats sowie gegebenenfalls die Gültigkeit des Zeitstempels geprüft.

³³ SR 0.172.030.4

³⁴ Für weiterführende Informationen siehe www.hcch.net. > Instrumente > Übereinkommen > 12 > e-APP.

3 Technische Analyse / Rahmenbedingungen

3.1 Elektronische Geschäftsverwaltung in der Bundesverwaltung

Die Verordnung vom 3. April 2019 über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung), welche sich auf Artikel 57h Absatz 3 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) stützt, hält fest, dass die Bundesverwaltung ihre geschäftsrelevanten Dokumente grundsätzlich in elektronischen Geschäftsverwaltungssystemen (GEVER-Systeme) zu bearbeiten hat (Art. 2 Abs. 1). Die VE nutzen dazu grundsätzlich das standardisierte GEVER (Art. 3 Abs. 1). Die GEVER-Standardlösung Acta Nova ist inzwischen für rund 30 000 Arbeitsplätze der zentralen Bundesverwaltung eingeführt (vgl. oben Ziff. 1.2). Im Personalbereich werden u. a. das Informationssystem Personaldatenmanagement (IPDM) oder das E-Personaldossier eingesetzt.

3.2 Elektronische Bestätigungen in Acta Nova

Artikel 14 der GEVER-Verordnung hält fest, dass es die GEVER-Systeme ermöglichen müssen, Informationen mit *elektronischen Bestätigungen* zu versehen, insbesondere um die Kenntnisnahme zu bestätigen oder eine Genehmigung einzuholen oder zu erteilen. Wie bereits erwähnt sind alle Mitarbeitenden der Bundesverwaltung bei diesen Prozessen über das Authentifizierungszertifikat auf ihrer Smartcard via eine 2-Faktor-Authentifizierung identifiziert. Damit ist genau nachvollziehbar, wer und wann genau welche GEVER-Bestätigung ausgeführt hat.

Bezüglich der Nachvollziehbarkeit ist die GEVER-Bestätigung somit vergleichbar mit einer elektronischen Signatur mit einem fortgeschrittenen Signaturzertifikat (Klasse B). Dabei ist die Authentizität indirekt durch das Authentisierungszertifikat, mit dem sich die Mitarbeitenden beim GEVER-System anmelden, und die Integrität des Dokumentes durch die Versionierung gesichert.

In GEVER sind folgende drei Bestätigungen vorgesehen:³⁵

- a) «Zur Kenntnis» - um die Kenntnisnahme zu bestätigen;
- b) «Zum Visieren» - um vor der Genehmigung die Zustimmung der vorprüfenden Stellen einzuholen;
- c) «Zur Genehmigung» - um die Genehmigung durchzuführen.

Diese Bestätigungen dienen der Abwicklung von arbeitsteiligen und mehr oder weniger standardisierten Prozessen. Typische Beispiele für bundesverwaltungsinterne Prozesse sind die Abwicklung von Anträgen an Departemente oder den Bundesrat im Rahmen der *Vorbereitung* des Mitberichtsverfahrens (vgl. oben Ziff. 2.4.6) oder die Erarbeitung von Erlassen. Dabei werden von bestimmten Personen oder Stellen erste Entwürfe erstellt, die dann von weiteren Personen oder Stellen ergänzt, überarbeitet oder auf bestimmte Vorgaben hin kontrolliert werden, bevor sie schliesslich auf unterschiedlichen Hierarchiestufen genehmigt werden. Diese automatisierten elektronischen Prozesse haben die Arbeiten auf Papier und damit allenfalls verbundenen handschriftliche Unterschriften oder Kürzeln in vielen, aber noch nicht allen Bereichen schon seit geraumer Zeit abgelöst.

3.3 Elektronische Signatur in Acta Nova

Neben den *GEVER-Bestätigungen* sind in Acta Nova auch elektronische Signaturen mit fortgeschrittenen Signaturzertifikaten (Klasse B), mit geregelten elektronischen Siegeln (sogenannte Behördenzertifikate, Klasse A) und mit qualifizierten Signaturzertifikaten (Klasse A) nach ZertES möglich. Elektronisch signiert werden dabei die Dokumente (PDF) selbst und die Signatur bildet mit dem Dokument eine untrennbare Einheit. Dies im Gegensatz zu den GEVER-Bestätigungen, die sich in den Metadaten, d. h. ausserhalb des Dokumentes befinden. Das hat zur Folge, dass die Metadaten nicht im Dokument integriert weitergegeben werden, wenn ein Dokument das GEVER-System verlässt. Daher sollten bereits genehmigte Dokumente, welche das GEVER-System verlassen oder extern zugestellt werden und eines besonderen Schutzes der Integrität und Authentizität bedürfen, elektronisch signiert werden.

³⁵ S. 15 der Erläuterungen der Bundeskanzlei zur GEVER-Verordnung vom 3. April 2019.

E-Signatur für verwaltungsinterne Dokumente

Seit 2018 kann in den GEVER-Systemen (u. a. auch aktuell in Acta Nova) mit dem für die Bundesverwaltung seit 2008 entwickelten Open eGov LocalSigner elektronisch signiert werden. Die Funktionalitäten sind hier beschränkt und die Erstellung einer elektronischen Signatur bedingt einige «Klicks». Im Rahmen der Weiterentwicklung von Acta Nova ist geplant, den Open eGov LocalSigner abzulösen und den serverbasierten Signatordienst anzubinden. Die Erweiterung der bisherigen Einzelsignatur mit einer Stapelsignatur-Funktionalität wird voraussichtlich ab Herbst 2021 bundesweit eingeführt. Im Herbst 2020 konnte schon die Massensiegelungs-Funktionalität aus Fachanwendungen eingeführt werden, die seit März 2021 von Fachanwendungen aktiv genutzt wird. Bis dahin ist daher die Erstellung einer elektronischen Signatur über Open eGov LocalSigner oder deren Überprüfung mit Hilfe des Validators zwar möglich, aber bis dato umständlicher und aufwendiger als der Einsatz von GEVER-Bestätigungen.

Für effiziente, schlanke Verwaltungsabläufe ist es wichtig, dass nur dort das praktisch und technisch anspruchsvollere Mittel eingesetzt wird, wo dies auch tatsächlich nötig ist. Im bundesverwaltungsinternen Verkehr genügen im Allgemeinen die blossen GEVER-Bestätigungen; elektronische Signaturen und Siegel sind im Allgemeinen bundesverwaltungsintern nicht erforderlich aber gleichwohl - wie unter Ziffer 2.4 dieses Berichts ausgeführt - in gewissen Fällen sinnvoll oder sogar notwendig. Das Einsatzgebiet von elektronischen Signaturen liegt somit primär bei rechtlich bedeutsamen Dokumenten, die mit Personen und Stellen mehrheitlich *ausserhalb* der Bundesverwaltung ausgetauscht werden.³⁶

4 Zusammenfassung

4.1 Mehrwert der elektronischen Bestätigung im Vergleich zur elektronischen Signatur

Für effiziente und schlanke Verwaltungsabläufe ist es wichtig, dass nur dort das praktisch und technisch aufwändigere Mittel – d. h. die persönliche elektronische Signatur oder das elektronische Siegel – eingesetzt wird, wo nötig. Im bundesverwaltungsinternen Verkehr genügen im Allgemeinen die GEVER-Bestätigungen und allenfalls, die bezüglich Nachvollziehbarkeit als vergleichbar zu betrachtenden fortgeschrittenen elektronischen Signaturen (Klasse B). Die qualifizierte Signatur oder das geregelte Siegel muss bzw. sollte - ausser den in Ziffer 2.4 ausgeführten bundesverwaltungsinternen Ausnahmen - v. a. bei rechtlich bedeutsamen Dokumenten eingesetzt werden, die mit Personen und Stellen *ausserhalb* der Bundesverwaltung ausgetauscht werden.

Der Mehrwert einer elektronischen Bestätigung ist deren Einfachheit. Die insgesamt zeitaufwändigeren elektronischen Signaturen sollen nur wo nötig oder sinnvoll eingesetzt werden.

4.2 Rechtliche «Hindernisse» oder anderer Handlungsbedarf

Wie die Ausführungen unter Ziffer 2.4 gezeigt haben, sind die nötigen bundesverwaltungsinternen Voraussetzungen für die elektronische Geschäftsführung vorhanden, sei es im Sinne elektronischer Bestätigungen (Ziff. 3.2) oder elektronischer Signaturen (Ziff. 3.3). Hinsichtlich der elektronischen Bestätigungen können die Bundesangestellten das elektronische Geschäftsverwaltungssystem Acta Nova nutzen. Gerade während der Corona Zeit und dem damit verbundenen Homeoffice hat sich gezeigt, dass der Austausch von Dokumenten auf Papier weitestgehend unnötig ist, und dass eine rein elektronische Geschäftsabwicklung möglich ist. Dies hat letztlich beim wichtigsten Faktor der Nutzung der elektronischen Geschäftsverwaltung – dem Menschen – zu einem erstarkten Bewusstsein geführt. So wurde die Entwicklung zur rein digitalen Abwicklung von Geschäften durch Corona stark beschleunigt.

³⁶ So können insbesondere privatrechtliche Verträge und Verwaltungsverfügungen, für deren Gültigkeit gesetzlich eine qualifizierte elektronische Signatur vorgesehen ist, nicht mit blosser GEVER-Bestätigung ausgestellt werden. Dieses Formerfordernis ist bei Verwaltungsverfügungen der Normalfall (Art. 34 Abs. 1^{bis} des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968 [VwVG; SR 172.021] und Art. 9 Abs. 4 und 5 der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens [VeÜ-VwV, SR 172.021.2]). Demgegenüber drängt sich der Einsatz der Schriftform auch ohne gesetzliches Erfordernis aus praktischen Gründen in vielen Fällen auf, um Klarheit zu schaffen, was Inhalt des Vertrags ist und ob erst ein Entwurf vorliegt oder schon ein von allen Seiten akzeptierter und damit verbindlicher Vertrag.

E-Signatur für verwaltungsinterne Dokumente

Nicht zuletzt der Bundesrat selber hat am 30. Januar 2019 ein starkes Zeichen für die Digitalisierung gesetzt, indem er beschlossen hat, dass die handschriftliche Unterschrift und die elektronische Signatur für das Mitberichtsverfahren einander gleichgestellt sind (vgl. Ziff. 2.4.6).

5 Schlussfolgerungen

Nicht nur seit der Überweisung des Postulats 18.3502 Dobler «E-Signatur für bundesverwaltungsinterne Dokumente» hat sich die Bundesverwaltung rasch technisch weiterentwickelt: einerseits bei der nun abgeschlossenen Einführung des vereinheitlichten GEVER-Systems Acta Nova, andererseits auch beim Aufbau und der Einbindung der neuen serverbasierten Signatordienste.

Insgesamt kommt der vorliegende Bericht zum Schluss, dass kaum Handlungsbedarf besteht. Im Bereich der Rechtsgrundlagen zur elektronischen Signatur sind diese – für den bundesverwaltungsinternen Bereich – ausreichend. Hingegen hat sich gezeigt, dass die technischen Voraussetzungen für die Verwendung der elektronischen Signatur noch verbessert werden könnten (Stichwort Ablösung des in die Jahre gekommenen Open eGov LocalSigner). Die Arbeiten zu dessen Ablösung durch die Signatordienste 2.0 und deren Anbindung an Acta Nova und einige wichtige Fachanwendungen sind aber im Gange und werden voraussichtlich bis Ende 2021 abgeschlossen (Ziff. 3.3).

Wann immer möglich sollte bei bundesverwaltungsinternen Geschäften auf die Verwendung einer elektronischen Signatur verzichtet werden und stattdessen die bestehenden Acta Nova Funktionen der GEVER-Bestätigungen und die analogen Funktionen von SAP-ERP verwendet werden. Elektronische Signaturen sind nur bei finalen Dokumenten (Verträgen, Vereinbarungen, interne Verfügungen) und nur in den Fällen einzusetzen, wo Dokumente das GEVER-System verlassen oder ausserhalb des GEVER-Systems aufbewahrt werden und eines besonderen Schutzes ihrer Integrität und Authentizität bedürfen. Entsprechend ist dies in der laufend nachgeführten bundesinternen Einsatzrichtlinie (Weisung und IKT-Vorgabe) E018 «Einsatz und Validierung von elektronischen Signaturen in PDF-Dokumenten» geregelt.

Da die Mitarbeitenden entweder mit ihrem Authentisierungszertifikat identifiziert (2-Faktor mit Zertifikaten der Klasse B) im GEVER-System oder in Fachanwendungen arbeiten oder mit ihrem fortgeschrittenen Signaturzertifikat (Klasse B) Dokumente (PDF) und E-Mail unterschreiben können, besteht in Bezug auf die elektronische Signatur bundesverwaltungsinterner Dokumente und elektronischer Geschäftsprozesse somit kein Defizit, weder an Infrastruktur noch an Regelungen. Für den bundesverwaltungsinternen Bereich sind in den Fällen, in denen GEVER-Bestätigungen nicht geeignet sind, fast ausschliesslich Signaturen mit den fortgeschrittenen Signaturzertifikaten (Klasse B) ausreichend.

Jede Verwaltungseinheit ist gefordert, die für sie geltenden rechtlichen Regelungen im Detail zu analysieren und Prozessabläufe zu vereinfachen. Dabei sollen die seltenen Fälle bestimmt werden, in denen bundesverwaltungsinterne Dokumente *qualifiziert* zu signieren sind (vgl. z. B. Ziff. 2.4.5). Entsprechend sind die hierfür zuständigen Personen mit einem qualifizierten Signaturzertifikat (Klasse A), welches beim BIT jederzeit bestellbar ist, auszustatten.

Zudem unterstützt der Bereich DTI der BK weiterhin die Parlamentsdienste bzgl. eines möglichen Bezugs der Standarddienste Bund, um den papierlosen Schriftverkehr zwischen Exekutive und Parlament umzusetzen, z. B. im Bereich der Zusatzdokumentationen zu Voranschlag und Staatsrechnung.

Das Anliegen des vorliegenden Postulats ist insofern erfüllt, weil die elektronischen Unterschriften für alle Einsatzbereiche verwendet werden *können*. Es besteht kein Zwang, dass sie eingesetzt werden *müssen* (bzw. dass auf die physische Unterschrift verzichtet werden muss). Zusätzlich zu den aufgeführten drei Massnahmen werden vier Massnahmen umgesetzt, mit denen eine effizientere Nutzung elektronischer Signaturen in der Bundesverwaltung weiter verbessert werden können:

Artikel 29 RVOV sieht vor, dass die Departemente und das Bundeskanzlei ein Organisationsreglement erlassen, das u.a. Regelungen zur Unterschrift enthält (Abs. 1), und dass dieses Reglement zu veröffentlichen ist (Abs. 3). Artikel 49 Absatz 3 RVOG schreibt nicht nur vor, dass die Leiter der Gruppen und

E-Signatur für verwaltungsinterne Dokumente

Ämter sowie die Generalsekretäre die Unterschriftsdelegation in ihrem Zuständigkeitsbereich regeln müssen, sondern auch, dass Verträge, Beschlüsse und andere formelle Verpflichtungen des Bundes, die einen Betrag von 100 000 CHF übersteigen, jeweils von 2 Personen unterzeichnet werden müssen.

Massnahme 4

Alle Departemente und die BK werden beauftragt, im Rahmen der Revision von Gesetzen und Verordnungen in ihren Bereichen sicher zu stellen, dass im Sinne von «digital first» elektronische Varianten zur Geschäftsabwicklung mit internen und externen Personen und Stellen unter Berücksichtigung der bundesinternen «Einsatzrichtlinie E018» angeboten werden.

Die Unterschriftenregelungen sind für den elektronischen Bereich in dem Sinne anzupassen, dass bestimmt wird, für welche Geschäfte mit qualifizierter elektronischer Signatur, für welche mit der fortgeschrittenen elektronischen Signatur (Klasse B) und für welche durch wen mit einem geregelten elektronischen Siegel signiert werden darf. Dabei sind auch die Vorschriften der Finanzhaushaltsverordnung (FHV, SR 611.01) Art. 37ff betreffend die Unterschriftenregelung bei Belegen und Zahlungsfreigaben zu beachten. Ebenso sind allfällige zivilrechtliche Formvorschriften einzuhalten.

Massnahme 5

Alle Departemente und die BK werden beauftragt, bis Ende 2022 ihre Unterschriftenregelung zu überarbeiten mit dem Ziel, dass möglichst einfache Verfahren eingesetzt werden können. In bundesinternen Geschäftsprozessen sollen formale Unterschriften im rechtlichen Sinne (handschriftliche oder qualifizierte elektronische Unterschriften nach ZertES) nur dann verlangt werden, wenn dies aufgrund ausdrücklicher Gültigkeitsvoraussetzung oder aufgrund zivilrechtlicher Formvorschriften notwendig ist. Entscheide werden in anderen Fällen über fortgeschrittene Zertifikate der Klasse B oder über Bestätigungen/Visierungen im Rahmen von Geschäftsprozessen gefällt und dokumentiert (z.B. GE-VER oder SAP). Die Departemente und die BK sorgen dafür, dass die Überarbeitung der Unterschriftenregelung in ihren Verwaltungseinheiten umgesetzt wird.

Damit die Verwendung der verschiedenen Möglichkeiten der elektronischen qualifizierten Signatur, fortgeschrittenen Signatur, elektronischen Siegel und Protokollierung der Geschäftsprozesse effizient erfolgt, sollen Hilfsmittel erstellt und den Verwaltungseinheiten zur Verfügung gestellt werden.

Damit bundesinterne wie auch bundesexterne Personen und Stellen sich einfach informieren können, ist zudem die Internet-Webseite³⁷ des BIT rund um die elektronische Signatur und die Internet Webseite des BAKOM zur elektronischen Signatur³⁸ zugänglich.

Massnahme 6

Die BK (DTI) wird beauftragt, bis Ende 2021 ein Hilfsmittel zu erstellen zur Frage, welche Arten von Willensbekundungen sich in welchen Fällen der internen und externen Zusammenarbeit anbieten und bewährt haben.

³⁷ www.bit.admin.ch/bit/de/home/themen/elektronische-signatur.html

³⁸ www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html

E-Signatur für verwaltungsinterne Dokumente

Der gesetzlich vorgeschriebene Identifikationsprozess für die Ausgabe eines qualifizierten Zertifikates soll effizienter und v. a. «kundenfreundlicher» ausgestaltet werden. Insbesondere ist auch für Mitarbeitende ausserhalb von Bern zu prüfen, wie erreicht werden kann, dass sie sich nicht mehr pro auszustellendes Zertifikat persönlich jedes Mal vor Ort (d. h. bei der Swiss Government PKI beim BIT) ausweisen, obwohl sich die Mitarbeitenden bereits bei Stellenantritt persönlich identifiziert haben.

Massnahme 7

Die BK (DTI) wird beauftragt, unter Einbezug des EFD (BIT) bis Ende 2022 sicherzustellen, dass die zertifizierten Bewirtschaftungsprozesse von elektronischen Zertifikaten, insbesondere von qualifizierten Zertifikaten und von geregelten elektronischen Siegeln, innerhalb der zentralen Bundesverwaltung effizienter und leistungsfähiger gestaltet werden.