14.015

Botschaft zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES)

vom 15. Januar 2014

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf zur Totalrevision des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

15. Januar 2014

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Didier Burkhalter
Die Bundeskanzlerin: Corina Casanova

Übersicht

Die vorliegende Totalrevision klärt und vereinfacht den Einsatz elektronischer Zertifikate für juristische Personen und Behörden und befriedigt damit die Bedürfnisse der Wirtschaft und der Verwaltung nach einer zeitgemässen, effizient anwendbaren Regelung.

Ausgangslage

Im Bundesgesetz über die elektronische Signatur von 2003 (ZertES) ist die qualifizierte elektronische Signatur, welche die Grundlage für die Gleichstellung mit der eigenhändigen Unterschrift im OR bildet, natürlichen Personen vorbehalten. Diese Einschränkung war als Schutz vor der Untergrabung fundamentaler Konzepte im Vertretungsrecht gedacht. Schon damals wurde die Frage eines geregelten Zertifikats für juristische Personen und Behörden intensiv diskutiert. Es war umstritten, ob mit der Einschränkung auf natürliche Personen die Latte nicht zu hoch gesetzt sei und insbesondere die Anwendung für Massengeschäfte zu kompliziert sei.

Inhalt der Vorlage

Mit der vorliegenden Totalrevision des ZertES soll dem Bundesrat die Kompetenz gegeben werden, nebst der bisherigen qualifizierten elektronischen Signatur, die weiterhin nur natürlichen Personen zugänglich ist, zwei weitere, ähnliche Anwendungen von elektronischen Zertifikaten zu regeln. Nebst der geregelten elektronischen Signatur, an die reduzierte Anforderungen gestellt werden, ist dies das geregelte elektronische Siegel, welches auch juristischen Personen und Behörden zugänglich ist. Beide neuen Anwendungen dürfen keinesfalls mit dem rechtlichen Konzept der elektronischen Unterschrift verwechselt werden. Ihre Verwendung hat keine direkten Rechtswirkungen und dient lediglich dazu, den Herkunftsnachweis sowie die Integrität der betreffenden Mitteilung zu gewährleisten.

Als weitere Anwendung elektronischer Zertifikate soll ferner die sichere Authentifizierung rechtlich geregelt werden. Schliesslich soll, wo immer möglich, der Einbezug der elektronischen Signatur oder des elektronischen Siegels in den verschiedenen Gesetzen und Verordnungen terminologisch bereinigt bzw. vereinfacht werden.

An den bestehenden Konzepten und Prinzipien der bisherigen Regelung, insbesondere der nicht abschliessenden Regelung von Zertifikatsprodukten, soll nichts geändert werden. Auch soll die schweizerische Gesetzgebung mit der entsprechenden europäischen Richtlinie weiterhin kompatibel bleiben.

Dass die Vorlage trotz der eigentlich wenigen materiellen Änderungen als «Totalrevision» bezeichnet wird, liegt daran, dass durch die Ausweitung von einer auf zwei geregelte Signaturen und die Anpassungen in der Terminologie die Mehrheit der Artikel von Änderungen betroffen war.

Inhaltsverzeichnis

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage

1.1.1 Problemstellung und Abklärungen

Im Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES; SR *943.03*) ist die qualifizierte elektronische Signatur, welche die Grundlage bildet für die Gleichstellung mit der eigenhändigen Unterschrift im Bundesgesetz betreffend die Ergänzung des Zivilgesetzbuches (Fünfter Teil: Obligationenrecht, OR; SR *220*), natürlichen Personen vorbehalten. Diese Einschränkung war als Schutz vor der Untergrabung fundamentaler Konzepte im Vertretungsrecht gedacht. Schon damals wurde die Frage eines geregelten Zertifikats für juristische Personen und Behörden intensiv diskutiert, und es war umstritten, ob mit der Einschränkung der elektronischen Signatur auf natürliche Personen die Latte nicht zu hoch gesetzt und insbesondere die Anwendung für Massengeschäfte zu kompliziert sei.

Im Nachgang zur Motion Baumann vom 3. Oktober 2008 (08.3741; Gesetzeswidrige Zertifizierungsanforderungen in MWSt-Verordnung) wurde dem BJ vom EJPD der Auftrag erteilt, vertiefte Abklärungen über die Revisionsbedürftigkeit des ZertES zu treffen. Es soll sichergestellt sein, dass dieses Gesetz auf die Bedürfnisse einer erfolgreichen Umsetzung der Strategie des Bundesrates zur Informationsgesellschaft Schweiz ausgerichtet ist.

In der Folge wurde der Handlungsbedarf analysiert. Diese Erkenntnisse flossen ein in den Bericht der interdepartementalen Arbeitsgruppe über die Ergebnisse des Prüfauftrages bezüglich Umsetzung der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz: Sicherstellung der Rechtsgrundlagen (vgl. Ziff. 3.3.3). Der Bundesrat hat den Bericht am 11. Juni 2010 zur Kenntnis genommen und das EJPD beauftragt, den konkreten Regelungsbedarf abzuklären.

Tatsächlich besteht im elektronischen Geschäfts- und Behördenverkehr ein grosser Bedarf nach Unternehmens- resp. Behördenzertifikaten. Gerade bei Massengeschäften ist es kaum praktikabel, die grosse Zahl der Meldungen regelkonform mit persönlichen Zertifikaten zu signieren. In solchen Fällen wird daher üblicherweise eine sogenannte fortgeschrittene Signatur eingesetzt, die auf das Unternehmen oder gar nur den Server lautet, und es werden – falls nötig – Formeinreden vertraglich ausgeschlossen. Dieses Vorgehen ist aber immer mit dem Nachteil verbunden, dass nicht auf eine bestimmte, staatlich definierte Qualität von Zertifikaten verwiesen werden kann, sondern diese im Einzelfall definiert werden muss.

Im einzigen Fall, in dem tatsächlich eine grosse Zahl von signierten Meldungen zwischen Wirtschaft und Verwaltung ausgetauscht wird, nämlich bei der Übermittlung der Rechnungen an die MWST-Verwaltung zur Anmeldung des Vorsteuerabzugs, wurde vom Finanzdepartement auf dem Verordnungsweg ein eigenes Unternehmenszertifikat geregelt und durchgesetzt. Dieses Vorgehen gab denn auch den Anlass für die vorstehend erwähnte Motion Baumann.

Das geschilderte Problem stellt sich nicht nur für private Unternehmen, sondern auch für Behörden, beispielsweise bei der automatisierten Produktion von Auszügen

aus dem Strafregister, dem Handelsregister oder dem Grundbuch. Entweder wird das qualifizierte Zertifikat einer bestimmten Person, z.B. des Registerführers verwendet – und bei jeder Personalmutation ebenfalls mutiert –, oder es muss ein fortgeschrittenes Zertifikat ohne gesetzlich definierte Qualität verwendet werden.

Diese Erfahrungen decken sich mit den Erfahrungen in anderen europäischen Ländern. So hat Österreich beispielsweise mit einem eigenen Erlass die sogenannte Amtssignatur eingeführt, bei der sich das Zertifikat auf eine bestimmte Behörde bezieht.

Im Zentrum der vorliegenden Revision steht somit das Anliegen, dass für juristische Personen resp. Behörden ebenfalls eine Funktion bereitgestellt wird, welche den Ursprung und die Integrität eines Dokuments nachweist.

Als weitere dringende Anliegen wurden die Regelung der elektronischen Authentifizierung, die Beseitigung von Unsicherheiten beim Umgang mit elektronisch signierten Dokumenten und die Vereinheitlichung der Terminologie in der gesamten Rechtsetzung genannt.

1.1.2 Ziele der Totalrevision

Mit der vorliegenden Totalrevision sollen prioritär drei Ziele erreicht werden.

- Erstens soll als Ergänzung zur bisherigen qualifizierten elektronischen Signatur, die nur natürlichen Personen zugänglich ist, juristischen Personen und Behörden ebenfalls ein Instrument zur Verfügung gestellt werden, mit welchem Sie den Ursprung und die Integrität eines Dokuments sichern können. Dieses Instrument kann zudem auf der Stufe der technischen Ausführungsvorschriften noch weiter auf die Anforderungen des geschäftlichen Einsatzes ausgerichtet werden. Der Gesetzgeber, der Formvorschriften festlegt, hätte somit künftig die Wahl zwischen der bisherigen qualifizierten elektronischen Signatur, der neuen geregelten elektronischen Signatur oder dem neuen geregelten elektronischen Siegel.
- Zweitens soll die gesetzliche Grundlage geschaffen werden, dass nebst der elektronischen Signatur auch die sichere Authentifizierung mit Zertifizierungsdienste-Produkten geregelt werden kann. In der Praxis wird das Vertrauen zwischen Partnern im elektronischen Verkehr in der Mehrzahl der Fälle nicht durch eine signierte Meldung, sondern durch die Authentisierung gegenüber einem Online-Dienst hergestellt.
- Schliesslich soll wo immer möglich eine terminologische Bereinigung bzw. Vereinfachung bei der Regelung der elektronischen Signatur in den verschiedenen Gesetzen und Verordnungen herbeigeführt werden.

Zusätzlich soll im Rahmen der Revisionsarbeiten geprüft werden, ob neu allenfalls ein Zeitstempel obligatorischer Bestandteil einer qualifizierten elektronischen Signatur sein soll.

Für die ersten zwei Punkte ist heute keine genügende Delegationsnorm im ZertES vorhanden. Mit der Totalrevision soll dem Bundesrat deshalb die Kompetenz gegeben werden, einen weiteren Typ von Signatur und weitere Anwendungen von Zertifikaten, insbesondere die Authentifizierung, in der Verordnung und mit technischen Vorgaben zu regeln.

Bei allen Änderungen soll an den bestehenden Konzepten und Prinzipien der bisherigen Regelung, insbesondere der nicht abschliessenden Regelung von Zertifikatsprodukten, nichts geändert werden. Auch die Kompatibilität der schweizerischen Gesetzgebung mit der europäischen Signaturrichtlinie (Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen; nachfolgend: EU-Richtlinie) soll im Hinblick auf eine zukünftige internationale Anerkennung nicht tangiert werden. Aus diesem Grunde wurden auch der für die Schweiz eher untypische Aufbau des Gesetzes mit den umfangreichen Begriffsdefinitionen und die europäisch geprägte Terminologie beibehalten, wenn nicht aus inhaltlichen Gründen eine Änderung notwendig war.

Wenn man sich das Ergebnis der Totalrevision unter dem Aspekt des Produktesortiments von Anbieterinnen von Zertifizierungsdiensten anschaut, soll dieses künftig wie folgt aussehen:

- *Jede beliebige Anbieterin* kann beliebige Zertifikate und andere Zertifizierungsprodukte für beliebige Anwendungen anbieten, ausser dem geregelten und dem qualifizierten Zertifikat und dem qualifizierten Zeitstempel.
- Eine *nach ZertES anerkannte Anbieterin* kann alle vorstehend genannten Produkte anbieten plus die drei vom revidierten ZertES geregelten Produkte:
  - Geregelte Zertifikate (neu):
    - Für natürliche und juristische Personen resp. Behörden
    - Für verschiedene Anwendungen (ausser für die qualifizierte elektronische Signatur) gemäss Ausführungsvorschriften des Bundesrates bzw. des Bundesamtes für Kommunikation (BAKOM).
  - Qualifiziertes Zertifikat (unverändert):
    - Nur für natürliche Personen
    - Nur für die qualifizierte elektronische Signatur
  - Qualifizierter Zeitstempel (neu)

1.2 Die beantragte Neuregelung

1.2.1 Geregeltes Zertifikat, geregelte elektronische Signatur und geregeltes elektronisches Siegel

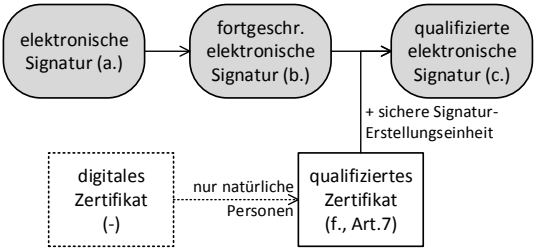
Das *bisherige Gesetz* definiert – in Übereinstimmung mit der EU-Richtlinie – die qualifizierte elektronische Signatur unter Verwendung eines qualifizierten Zertifikats und gibt dem Bundesrat in Artikel 6 die Kompetenz, die dazu verwendete Schlüsselgenerierung sowie die zugehörigen Signaturerstellungseinheiten zu regeln. Die wesentlichen Inhalte eines qualifizierten Zertifikats werden in Artikel 7 vorgegeben. Der Bundesrat erhält die Kompetenz zur Regelung des Zertifikatformats.

Basierend auf der elektronischen Signatur (Art. 2 Bst. a) wurde *bisher* die fortgeschrittene elektronische Signatur (Art. 2 Bst. b) als zweite Stufe und die qualifizierte elektronische Signatur (Art. 2 Bst. c) als dritte Stufe definiert. Die qualifizierte elektronische Signatur hat alle Anforderungen an die fortgeschrittene elektronische Signatur zu erfüllen und diese wiederum alle Vorgaben der elektronischen Signatur.

Nach geltendem Recht sieht die Kaskade der elektronischen Signaturen wie folgt aus:

Abbildung 1

Kaskade der elektronischen Signaturen nach geltendem Recht

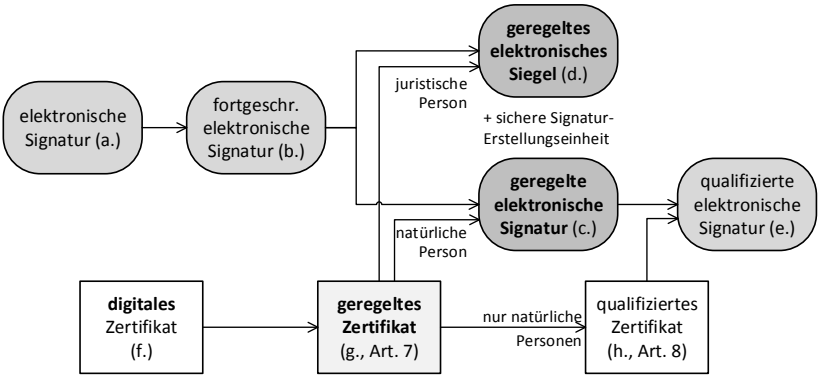


Dies bleibt in der revidierten Version unverändert, es wird jedoch als Vorstufe der qualifizierten elektronische Signatur neu die «geregelte elektronische Signatur» für natürliche Personen resp. das «geregelte elektronische Siegel» für juristische Personen und Behörden eingeführt.

Neu sieht die Kaskade demnach wie folgt aus: Basis für alle Signaturen und das neue Siegel bleibt die elektronische Signatur und die auf ihr basierende fortgeschrittene elektronische Signatur als zweite Stufe. Neu wird als dritte Spezialisierungsstufe für natürliche Personen die geregelte elektronische Signatur und für juristische Personen und Behörden das geregelte elektronische Siegel eingeführt. Erst in der vierten Stufe steht nun die qualifizierte elektronische Signatur. Die qualifizierte elektronische Signatur hat alle Anforderungen an die geregelte elektronische Signatur zu erfüllen und diese wiederum alle Vorgaben der fortgeschrittenen elektronischen Signatur.

Abbildung 2

Neue Kaskade der elektronischen Signaturen gemäss Entwurf



Im geltenden Recht basiert die qualifizierte elektronische Signatur auf einem qualifizierten Zertifikat. Dies bleibt in der revidierten Version unverändert, es wird jedoch als Vorstufe des qualifizierten Zertifikats neu das «geregelte Zertifikat» mit

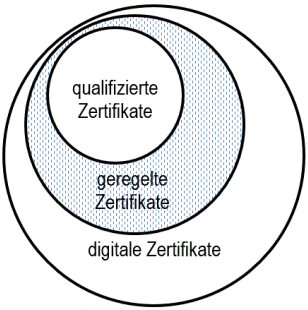
etwas weniger restriktiven Anforderungen definiert. Anwendungen des geregelten Zertifikats sind:

- die «geregelte elektronische Signatur» für natürliche Personen,
- das «geregelte elektronische Siegel» für juristische Personen und Behörden,
- sowie weitere Anwendungen gemäss Ausführungsvorschriften zu diesem Gesetz, insbesondere die sichere Authentifizierung.

Der Bundesrat erhält die Kompetenz, auch die Generierung und Anwendung der zu diesen Zertifikaten gehörigen Schlüssel zu regeln und die Formate der Zertifikate festzulegen.

Abbildung 3

Kaskade der elektronischen Zertifikate gemäss Entwurf



Das digitale Zertifikat bildete zwar schon bisher die Basis für das qualifizierte Zertifikat, war aber seinerseits im Gesetz nicht definiert.

Neu ist das geregelte Zertifikat ein Spezialfall des digitalen und das qualifizierte ein Spezialfall des geregelten. Jedes qualifizierte Zertifikat ist somit auch ein geregeltes, wodurch alle Vorschriften für die geregelten Zertifikate (insbes. Art. 7) auch für die qualifizierten gelten.

Der wesentlichste Unterschied des qualifizierten Zertifikats zum geregelten ist, dass das qualifizierte – wie bisher – nur natürlichen Personen zugänglich ist, wohingegen das geregelte Zertifikat nebst natürlichen auch juristischen Personen oder Behörden als Inhaberinnen aufweisen kann. Das geregelte Zertifikat kann demnach kein reines Maschinenzertifikat sein, also einzig auf eine Maschine wie z.B. einen Server ausgestellt sein.

Im Hinblick auf die terminologische Vereinfachung wird beim geregelten und beim qualifizierten Zertifikaten schon in der Definition (vgl. Art. 2 Bst. g und h) neu die Anforderung gestellt, dass sie von einer anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt sein müssen. Diese Ergänzung vereinfacht die Art, wie die in der Schweiz normalerweise anerkannte elektronische Signatur benannt werden kann. Bisher war dazu eine Formulierung wie die nachstehende notwendig: «Anerkannt wird die qualifizierte elektronische Signatur nach ZertES, welche mit einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten erstellt wurde.» Zwar bedingte die qualifizierte elektronische Signatur ein qualifiziertes Zertifikat, ein solches hätte aber bisher theoretisch auch von einer nicht anerkannten Anbieterin stammen können. Da solche Produkte auf dem Markt nicht existieren und auch keine sinnvolle Anwendung dafür absehbar ist, werden sie in der neuen Definition ausgeschlossen. Mit der neuen Verkettung wird inskünftig die nachstehende Formulierung genügen: «Anerkannt wird die qualifizierte elektronische Signatur nach ZertES.»

Wenn nun im neuen Gesetz dem Bundesrat die Kompetenz gegeben wird, zwei statt bisher eine Klasse von Zertifikaten zu regulieren, so darf dabei nicht übersehen werden, dass es darüber hinaus jeder anerkannten oder auch nicht anerkannten Anbieterin von Zertifizierungsdiensten frei steht, beliebige andere Zertifikate anzubieten.

Damit die Kompetenz des Bundesrates zur Regelung der Generierung, Speicherung und Anwendung der Schlüssel nicht für jeden Anwendungsfall von Zertifikaten – die geregelte elektronische Signatur, das geregelte elektronische Siegel, die qualifizierte elektronische Signatur, die nachstehend beschriebene Authentifizierung und allenfalls weitere Anwendungen – separat formuliert werden muss, wurde der bisherige Artikel 6, der dies für die qualifizierte elektronische Signatur bestimmte, durch einen neuen, anwendungsneutralen Artikel 6 ersetzt. Er gibt dem Bundesrat diese Kompetenz also nicht mehr nur für eine bestimmte Anwendung der beiden geregelten Zertifikatstypen, sondern für beliebige Anwendungen. Die bisherigen Kompetenzen bezüglich qualifizierter elektronischer Signatur bleiben die gleichen und damit bleibt auch die Kompatibilität zur EU-Richtlinie erhalten. Der Bundesrat erhält einzig die gleiche Kompetenz zur Regelung der Generierung, Speicherung und Anwendung der Schlüssel auch für einen zweiten, landesspezifischen Typ von Zertifikaten und für weitere Anwendungen dieser Zertifikate.

1.2.2 Regelungskompetenz auch für Authentifizierung

Für einen gedeihlichen elektronischen Geschäftsverkehr unter Privaten sowie auch mit Behörden ist es für die teilnehmenden Partner wichtig, sicher zu sein, mit wem genau sie kommunizieren, bzw. sicher zu sein, ob die andere Seite auch wirklich die ist, die sie vorgibt zu sein.

Als das heutige ZertES vor rund zehn Jahren geschaffen wurde, ging man davon aus, dass der elektronische Geschäftsverkehr primär durch den Austausch von Meldungen in der Art von E-Mail oder strukturierten Daten geschehen und die Sicherheit über die Identität der Absenderinnen und Absender demzufolge durch elektronisch signierte Meldungen hergestellt würde. Dieses Kommunikationsmodell hat sich nur in Teilbereichen und eher für die Kommunikation unter professionellen Geschäftspartnern durchgesetzt. Hingegen läuft die Online-Kommunikation immer häufiger nach dem Modell, dass sich der eine Kommunikationspartner – meist der Kunde oder die Bürgerin – bei einem Anwendungssystem bzw. Portal der anderen Kommunikationspartnerin – meist die Unternehmung oder Behörde – anmeldet und auf diesem System ihr resp. sein Geschäft abwickelt. Oder die Anmeldung geschieht eine Ebene tiefer, indem sich eine Anwendung des Kunden mit einem Webdienst der Anbieterin verbindet und die beiden Programme sich gegenseitig authentifizieren. In beiden Fällen wird die Gewissheit über die Identität des Kommunikationspartners sofort bei der Verbindung der beiden Systeme über eine sogenannte Authentisierung (aus Sicht der anmeldenden Person) bzw. Authentifizierung (aus Sicht des Dienstes) bewerkstelligt. Zwar werden bei diesem Verfahren auf einer tieferen Ebene auch signierte Meldungen ausgetauscht, jedoch nicht in der Art von willentlich signierten Meldungen. Entsprechend werden grundsätzlich auch gleiche Zertifikate wie für die elektronische Signatur verwendet, allerdings nicht das gleiche Zertifikat für beide Anwendungen, weil sonst gewisse Angriffe durch Dritte und somit Missbräuche möglich wären.

Die Wirtschaft wünscht sich daher schon lange auch für bestimmte Fälle der Authentifizierung ein vom Staat geregeltes Zertifikat, das durch seinen offiziellen Charakter und eine geregelte Qualität zusätzliche Sicherheit in die Verhältnisse bringen könnte. Es gibt verschiedene heutige und geplante Anwendungen, die hohe Anforderungen an Datenschutz und Informationssicherheit stellen, beispielsweise im Bereich eHealth das Patientendossier, wo eine starke Authentisierung notwendig ist und entsprechende Zertifikate hoch willkommen wären.

Das bisherige qualifizierte Zertifikat ist dafür prädestiniert, für elektronische Signaturen, insbesondere die qualifizierte elektronische Signatur mit ihren besonderen Wirkungen, eingesetzt zu werden. Aus technischen Gründen, bzw. weil sonst gewisse Tore für Angriffe gegen die sichere Signierung geöffnet würden, wird es aber auch auf die Verwendung für die elektronische Signatur eingeschränkt.

Das neue, leicht weniger anspruchsvolle Zertifikat, das geregelte Zertifikat, soll – als Typus – dieser Spezialisierung nicht unterliegen. Dieser Typ von Zertifikat lässt sich aus rechtlicher Sicht sowohl für elektronische Signaturen und Siegel in verschiedenen Einsatzgebieten verwenden, beispielsweise für die Archivierung, die Siegelung von Programmen oder das Signieren von E-Mails, als auch für die Authentifizierung oder auch andere Sicherheitsanwendungen wie das SSL-Zertifikat.

Gesetzgebungstechnisch werden daher neu alle Formulierungen, die bisher auf die Anwendung des Zertifikats für die Signatur ausgerichtet waren, anwendungsneutral formuliert. So wird z.B. nicht mehr von Signatur- oder Signaturprüfschlüssel gesprochen, sondern von öffentlichen und privaten kryptografischen Schlüsseln. Dabei ist zu beachten, dass mit diesen neuen, offeneren Formulierungen für das qualifizierte Zertifikat, das nur zu Signaturzwecken eingesetzt wird, sich materiell nichts ändert.

1.2.3 Zeitstempel als obligatorischer Bestandteil der elektronischen Signatur

In den letzten Jahren wurde in der einschlägigen Branche mehrfach die Forderung laut, die qualifizierte elektronische Signatur obligatorisch mit einem sicheren Zeitstempel anzureichern. Ein Zeitstempel signiert, bzw. siegelt die Quersumme einer Datei zusammen mit einer offiziellen Zeit, womit – sofern der Zeitstempel vertrauenswürdig ist – bewiesen werden kann, dass eine bestimmte Datei zu einem bestimmten Zeitpunkt existierte, oder dass eine Signatur zu einem bestimmten Zeitpunkt erstellt worden ist. Ohne Zeitstempel hat der Zeitpunkt einer Signatur streng genommen nur den Wert einer unbestätigten Behauptung. Gewisse Angriffe, bzw. Betrugsszenarien lassen sich nur verhindern, indem die elektronische Signatur mit einem Zeitstempel verbunden wird. Im Hinblick auf diesen Sachverhalt sind schon heute nach Artikel 12 des geltenden ZertES die anerkannten Anbieterinnen von Zertifizierungsdienstleistungen verpflichtet, einen Zeitstempeldienst anzubieten.

Heutige Signaturprogramme bieten normalerweise die Integration eines Zeitstempels in die Signatur an. Meist kann diese Variante auch als Standardvorgabe eingestellt werden.

Für die Einbettung eines Zeitstempels in die elektronische Signatur muss man zum Zeitpunkt des Signierens mit dem Internet verbunden sein. Diese Anforderung stellte zum Entstehungszeitpunkt des heutigen ZertES noch eine zu hohe Hürde dar. Als

Beispiel dafür wurde oft der Notar genannt, der anlässlich einer Gründungsversammlung vor Ort Statuten oder Protokolle mit seiner Unterschrift beglaubigen sollte. Inzwischen ist diese Bedingung wesentlich einfacher einzuhalten, in wenigen Jahren dürfte sie in fast jeder Situation selbstverständlich erfüllt sein.

Im Rahmen der Revisionsarbeiten zum Gesetz wurden drei Ansätze für eine Einbindung von Zeitstempeln geprüft und in die Vernehmlassung gegeben:

1. Zu einer qualifizierten elektronischen Signatur gehört per definitionem zwingend der Zeitstempel einer anerkannten Anbieterin von Zertifizierungsdiensten.
2. Es werden zwei Subtypen von qualifizierten elektronischen Signaturen vorgesehen, einer mit und der andere ohne Zeitstempel.
3. Der Zeitstempel wird zwar nicht für die qualifizierte elektronische Signatur gemäss ZertES vorgeschrieben, jedoch für die Anerkennung dieser Signatur im OR als Ersatz für die eigenhändige Unterschrift.

Nach Auswertung der Vernehmlassung schlägt der Bundesrat die dritte Variante vor, bei der sich das ZertES selbst zu dieser Frage nicht äussert und erst die konkrete Anwendung bei Bedarf dieses Erfordernis anstellt. Im Falle von Artikel 14 Absatz 2bis OR, wo die qualifizierte elektronische Signatur der eigenhändigen Unterschrift zur Einhaltung der Schriftform gleichgestellt wird, wird dann der Zeitstempel obligatorisch verlangt.

1.2.4 Terminologische Anpassungen

Die Basis für eine wichtige terminologische Vereinfachung wurde schon in Ziffer 1.2.1 bei den Ausführungen zu den neuen Definitionen für die Zertifikate beschrieben. Nachdem nun geregelte Zertifikate, und damit auch qualifizierte, immer von einer anerkannten Anbieterin von Zertifizierungsdiensten stammen müssen, kann diese Anforderung bei der Referenz weggelassen werden. Die typischerweise für den Ersatz der Schriftform benötigte Signatur kann nun in einem Erlass wesentlich kürzer einfach als «geregelte elektronische Signatur nach ZertES» bzw. «qualifizierte elektronische Signatur nach ZertES» referenziert werden.

Generell wurde darauf geachtet, dass neu die wichtigsten Konzepte des ZertES möglichst direkt über einen Begriff des Gesetzes referenziert werden können. Aus diesem Grund wurde über das schon Erwähnte hinaus der Zeitstempel gemäss Artikel 13 (bisher 12) zum «qualifizierten elektronischen Zeitstempel» umbenannt, um ihn, da er ja von einer anerkannten Anbieterin von Zertifizierungsdienste angefertigt wird, von irgendeinem Zeitstempel einer beliebigen Anbieterin klar zu unterscheiden.

Qualitativ hochwertige elektronische Zeitstempel von unabhängigen Dritten finden immer mehr wichtige Anwendungen. Als Beispiel sei hier die Zeitstempelung von zu archivierenden Dateien, z.B. einer Buchhaltung, genannt, wodurch später bewiesen werden kann, dass die Datei zu einem bestimmten Zeitpunkt genau so bestanden hat, bzw. seither nicht verändert wurde. Neu kann nun ein solcher Zeitstempel, der besonders vertrauenswürdig ist, da er von einer anerkannten Anbieterin erstellt wird, direkt als «qualifizierter elektronischer Zeitstempel nach ZertES» referenziert werden.

1.2.5 Änderung anderer Erlasse

Mehrere Gesetze und Verordnungen nehmen inzwischen Bezug auf die Konzepte des ZertES, insbesondere natürlich auf das Konzept der qualifizierten elektronischen Signatur. Neu soll in diesen Erlassen nun im Normalfall auf die geregelte elektronische Signatur oder das geregelte elektronische Siegel verwiesen werden. Die qualifizierte elektronische Signatur soll nur verlangt werden, wenn die direkte Zuordnung zu einer natürlichen Person unabdingbar ist. Dies entspricht der generellen Strategie, die Hürden für den elektronischen Geschäftsverkehr nicht höher zu legen, als es sachlich unbedingt notwendig ist.

Im Verlauf der letzten Jahre wurden alle Prozessordnungen des Bundes mit Bestimmungen für elektronische Eingaben und für die elektronische Zustellung von Verfügungen und Entscheiden versehen. Dabei wurden teilweise unterschiedliche Konzepte, insbesondere aber eine uneinheitliche Terminologie verwendet. Es gehört zu den Zielen dieser Vorlage, diese Regelungen inhaltlich und terminologisch so weit wie möglich zu harmonisieren. Die im Vorentwurf vorgeschlagene Harmonisierung ging vielen Vernehmlassungsteilnehmern noch zu wenig weit, worauf im vorliegenden Entwurf die Bestrebungen zur Harmonisierung noch verstärkt wurden. Eine noch stärkere Harmonisierung würde zu grosse Eingriffe in die verschiedenen Prozessordnungen verlangen und insbesondere auch eine umfassendere und übergreifende Regelung für die elektronische Zustellung verlangen. Diese Ziele werden aber in einem separaten Projekt unter dem Titel «Vereinheitlichung der Gesetzgebung über die Zustellung» verfolgt, mit dem der Bundesrat Ende 2012 das EJPD zusammen mit dem UVEK und dem EFD beauftragt hat.

1.3 Begründung und Bewertung der vorgeschlagenen Lösung

1.3.1 Einführung des geregelten Zertifikats und des elektronischen Siegels für Unternehmen und Behörden

Während der ganzen Entstehungsgeschichte des ZertES war umstritten, ob qualifizierte Zertifikate natürlichen Personen vorbehalten sein sollen oder ob sie auch juristischen Personen offenstehen sollen. Noch in der Botschaftsversion von 2001 war das qualifizierte Zertifikat diesbezüglich offen; dafür bestimmte ein zusätzlicher Absatz im Artikel 7, dass ein qualifiziertes Zertifikat, das auf eine juristische Person lautet, nicht zu deren Vertretung führe. Dieser Vorbehalt zeigt die Bedenken, die einem solchen Unternehmenszertifikat entgegengebracht werden. Es könnte nämlich rein aus der Tatsache des Zugriffs auf dieses Zertifikat zur Annahme verleiten, dass die jeweilige Benutzerin oder der jeweilige Benutzer des Unternehmenszertifikats eine Vertretungskompetenz für diese juristische Person hätte. Im Einklang mit dem fundamentalen Prinzip des Vertretungsrechts, dass juristische Personen letztlich nur durch natürliche Personen handeln können (insb. Organe und Hilfspersonen), wurde schliesslich das qualifizierte Zertifikat auf natürliche Personen eingeschränkt. An diesen Bedenken hat sich seit Erlass des ZertES nichts geändert.

Die Praxis seit Inkrafttreten des ZertES hat jedoch gezeigt, dass im elektronischen Geschäfts- und Behördenverkehr zusätzlich zur qualifizierten elektronischen Signa-

tur ein grosser Bedarf nach Unternehmens- resp. Behördenzertifikaten besteht, die einerseits staatlich reguliert sind und daher Gewähr für die Einhaltung von Mindestanforderungen bieten (Herkunftsnachweis, Integrität etc.) und andererseits einfach in der alltäglichen Handhabung sind. Gerade bei Massengeschäften ist es kaum praktikabel, wenn bei Meldungen, die nur den Mindestanforderungen genügen sollen, der persönliche PIN eingegeben werden muss, wie es heute bei der qualifizierten elektronischen Signatur verlangt wird.

Die vorliegende Revision hat zum Ziel, diesen Mangel zu beheben. Sie bedient sich hierfür aber nicht der ursprünglich vorgesehenen Ausweitung des qualifizierten Zertifikats, sondern kreiert als Zwischenstufe zwischen dem fortgeschrittenen und dem qualifizierten Zertifikat ein neues «geregeltes Zertifikat» eigener Art, das mit wenigen Abstrichen dem bisherigen qualifizierten Zertifikat entspricht, aber insbesondere direkt auf juristische Personen und Behörden lauten kann.

Die rechtliche Bedeutung des geregelten Zertifikats bzw. des damit erzeugten elektronischen Siegels wird jeweils im betreffenden Gesetz festgelegt, so etwa in den verschiedenen Prozessgesetzen. Das ZertES regelt nur die Qualität gewisser Zertifizierungsprodukte und die Pflichten, die den Anbieterinnen solcher Produkte obliegen. Die Bedeutung dieser Produkte oder Verfahren für den Rechtsverkehr und insbesondere die damit verbundenen Rechtsfolgen werden hingegen nicht im ZertES geregelt (so ausdrücklich der neue Art. 1 Abs. 2). Sofern keine gesetzliche Formvorschrift besteht, können die Parteien vorsehen, dass ihre Willenserklärungen zur Gültigkeit mit einem auf einem geregelten Zertifikat basierenden geregelten elektronischen Siegel versehen werden müssen (gewillkürte Form im Sinn von Artikel 16 OR). Im Unterschied zur bisherigen Regelung steht für solche Zwecke nun aber wie von der Wirtschaft gewünscht ein einheitlich geregeltes Zertifikat und Verfahren zur Verfügung.

Die vorgeschlagene Lösung ändert nichts daran, dass nur die qualifizierte elektronische Signatur gemäss Artikel 14 Absatz 2bis OR der eigenhändigen Unterschrift gleichgestellt ist. Das mit einem elektronischen Siegel versehende Dokument erfüllt somit nicht die gesetzlich vorgeschriebene Form der Schriftlichkeit (Art. 12 ff. OR). Auch darf die Empfängerin oder der Empfänger eines Dokuments, das mit einem elektronischen Siegel – oder einer qualifizierten elektronischen Signatur – versehen ist, nicht automatisch darauf vertrauen, dass die betreffende juristische Person dadurch rechtsgültig verpflichtet wird. Diese Frage bestimmt sich ausschliesslich nach den bestehenden und weiterhin gültigen Grundsätzen des Vertretungsrechts. Die Empfängerin oder der Empfänger wird aber zumindest durch den Haftungstatbestand von Artikel 59*a* OR geschützt, dessen Anwendungsbereich auf geregelte Zertifikate und damit auch auf das elektronische Siegel ausgeweitet werden soll (vgl. Ziff. 1.3.2).

Das in diesem Revisionsentwurf neu eingeführte elektronische Siegel basiert in technischer Hinsicht auf den genau gleichen Verfahren wie die elektronische Signatur und dient zumindest teilweise auch dem gleichen Zweck, nämlich dem Nachweis des Ursprungs und der Unversehrtheit (Integrität) der Daten. Noch im Vorentwurf für die Vernehmlassung wurde diese Anwendung von digitalen Zertifikaten durch juristische Personen und Behörden wie bisher üblich ebenfalls «elektronische Signatur» genannt.

In einem von der Europäischen Kommission am 4. Juni 2012 verabschiedeten Entwurf einer Verordnung zur Ablösung der heutigen Signatur-Richtlinie der EU[1] wird das von einer juristischen Person erstellte Pendant zur elektronischen Signatur «elektronisches Siegel» genannt. Diese neue Terminologie würde den in der vorstehenden Ziffer ausgeführten Gefahren der Fehlinterpretation einer staatlich geregelten «elektronischen Signatur» von juristischen Personen und Behörden bestens Rechnung tragen und wurde daher nach der Vernehmlassung in diese Vorlage übernommen.

Dass auch bei der «digitalen Signatur» mit Zertifikaten von nicht natürlichen Personen der Begriff der «elektronischen Signatur» verwendet wird, ist in der einschlägigen Wissenschaft und auch im Publikum seit Jahrzehnten etabliert. Es dürfte daher schwierig sein, hier einen neuen Begriff einzuführen, auch wenn er aus juristischen Gründen besser passt. In einem E-Mail-Programm oder einem PDF-Viewer wird das neue Konstrukt noch lange «elektronische Signatur» genannt werden, unabhängig davon, dass es von einer juristischen Person erstellt wurde und daher in den einschlägigen Erlassen «elektronisches Siegel» genannt wird. Alleine hätte die Schweiz daher eine solche neue Terminologie kaum einführen können. Im Schlepptau der EU sollte dies aber möglich sein.

1.3.2 Exkurs zur Haftung des Signaturschlüsselinhabers gemäss Artikel 59*a* Obligationenrecht

Mit dem Artikel 59*a* OR wurde ab Einführung des ZertES eine gewisse Haftung des Signaturschlüsselinhabers gegenüber Dritten als wesentlicher Teil des Konzepts der qualifizierten elektronischen Signatur eingeführt. Diese Haftung widerspiegelt die besondere Konstellation bei der elektronischen Signatur, bei welcher die Empfängerin oder der Empfänger des signierten Dokuments im typischen Fall weder mit der Anbieterin des Zertifikats noch mit dem signierenden Absender in einer vertraglichen Beziehung steht. Damit er der qualifizierten elektronischen Signatur trotzdem ein hohes Vertrauen entgegen bringt, haften ihm sowohl die Zertifikatsanbieterin gemäss ZertES Artikel 17 (neu, bisher 16) als auch der Zertifikatsinhaber gemäss Artikel 59*a* OR für eine gewisse Sorgfalt bei der Wahrnehmung ihrer jeweiligen Pflichten.

Diese Bestimmung ist seit ihrer Entstehung bei der Einführung des ZertES umstritten. So haben auch bei der Vernehmlassung zur vorliegenden Totalrevision verschiedene Kreise verlangt, dass sie abgeschwächt oder ganz gestrichen werde. Dabei wird insbesondere argumentiert, die Bestimmung sei zu streng für die Inhaberin oder den Inhaber des Zertifikats und halte dadurch viele potentielle Anwenderinnen und Anwender davon ab, die elektronische Signatur überhaupt einzusetzen. Der Bundesrat hat daher vertieft geprüft, ob die Bestimmung beibehalten, grundsätzlich geändert oder gestrichen werden soll.

Einer solchen Prüfung ist der ganze Artikel 59*a* OR zugrunde zu legen und nicht bloss der von der Revision betroffene Absatz 1. Absatz 2 besagt, dass die Haftung entfällt, wenn der Schlüsselinhaber glaubhaft machen kann, dass er die notwendigen

[1] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, COM(2012)238final.

und zumutbaren Sicherheitsvorkehrungen zur Verhinderung eines Missbrauchs getroffen hat. Absatz 3 schliesslich beauftragt den Bundesrat, die einzuhaltenden Sicherheitsvorkehrungen zu umschreiben. Für die Auslegung dieser Bestimmungen liefern die Materialien aus der Entstehungszeit des ZertES, insbesondere die Botschaft, nicht zu allen Aspekten Anhaltspunkte, weil Artikel 59*a* OR im Laufe der parlamentarischen Beratung mehrmals massgeblich verändert wurde. Rechtsprechung zu diesem Artikel gibt es, soweit ersichtlich, keine, und auch in der Lehre ist es bisher nur vereinzelt zu vertieften Auseinandersetzungen mit den Haftungsfragen gekommen.

Eine elektronische Unterschrift erfüllt ihren Zweck dann, wenn sie der Empfängerin oder dem Empfänger der signierten Erklärung zusätzliche Sicherheit über die Authentizität des Absenders und die Unverfälschtheit des Inhalts gibt. Technisch gesehen ist die elektronische Signatur in dieser Hinsicht sehr zuverlässig. Nur wer den PIN kennt und gleichzeitig Zugriff auf die nicht gesperrte Signaturkarte hat, kann eine gültige Signatur erzeugen. Der Schwachpunkt am ganzen Verfahren ist, dass die Empfängerin oder der Empfänger nicht erkennen kann, ob tatsächlich die rechtmässige Inhaberin, bzw. der rechtmässige Inhaber oder eine andere Person diese Bedingungen erfüllte und die Signatur anfertigte. Wenn ein unvorsichtiger Inhaber leichtfertig mit seinem PIN und seiner Signaturkarte umgeht oder die Signatur auf einem sehr schlecht geschützten Gerät bzw. Computer einsetzt, so ist ein Missbrauch durch eine dritte Person grundsätzlich möglich.

Hier soll Artikel 59*a* OR auf der einen Seite der Empfängerin oder dem Empfänger der signierten oder (neu) gesiegelten Erklärung eine gewisse zusätzliche Sicherheit geben und auf der anderen Seite die Inhaberin oder den Inhaber aufgrund seines Haftungsrisikos dazu veranlassen, beim Einsatz der elektronischen Signatur eine minimale, definierte Sorgfalt anzuwenden. Wenn die Inhaberin oder der Inhaber nämlich nicht glaubhaft machen kann, dass sie resp. er sorgfältig handelte, haftet sie resp. er für den Schaden, den die Empfängerin oder der Empfänger einer mit ihrem resp. seinem Signaturschlüssel erstellten Erklärung erlitten haben, weil diese sich auf die Gültigkeit des geregelten Zertifikats verlassen haben.

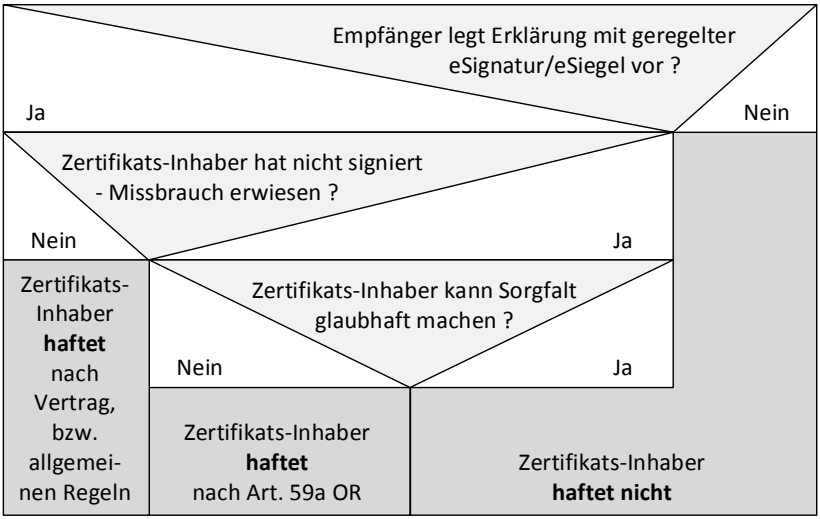
Im Unterscheid zu den Befürchtungen verschiedener Vernehmlassungsteilnehmer ist der Anwendungsbereich der Haftung des Inhabers indessen stark eingeschränkt:

- Ausgangspunkt ist, dass die Empfängerin oder der Empfänger ein elektronisches Dokument vorlegen kann, das mit einem gültigen geregelten Zertifikat der Absenderin oder des Absenders elektronisch signiert oder gesiegelt ist. Sie oder er verfügt damit über einen technisch sehr sicheren Nachweis für die Authentizität der Absenderin oder des Absenders und die Integrität des Inhalts.
- Der Inhaber oder die Inhaberin des verwendeten Zertifikats kann nun die Echtheit des Dokuments bestreiten, indem sie oder er vorbringt, dass nicht sie oder er, sondern eine Drittperson das Dokument elektronisch signiert bzw. mit einem elektronischen Siegel versehen habe. Diese Bestreitung muss sie oder er jedoch ausreichend begründen (Art. 178 der Zivilprozessordnung, ZPO, SR *272*). Gelingt ihr oder ihm das nicht, gilt sie oder er rechtlich als die Unterzeichnerin resp. der Unterzeichner des Dokuments und muss dafür nach den allgemeinen Regeln einstehen.
- Nur wenn beweismässig feststeht, dass das Dokument nicht von der rechtmässigen Inhaberin resp. dem Inhaber des Zertifikats stammt, kommt Arti-

kel 59*a* OR mit seiner spezifischen Haftung überhaupt zum Zuge. Ohne diesen Artikel würde die Inhaberin oder der Inhaber des Zertifikats nach den allgemeinen Regeln (insb. Verschuldenshaftung) für den Missbrauch kaum haften, namentlich da die Widerrechtlichkeit der Schädigung ansonsten fraglich ist (allenfalls könnte Art. 11 der Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur [Verordnung über die elektronische Signatur, VZertES; SR *943.032*] als Schutznorm qualifiziert werden), und die Empfängerin oder der Empfänger müsste den allfälligen Schaden selber tragen. Ebenfalls keine Haftung nach Artikel 59*a* OR ist gegeben, wenn mit einem nicht geregelten Zertifikat signiert wurde.

– Kann die Inhaberin oder der Inhaber des Zertifikats jedoch gemäss Artikel 59*a* Absatz 2 OR glaubhaft machen, dass sie oder er mit dem Signaturschlüssel sorgfältig umgegangen ist, entfällt auch diese Haftung. Gelingt ihr oder ihm das nicht, so haftet sie oder er der Empfängerin oder dem Empfänger für den Schaden, der diesen entstanden ist, weil sie sich auf die Signatur verlassen haben, also für das sogenannte «negative Vertragsinteresse».

Den klassischen Fall kann man sich etwa bei einer qualifizierten elektronischen Signatur so vorstellen: Die Schlüsselinhaberin legt glaubhaft dar, sie habe gar nicht unterschrieben können, weil sie zum Signaturzeitpunkt hospitalisiert war. Es könne aber nicht ausgeschlossen werden, dass ein Kollege oder sonst jemand, der Zutritt zum seinem Büro hat, mit ihrem Schlüssel signiert hätte. Ihre Signaturkarte liege inklusive PIN-Code normalerweise auf seinem Pult. Ohne Artikel 59*a* OR würde sie in diesem Fall wohl nicht haften und der Empfänger müsste den Schaden tragen. Mit der geltenden Regelung haftet sie nach Artikel 59*a* Absatz 1 OR, weil sie die Sicherheitsvorkehrungen gemäss den Absätzen 2 und 3 nicht eingehalten hat.



Es ist ein wichtiges Ziel der ZertES-Gesetzgebung, dass elektronischen Signaturen oder elektronischen Siegeln, die mit einem geregelten (oder gar qualifizierten) Zertifikat erstellt wurden, ein besonderes Vertrauen zukommt, indem diese durch

eine Haftungsbestimmung abgesichert sind. Der Schlüsselinhaberin resp. dem -inhaber wird dadurch ein bestimmtes Mass an Sorgfalt auferlegt, was die Sicherheit des Verfahrens fördert. Dies wiederum stärkt das Vertrauen in die unter diesem Regime erstellten Signaturen und Siegel, was schliesslich deren Wert und deren Akzeptanz steigert. Die vorliegende Totalrevision belässt daher diesen Artikel und weitet ihn auf alle geregelten Zertifikate und die damit erstellten Signaturen und Siegel aus.

1.3.3 Zur Revisionstechnik

Die vorliegende Revision war ursprünglich als Teilrevision geplant. Von den relativ begrenzten Zielen her (siehe vorstehend, Ziff. 1.1.2) könnte man sie weiterhin so betrachten. Weil aber das Gros der Bestimmungen neu nicht nur das qualifizierte, sondern beide geregelten Zertifikate betrifft und weil die Schlüssel neu überall anwendungsneutral genannt werden – z.B. «kryptografischer Schlüssel» statt Prüfschlüssel – ist die Mehrzahl der Artikel von der Revision betroffen, wodurch sie nach den üblichen Kriterien formell zu einer Totalrevision wurde.

1.3.4 Vernehmlassungsverfahren

Die Vernehmlassung zur vorliegenden Vorlage fand zwischen dem 29. März und dem 6. Juli 2012 statt. Der Bericht vom 29. Oktober 2012 mit der Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens findet sich auf der Vernehmlassungs-Website der Bundeskanzlei (www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2012 > Eidgenössisches Justiz- und Polizeidepartement).

Im Rahmen der Vernehmlassung haben sich alle Kantone, alle Bundesratsparteien, verschiedene Dachverbände der Wirtschaft und zahlreiche weitere interessierte Kreise geäussert. Die Ziele der Vorlage, insbesondere die Bereitstellung eines gesetzlich geregelten Zertifikats für juristische Personen und Behörden, fanden breiteste Zustimmung.

Grössere Differenzen ergaben sich bei den nachstehenden Themen, die aber alle nicht das ZertES selbst betreffen:

- Eine Minderheit von drei Kantonen und einigen spezialisierten Unternehmungen lehnten die Einführung des *qualifizierten Zeitstempels* zur Gleichstellung der elektronischen Signatur mit der konventionellen Unterschrift in Artikel 14 Absatz 2bis OR ab. Der Gewinn an Sicherheit wurde zwar nicht bestritten, jedoch wurde die Notwendigkeit einer Online-Verbindung zum Zeitpunkt der Signaturerstellung als zu grosse Einschränkung beurteilt.
- Drei Kantone und zahlreiche der Informatik nahestehende Verbände und Unternehmungen wünschten sich eine Lockerung oder gar Aufhebung der Haftung des Signaturschlüssel-Inhabers nach Artikel 59*a* OR. Dies veranlasste den Bundesrat, die Frage separat und vertieft untersuchen zu lassen. Ein Ergebnis dieser Untersuchung ist, dass die Auslegung des Artikels unklar ist und dass die entsprechende Haftung oft falsch, bzw. als zu gravie-

rend verstanden wird. Weiterführende Ausführungen zu dieser Frage finden sich im eigens dieser Frage gewidmeten Ziffer 1.3.2.

– Verschiedene interessierte Kreise, insbesondere auch der Anwaltsverband, wünschten sich eine viel weitergehende Regelung sämtlicher Aspekte des elektronischen Behördenverkehrs. Die meisten dieser Anliegen werden vom Bundesrat anerkannt, sie gehören jedoch nicht direkt zu dieser relativ eng fokussierten Vorlage und sind inzwischen grösstenteils auch schon in anderen Gesetzgebungsvorhaben enthalten.

Zwei grössere Neuerungen sind erst nach der Vernehmlassung hinzugekommen:

– Die Umbenennung der geregelten elektronischen Signatur von juristischen Personen und Behörden in «geregeltes elektronisches Siegel», ausgelöst durch die entsprechende Terminologie im Entwurf für eine neue Verordnung der EU in dieser Sache, der erst nach dem Start der Vernehmlassung publiziert wurde.

– Die vorliegende, relativ intensive Harmonisierung der Bestimmungen zur elektronischen Übermittlung in den verschiedenen Prozessordnungen des Bundes. Diese war in der Vernehmlassungsvorlage noch rudimentärer.

1.4 Abstimmung von Aufgaben und Finanzen

Das ZertES überträgt die Bereitstellung von gesetzlich geregelten Zertifikaten und darauf basierenden Produkten der Privatwirtschaft. Der Staat stellt nach diesem Modell keine entsprechenden Infrastrukturen oder Dienstleistungen bereit. Was bleibt, ist die Regulierung, einerseits durch das vorliegende Gesetz und andererseits durch eine relativ umfangreiche Umsetzung auf Stufe Verordnung sowie durch technische und administrative Vorschriften. Diese Aufgaben können mit den vorhandenen personellen und finanziellen Mitteln erledigt werden.

1.5 Rechtsvergleich, insbesondere mit dem europäischen Recht

Die Kompatibilität mit dem europäischen Recht war schon immer eine wichtige Rahmenbedingung für die Gesetzgebung zur elektronischen Signatur und anderer Anwendungen elektronischer Zertifikate. In Anbetracht der Internationalität des elektronischen Geschäftsverkehrs und der intensiven Geschäftsbeziehungen der Schweiz mit dem europäischen Umfeld steht dieses Ziel ausser Frage (siehe dazu die entsprechenden Ausführungen in Ziffer 1.1.2 über die Ziele der Totalrevision). In diesem Sinne war das ZertES immer eine autonome nationale Umsetzung der europäischen Signaturrichtlinie mit ein paar wenigen, sorgfältig ausgewählten Vereinfachungen. Gerade im Hinblick auf die Kompatibilität zur europäischen Regelung und eine künftige gegenseitige Anerkennung wurde die Terminologie und Gesetzestechnik der europäischen Richtlinie in einem Masse übernommen, dass das ZertES ein Stück weit einen Fremdkörper innerhalb der schweizerischen Gesetzgebung bildet. Die hohe technische Komplexität sollte nicht durch eine Umsetzung in die schweizerischen Gepflogenheiten der Gesetzgebung noch erhöht werden. Da es sich um ein eher technisches Gebiet handelt, wurde dieses Vorgehen als akzeptabel beurteilt.

Die EU beschäftigt sich seit einigen Jahren mit einer Revision und umfangreichen Ausweitung der Signatur-Richtlinie. Am 4. Juni 2012, also kurz nach Eröffnung der Vernehmlassung zu dieser Vorlage, hat die Europäische Kommission einen Verordnungs-Vorschlag in dieser Sache zuhanden des Europäischen Parlaments und des Rates verabschiedet[2]. Damit stellte sich die Frage, ob die Anpassungen an diese neue EU-Verordnung mit der laufenden Revision zusammengelegt werden sollten. Gleich mehrere Gründe lassen aber eine solche Fusion nicht geraten erscheinen: Bis die EU-Verordnung definitiv verabschiedet und ihr gesamter Inhalt sorgfältig analysiert und nach Mass ins schweizerische Recht überführt ist, dürfte es noch einige Zeit dauern. Der Vorschlag der EU-Verordnung umfasst zudem grössere Bereiche, bei denen in der Schweiz zuerst noch eine umfassende Diskussion darüber stattfinden muss, ob man sie überhaupt übernehmen will. Diese betreffen aber nicht in erster Linie die elektronische Signatur, sondern Fragen der sicheren elektronischen Übermittlung oder der elektronischen Identität. Dazu hat der Bundesrat Ende 2012 eigenständige Gesetzgebungsprojekte gestartet. Es wäre deshalb schade, wenn die seit langem bekannten und nun zur Umsetzung bereiten Anliegen der laufenden Revision noch Jahre warten müssten. Soweit heute absehbar, steht kein Teil der vorliegenden Revision der künftigen EU-Regelung entgegen.

1.6 Umsetzung

Mit dem revidierten Gesetz erhält der Bundesrat die Kompetenz, weitere zertifikatsbasierte Produkte zu regeln, wie er das schon für die qualifizierte elektronische Signatur getan hat. Die einschlägige Branche erwartet eine relativ zügige Regulierung des geregelten elektronischen Siegels für juristische Personen und Behörden. Auch die Regelung einer starken elektronischen Identifikation zeichnet sich als Aufgabe ab.

Definitiv Wirkung entfaltet die Revision erst, wenn die Anbieterinnen die entsprechenden Produkte entwickeln, vermarkten und bereitstellen.

1.7 Erledigung parlamentarischer Vorstösse

Es existieren keine pendenten Vorstösse, die mit dieser Revision erledigt werden sollen. Einer der Auslöser dieser Revision war allerdings die inzwischen erledigte Motion Baumann (08.3741), *Gesetzeswidrige Zertifizierungsanforderung in MWSt-Verordnung*.

[2] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, COM(2012)238final.

2 Erläuterungen zu einzelnen Artikeln

2.1 Bundesgesetz über die elektronische Signatur

2.1.1 Titel des Gesetzes

Der ausgeweitete Anwendungsbereich der nach diesem Gesetz und seinen Ausführungsbestimmungen geregelten Zertifizierungsprodukte soll sich auch im neuen Titel widerspiegeln. Im Fokus stehen dabei in erster Linie das elektronische Siegel und die Authentisierung, andere Anwendungen digitaler Zertifikate sind aber auch denkbar, daher die offene Formulierung.

2.1.2 1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand und Zweck

Das ZertES wird vom Gegenstand der Regelung her oft überinterpretiert, indem beispielsweise angenommen wird, es regle die elektronische Signatur, inklusive ihrer Wirkung. Dabei beschränkt sich das Gesetz im Wesentlichen auf die Regelung der Qualität einiger ausgewählter Zertifikatsprodukte, indem es gewisse Anforderungen an die Produkte selbst und insbesondere an die Anbieterinnen solcher Produkte stellt. Ein neuer erster Buchstabe zum Gegenstand soll diesen spezifischen, recht eingeschränkten Gegenstand des Gesetzes besser verständlich machen.

Das revidierte Gesetz regelt und begünstigt nun nicht mehr nur die qualifizierte elektronische Signatur als Anwendung von Zertifikaten, sondern elektronische Signaturen generell und auch andere Anwendungen von geregelten digitalen Zertifikaten. Entsprechend werden Absatz 1 Buchstabe b (bisher Bst. a) und Absatz 3 Buchstabe b (bisher Abs. 2 Bst. b) weiter als bisher formuliert.

Der neue Absatz 2 nimmt die in der vorstehenden Ziffer 1.3.1 abgehandelten Bedenken auf, ein auf eine juristische Person oder eine Behörde ausgestelltes geregeltes Zertifikat könnte den Anschein nicht vorhandener Vertretungsbefugnisse wecken. Die Tatsache, dass ein Zertifikat eine nach diesem Gesetz geregelte Qualität hat – und die erwähnten Haftungsbestimmungen dienen einzig der Absicherung dieser Qualität – macht über die Einhaltung dieser Qualitätsmerkmale hinaus keine Aussage zur rechtlichen Wirkung einer bestimmten Anwendung dieser Zertifikate. Eine solche Wirkung muss im Kontext dieser Anwendung gesetzlich oder allenfalls auch vertraglich bestimmt werden.

Absatz 3 Buchstabe a harmonisiert die Terminologie zum Absatz 1 und Buchstabe b passt die Formulierung der schon mehrfach erwähnten Ausweitung im Zweck an.

Art. 2 Begriffe

Die neu geregelten Begriffe werden an ihrem systematischen Platz eingefügt, was auch eine Neunummerierung der beibehaltenen Definitionen in den Buchstaben e, h, k und l mit sich bringt.

- *Bst. c: geregelte elektronische Signatur*
  Die geregelte Signatur – neu zwischen der fortgeschrittenen und der qualifizierten elektronischen Signatur eingefügt – wird nach dem Beispiel der bisher unter diesem Buchstaben definierten qualifizierten elektronischen

Signatur definiert. Der erste vorgesehene Spezialfall der fortgeschrittenen Signatur ist also neu die geregelte elektronische Signatur (und nicht wie bisher die qualifizierte elektronische Signatur). Zur Abgrenzung mit dem nachfolgenden elektronischen Siegel wird sie auf natürliche Personen begrenzt.

– *Bst. d: geregeltes elektronisches Siegel*
Als Gegenstück zur geregelten elektronischen Signatur wird das geregelte elektronische Siegel genau gleich definiert wie letztere, jedoch auf juristische Personen und Behörden begrenzt. Mit der Verwendung des Begriffs «UID-Einheiten» gemäss Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010 (UIDG, SR *431.03*) werden das Gros der juristischen Personen und auch Behörden erfasst. Weitere Ausführungen dazu finden sich bei den Erläuterungen zum Artikel 7.

– *Bst. e: qualifizierte elektronische Signatur*
Die bisher in Buchstabe c definierte qualifizierte elektronische Signatur wird gleich erzeugt wie die geregelte elektronische Signatur, ist aber davon wiederum ein Spezialfall, weil ein qualifiziertes Zertifikat, bzw. Schlüsselpaar verwendet werden muss.

– Die bisherigen Definitionen des Signaturschlüssels (Bst. d) und Signaturprüfschlüssels (Bst. e) werden gestrichen, da neu die Anwendung der Schlüssel immer generisch formuliert wird und darum direkt die Begriffe «privater kryptografischer Schlüssel» und «öffentlicher kryptografischer Schlüssel» verwendet werden.

– *Bst. f: digitales Zertifikat*
Der Begriff «digitales Zertifikat» wurde bisher zur weiteren Definition des «qualifizierten Zertifikats» einfach verwendet, ohne dass er selbst im Gesetz definiert worden wäre. Dies war ein gewisser Bruch in der Systematik der Definitionen und eine Abweichung von der EU-Richtlinie und der Gesetzgebung in den Nachbarländern. Selbst die eigenen Umsetzungserlasse haben die Definition explizit eingeführt. Diese neue Definition soll also keine inhaltliche Änderung bewirken, dient aber dem Anliegen der Verständlichkeit und systematischen Konsistenz.

  In einem beliebigen digitalen Zertifikat – im Unterschied zu einem geregelten oder qualifizierten – kann das Schlüsselpaar grundsätzlich nicht nur einer Person, sondern irgendeinem Objekt, z.B. einer Maschine oder einer Website zugeordnet werden. In der englischen Fachterminologie wird dafür oft der Begriff ‚entity» verwendet. Trotzdem wird hier der Begriff, Inhaber oder Inhaberin» gewählt, aus dem einfachen Grund, dass terminologisch keine überzeugende Alternative gefunden werden konnte. Die direkte Übersetzung «Einheit» oder auch der als Alternative geprüfte Begriff «Objekt» wurden als zu wenig verständlich eingeschätzt.

– *Bst. g: geregeltes Zertifikat*
Das neu geregelte Zertifikat wird nach dem Beispiel des bisher unter Buchstabe f definierten qualifizierten Zertifikates definiert. Gemäss den Anforderungen von Artikel 7 ist es ein etwas allgemeiner einsetzbares digitales Zertifikat als das qualifizierte Zertifikat und bildet neu die Basis des letzteren.

Im Hinblick auf die terminologische Vereinfachung wird neu die Anforderung integriert, dass jedes geregelte Zertifikat von einer anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt sein muss.

– *Bst. h: qualifiziertes Zertifikat*
Das qualifizierte Zertifikat wurde bisher in Buchstabe f definiert. Nach neuer Systematik ist es ein Spezialfall des in Buchstabe g neu eingeführten, geregelten Zertifikats, das um ein paar zusätzlichen Anforderungen ergänzt worden ist. In der Summe handelt es sich aber um die bisherigen Anforderungen, ausser der hier – via das geregelte Zertifikat – neu hinzugekommenen Anforderung, dass es immer von einer anerkannten Anbieterin ausgestellt sein muss.

– *Bst. i: elektronischer Zeitstempel*
Der Zeitstempel wurde bisher direkt im Artikel 12 eingeführt und dort definiert. Aus Gründen der systematischen Konsistenz wird er nun auch in diesem Artikel zweistufig definiert. Hier wird vorerst definiert, was ein elektronischer Zeitstempel überhaupt ist.

– *Bst. j: qualifizierter elektronischer Zeitstempel*
Qualifiziert kann der Zeitstempel dann bezeichnet werden, wenn er von einer nach diesem Gesetz anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt wird. Im Artikel 13 (neu) steht dann nur noch die Verpflichtung, diesen anbieten zu müssen.

2.1.3 2. Abschnitt: Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Am bisherigen System der Anerkennung wird nichts geändert. Eine geprüfte, aber verworfene, Variante war, je eine separate Anerkennung vorzusehen für Anbieterinnen, die nur einfache geregelte Zertifikate anbieten und solche, die auch qualifizierte Zertifikate anbieten. Eine solche Lösung hätte aber zusätzliche Komplexität in das Gesamtsystem der Anerkennung gebracht, ohne einem echten Bedürfnis zu entsprechen.

Die vorgeschlagene Lösung ohne Änderung am bestehenden Text bedeutet somit, dass es nur *eine* Anerkennung für Anbieterinnen gibt. Voraussetzung ist, dass diese in der Lage ist, qualifizierte Zertifikate anzubieten, womit sie automatisch auch in der Lage ist, geregelte Zertifikate anzubieten, weil qualifizierte Zertifikate ja geregelte sind, die zusätzliche Anforderungen erfüllen. Die bisher anerkannten Anbieterinnen können künftig also einen weiteren gesetzlich geregelten Typ von Zertifikaten anbieten – und selbstverständlich nach wie vor auch andere, gesetzlich nicht geregelte.

Geändert werden hier somit nur die Artikelnummern der beiden Referenzen auf die Einstellung der Geschäftstätigkeit (neu Art. 14) und die Haftung (neu Art. 17) im Artikel 3 Absatz 1 Buchstabe f. Zudem wird Artikel 4 Absatz 2 redaktionell an die Tatsache angepasst, dass es inzwischen eine Akkreditierungsstelle gibt.

2.1.4 3. Abschnitt: Generierung, Speicherung und Verwendung kryptografischer Schlüssel

Der bisherige Titel «Generierung und Verwendung von Signatur- und Signaturprüfschlüsseln» musste auf eine allgemeinere Formulierung geändert werden, weil neu in diesem Abschnitt auch Schlüssel für das Siegel, für die Authentifizierung oder gar für beliebige Anwendungen von Zertifikaten angesprochen werden. Als genügend allgemeiner Ausdruck blieben die «kryptografischen Schlüssel». Vom normativen Geltungsbereich her sind nur die im Zusammenhang mit den geregelten Zertifikaten benötigten kryptografischen Schlüssel gemeint.

Art. 6

Bisher hat Artikel 6 als Umsetzung des Anhangs III der EU-Richtlinie nur von der Signaturanwendung gesprochen. Dazu kommen nun auch Anwendungen des elektronischen Siegels. Ebenso soll – wie in Ziffer 1.2.1 beschrieben – der Bundesrat neu aber auch die Kompetenz erhalten, weitere Anwendungen von Zertifikaten und zugehörigen Schlüsseln zu regeln, insbesondere die Authentifizierung. Daher spricht der Artikel neu nicht mehr von Signatur und Signaturprüfung, sondern von der Verwendung von Schlüsseln generell.

Mit der Kompetenz, verschiedene Zertifikate für verschiedene Anwendungen zu regeln kann der Bundesrat mehrere Kombinationen von Zertifikaten und Anwendungen regulieren, also zum Beispiel nicht nur eine Anwendung pro Zertifikatstyp. Aus heutiger Sicht sprechen wir aber insbesondere von den folgenden Produkten:

1. Ein qualifiziertes Zertifikat für natürliche Personen für die qualifizierte elektronische Signatur (wie bisher).
2. Ein geregeltes Zertifikat für natürliche Personen für die geregelte elektronische Signatur.
3. Ein geregeltes Zertifikat für juristische Personen und Behörden für das geregelte elektronische Siegel.
4. Ein geregeltes Zertifikat für natürliche Personen für starke Authentisierung, bzw. Online-Identitätsnachweis (eID).

In diesem Kontext darf nicht übersehen werden, dass es nebst den geregelten Produkten immer noch beliebig viele ungeregelte Zertifikate und ähnliche Produkte für beliebige Anwendungen geben kann, die von beliebigen Anbieterinnen angeboten werden.

Dass bisher im Abschnittstitel von der Generierung und Verwendung, im Absatz 1 von Artikel 6 nur von der Generierung und im Absatz 2 von der Erzeugung die Rede ist, hat keine materielle Grundlage und wurde daher im Sinne einer terminologischen Klärung an allen drei Orten auf die einheitliche Bezeichnung «Generierung, Speicherung und Verwendung» geändert.

Im Buchstabe a von Absatz 2 steht die Anforderung, dass Signaturschlüssel, bzw. neu die kryptografische Schlüssel für die geregelten Produkte «praktisch nur einmal auftreten können». In der Vernehmlassung haben verschiedene Anbieter von Zertifizierungsprodukten darauf hingewiesen, dass sie für den sicheren Betrieb des Server-Signings eine Backup-Kopie des privaten Schlüssels erstellen müssen und dass sie befürchten, dass diese Bestimmung das verhindert. Dies ist nicht der Fall und es

braucht daher keine Änderung dieser Bestimmung. Nachforschungen zur Entstehung dieser Bestimmung haben ergeben, dass mit der Formulierung gemeint ist, dass der Schlüssel eindeutig sein müsse, also garantiert werden muss, dass nicht zweimal der gleiche Schlüssel an verschiedene Personen abgegeben wird. Somit ist es nicht untersagt, eine Backup-Kopie eines Schlüssels zu erstellen, wenn diese sicher der Person zugeordnet bleibt und die Aufbewahrung die Sicherheitsanforderung erfüllt, die für das Original gelten.

Der bisherige Absatz 3 über die Gestaltung des Signaturprüfvorgangs wurde beinahe eins zu eins aus dem Anhang IV der EU-Richtlinie entnommen. Er passt in verschiedener Hinsicht nicht in ein schweizerisches Gesetz, da er in der bisherigen Version nur eine Empfehlung beinhaltet und separate, kaum greifbare Normadressaten, in erster Linie die Lieferanten von PDF-Viewern, anspricht. Es stellte sich die Frage, ob die Bestimmungen trotzdem beibehalten werden müssen, um der Kontinuität und der Konformität mit der EU-Richtlinie willen, allerdings neu in der Form einer Kann-Kompetenz mit Leitlinien für den Bundesrat. Schliesslich wurde die Variante bevorzugt, den ganzen Absatz zu streichen, da er rein deklaratorischen Charakter hat und in der Praxis nicht durchsetzbar und nicht notwendig ist. Die Empfängerin oder der Empfänger einer elektronischen Signatur wird aus eigenem Interesse taugliche Werkzeuge für die Überprüfung verwenden.

2.1.5 4. Abschnitt: Geregelte Zertifikate

Da der Abschnitt neu zwei Typen von Zertifikaten regelt, das geregelte und das qualifizierte als Spezialform des geregelten, wurde der Titel von «Qualifizierte Zertifikate» auf «Geregelte Zertifikate» geändert.

Art. 7 Anforderungen an alle geregelte Zertifikate

Artikel 7 übernimmt für alle geregelten Zertifikate in materieller Hinsicht den Grossteil der bisherigen Anforderungen an das qualifizierte Zertifikat aus dem bisherigen Artikel 7. Die nur für das qualifizierte Zertifikat geltenden, zusätzlichen Anforderungen befinden sich im neuen Artikel 8.

Im Gegensatz zu den qualifizierten Zertifikaten, die nur für natürliche Personen ausgestellt werden dürfen, können geregelte Zertifikate sowohl an natürliche als auch an juristische Personen und Behörden ausgestellt werden. Dieses Wesensmerkmal des geregelten Zertifikats wird nicht einfach im entsprechenden Buchstaben nachgeführt, sondern als neuer Absatz 1 prominenter aufgeführt.

Mit der Verwendung des Begriffs «UID-Einheiten» gemäss UIDG werden das Gros der juristischen Personen und auch Behörden erfasst. Damit sind nicht nur die im Handelsregister eingetragenen Rechtsträger (Art. 3 Abs. 1 Bst. c Ziff. 1 UIDG) erfasst, sondern auch andere juristische Personen. Unter den Begriff der «UID-Einheit» fallen insbesondere auch Behörden und Gerichte (Art. 3 Abs. 1 Bst. c Ziff. 7 UIDG). Nicht erfasst von dieser Formulierung wären somit einzig die juristischen Personen, die nicht im UID-Register eingetragen sind, wie beispielsweise nicht eingetragene Vereine und Stiftungen. Diese hätten hier entweder separat genannt werden müssen, oder sie werden nach der vorliegenden Lösung bewusst ausgeschlossen. Einer juristischen Person, deren öffentliches Profil so schwach ist, dass keiner der Gründe gemäss Artikel 3 Absatz 1 Buchstabe c UIDG für eine

Eintragung in das UID-Register gegeben ist, die also z.B. zu keiner Behörde eine Beziehung hat, soll auch keine elektronische Identität in Form eines geregelten Zertifikats erhalten. Die Identitätsfeststellung durch die Anbieterin von Zertifizierungsdiensten könnte sich aufwendig gestalten. Sollte eine solche Person trotzdem am elektronischen Geschäftsverkehr teilnehmen wollen, was eher unwahrscheinlich ist, kann sie dies durch eine natürliche Person, die sie vertritt, tun.

Abs. 2

Buchstabe b wird wie überall auf geregelte Zertifikate allgemein ausgeweitet.

Buchstabe c, der wie bisher die Nennung des Namens, des Pseudonyms und allfälliger Zusätze zur Vermeidung von gleichlautenden Namen vorschreibt, wird neu auf die drei separaten Buchstaben c, d und e aufgeteilt. Buchstabe c regelt den Namen, bzw. die Bezeichnung des Inhabers bzw. der Inhaberin des Schlüssels und die Auflösung von Kollisionen. Statt wie bisher vom Inhaber des Signaturprüfschlüssels wird vom Inhaber bzw. der Inhaberin des geheimen kryptografischen Schlüssels gesprochen. Dieser Wechsel dient einerseits der schon mehrfach erwähnten Generalisierung der Anwendung über die Signatur hinaus und behebt andererseits eine Unschönheit aus der Entstehungszeit; es hätte hier schon immer – gleich wie in Buchstabe a von Absatz 2 – präziser Signaturschlüssel und nicht Signaturprüfschlüssel heissen sollen. Der öffentliche Schlüssel wird in Buchstabe f (früher d) der Inhaberin oder dem Inhaber zugeordnet.

Nur für natürliche Personen gilt Buchstabe d, welcher Pseudonyme genau wie bisher ermöglicht. Nur an UID-Einheiten schliesslich wendet sich Buchstabe e, welcher die UID-Nummer als eindeutigen Identifikator verlangt.

Buchstabe f ersetzt den bisherigen Buchstaben d und wechselt vom bisherigen «Signaturprüfschlüssel» auf den allgemeineren Begriff «öffentlicher kryptografischer Schlüssel», weil geregelte Zertifikate ja nicht nur für die Signatur, sondern z.B. auch für die Authentifizierung vorgesehen sein können.

Der bisherige Buchstabe g, der verlangte, dass Informationen über die Anerkennung der Anbieterin enthalten sein müssen, wird als schweizerische Sonderlösung gestrichen.

Buchstabe h: Nachdem mit dem neuen geregelten Siegel auch für juristische Personen eine «Signatur» mit definierter Qualität zur Verfügung stehen wird, kann hier – wie auch beim Zeitstempel – auf die bisherige Anomalie verzichtet werden, dass Anbieterinnen von Zertifizierungsdiensten als einzige nicht natürliche Personen ein qualifiziertes Zertifikat erhalten und damit eine qualifizierte Signatur erstellen können. Das geregelte elektronische Siegel unter Verwendung eines geregelten Zertifikats deckt genau dieses Bedürfnis ab.

Abs. 3

Absatz 3 (bisher 2) wird zuerst einmal gesetzgebungstechnisch besser formuliert. Zudem wird der bisherige Buchstabe a über die optionale Angabe von zusätzlichen Attributen und einer allfälligen Vertretung neu auf die 2 Buchstaben a und b aufgeteilt.

Buchstabe a führt die optionalen Attribute auf und bringt zur Veranschaulichung als Beispiel die in der Praxis öfters verwendete berufliche Qualifikation.

Die neu im separaten Buchstaben b aufgeführte Vertretung ist zwar auch in einfachen geregelten Zertifikaten möglich, soll aber nur natürlichen Personen zugänglich sein. Im Rahmen der Revisionsarbeiten ebenfalls diskutiert wurde die Variante, dass die Vertretung nur in qualifizierten Zertifikaten möglich sein soll; es wurden jedoch keine schlagenden Gründe für eine solche Einschränkung gefunden.

Die Buchstaben c und d ersetzen die bisherigen Buchstaben b und c. Die Überarbeitung soll nur die bisherige Bedeutung sprachlich klarer zum Ausdruck bringen.

Art. 8 Zusätzliche Anforderungen an qualifizierte Zertifikate

Da das Gros der bisherigen Anforderungen an das qualifizierte Zertifikat neu im vorangehenden Artikel über die Anforderungen an das geregelte Zertifikat enthalten ist, werden für das qualifizierte Zertifikat als Spezialfall eines geregelten Zertifikats im revidierten Artikel 8 nur noch die zusätzlichen Anforderungen aufgeführt. In der Summe sollen die aus Artikel 7 aus systematischen Gründen (Art. 2 Bst. g) übernommenen und die zusätzlichen Anforderungen nach Artikel 8 grundsätzlich, d.h. mit Ausnahme der expliziten Änderungen, den bisherigen Anforderungen an das qualifizierte Zertifikat entsprechen.

Absatz 1 nennt die wichtigste Abgrenzung des qualifizierten zum einfachen geregelten Zertifikat, nämlich die Einschränkung auf natürliche Personen.

In Absatz 2 wird neu zusätzlich explizit bestimmt, dass ein qualifiziertes Zertifikat nur für die elektronische Signatur bestimmt ist. Hier handelt es sich wieder um eine Ausnahme vom Grundsatz dieser Revision, dass nur Änderungen vorgenommen werden sollen, die für die genannten Ziele unabdingbar sind. Zurzeit ist diese Vorschrift nur auf der Ebene der technischen und administrativen Vorschriften (TAV, SR *943.032.1* / Anhang) umgesetzt, indem für das Feld «key usage» ein bestimmter Wert, eben der für die Signatur von Dokumenten, vorgeschrieben wird. Nichttechnische Kreise haben sich immer daran gestört, dass eine so wichtige Einschränkung, die sich offenbar aus technischen Gründen aufdrängt und daher vorerst nur einmal Technikern plausibel erscheint, nicht explizit im Gesetz aufgeführt ist.

Absatz 3 übernimmt den Buchstaben b aus dem bisherigen Artikel 7 Absatz 1.

2.1.6 Diverse Anpassungen in den Abschnitten 5–9

Drei Anpassungen betreffen alle oder mehrere der nachfolgenden Artikel und sollen hier nur summarisch erwähnt werden.

Anpassung der Artikelnummer

Bis auf den letzten Artikel werden alle Artikelnummern um eine Ziffer erhöht.

Ersatz «qualifiziertes Zertifikat» durch «geregeltes Zertifikat»

Im Normalfall sollen alle Bestimmungen des Gesetzes, welche bisher das qualifizierte Zertifikat betroffen haben, neu beide gesetzlich geregelten Zertifikate betreffen, nämlich das geregelte Zertifikat (i.e.S.) und das qualifizierte Zertifikat als spezialisierter Subtyp des geregelten. Daher wird in allen einschlägigen Formulierungen der Ausdruck «qualifiziertes Zertifikat» durch den Ausdruck «geregeltes Zertifikat» ersetzt, womit dann beide geregelten Zertifikate gemeint sind. Aus-

nahmsweise wird mit dem gleichen Zweck einer eleganteren Formulierung der Vorzug gegeben.

Diese Anpassung betrifft die (neuen) Artikel 9–14, 17, 18 und 21.

Ersatz «elektronische Signatur» und «Signaturschlüssel» durch neutralen Begriff

Da neu nicht mehr nur die Signatur sondern auch andere Anwendungen digitaler Zertifikate geregelt werden sollen, werden die Begriffe «elektronische Signatur» und «Signaturschlüssel» durchgehend durch neutralere Wendungen oder geeignete Umformulierungen ersetzt.

Diese Anpassung betrifft die (neuen) Artikel 10, 11, 16, 17, und 20.

Weitere Änderungen sind für die Anpassung der Verweise auf die geänderten Artikel- und Absatznummern notwendig geworden (vgl. Art. 16, 17 Abs. 3, und 18).

2.1.7 5. Abschnitt: Pflichten anerkannter Anbieterinnen von Zertifizierungsdiensten

Art. 9 (bisher 8) Ausstellung geregelter Zertifikate

Die Regeln für das Prozedere bei der Beantragung eines geregelten Zertifikats müssen neu auch auf «UID-Einheiten» ausgeweitet werden. Daher wird Absatz 1 in zwei Litera aufgegliedert. Buchstabe a bestimmt das Prozedere für natürliche Personen genau gleich wie bisher, Buchstabe b bestimmt das Prozedere für die Beantragung von geregelten Zertifikaten von «UID-Einheiten». Natürliche Personen, die gleichzeitig UID-Einheiten sind, sollen nach Buchstabe a persönlich erscheinen müssen.

Der zweite Teil des bisherigen, etwas überladenen Absatzes 1 wird in zwei neue Absätze 2 und 3 umgeordnet, wodurch die weiteren Absatznummern je um zwei erhöht werden.

Im Rahmen der Vernehmlassung haben die Anbieterinnen von Zertifizierungsdiensten und andere Interessierte darauf hingewiesen, dass es für ein grösseres Unternehmen sehr aufwendig wäre, wenn bei jedem Antrag für ein geregeltes Zertifikat eine Vertretung persönlich erscheinen müsse und dass mindestens in den Fällen, wo die Vertretung im Handelsregister ersichtlich sei, ein elektronischer Antrag möglich sein müsste.

Der Bundesrat hält dafür, dass genau für solche Fälle schon bisher der Absatz 2 (neu 4) vorgesehen ist, der ihm die Kompetenz gibt, Ausnahmen vorzusehen. Es erscheint angebracht, auf Verordnungsstufe vorzusehen, dass ein elektronischer Antrag dann zulässig ist, wenn die zur Vertretung befugte Person den Antrag mit ihrer qualifizierten Signatur unterzeichnet und sich die Vertretung aus einem öffentlichen Register ergibt, also beispielsweise aus dem Handelsregister oder einem Behördenregister.

Art. 11 (bisher 10) Ungültigerklärung geregelter Zertifikate

Gemäss der neuen Formulierung in Absatz 1 Buchstabe b des bisherigen Artikels 10 wird eine Ungültigerklärung eines Zertifikats neu auch möglich, wenn sich berufs-

bezogene oder sonstige Angaben zur Person (vgl. Art. 7 Abs. 3) als falsch erweisen, seien sie schon ursprünglich falsch gewesen oder inzwischen nicht mehr richtig.

Dabei dürfen sich die Anbieterinnen selbstverständlich auf Mitteilungen der nach Artikel 9 Absatz 2 für diese Angaben zuständigen Stellen verlassen, eine Folgerung, auf welche die Anbieterinnen anlässlich der Vernehmlassung grossen Wert gelegt haben. Wenn also beispielsweise aufgrund der Meldung einer Standesorganisation die Mitgliedschaft dieser Person im Zertifikat vermerkt wurde und dieselbe Organisation später mitteilt, dass die Mitgliedschaft nicht mehr existiert, dann darf die Anbieterin sich für die Löschung des Zertifikats auf diese Mitteilung verlassen.

Art. 12 (bisher 11) Verzeichnisdienst für geregelte Zertifikate

Die neue Formulierung von Absatz 2 beseitigt eine bisherige Unklarheit.

Art. 13 (bisher 12) Qualifizierte elektronische Zeitstempel

Nachdem der elektronische Zeitstempel neu in Artikel 2 Buchstabe i und der qualifizierte elektronische Zeitstempel in Buchstabe j definiert sind, muss hier nur noch die Verpflichtung zur Bereitstellung dieses Dienstes geregelt werden.

Art. 15 (bisher 14) Datenschutz

Ersatz von «notwendig» durch «erforderlich» als rein terminologische Harmonisierung.

Art. 17 (bisher 16) Haftung der Anbieterin von Zertifizierungsdiensten

Mit der Änderung von, Anbieterin» auf, anerkannte Anbieterin» soll noch klarer hervorgehoben werden, dass diese Bestimmung nicht für irgendwelche Zertifizierungsdienste beliebiger Anbieter gilt.

Art. 19 (bisher 18) Verjährung

Parallel zu diesem Vorhaben läuft eine Revision des Verjährungsrechts, die auch in diesem Artikel Veränderungen vorsieht. Je nachdem wie sich die Behandlung und Verabschiedung dieser beiden Vorlagen im Parlament zeitlich zueinander verhalten, müsste die entsprechende Änderung direkt in dieses Vorhaben übernommen werden.

Art. 20 (bisher 19)

Verschiedene terminologische Präzisierungen.

Art. 21 (bisher 20) Vollzug

Absatz 3 sah bisher schon vor, dass der Bundesrat zur Erfüllung des Gesetzeszweckes eine Verwaltungseinheit des Bundes beauftragen kann, Zertifikate auch für den Privatrechtsverkehr auszustellen. Diese Bestimmung war insbesondere für den Fall gedacht, dass keine privaten Anbieter am Markt erscheinen würden. Im Rahmen der Vernehmlassung haben mehrere Kantone darauf hingewiesen, dass es inzwischen auch kantonale Stellen gibt, die Erfahrung mit der Herausgabe von Zertifikaten haben und daher ebenso gut für diese Aufgabe geeignet wären. Mit der neuen

Formulierung wäre auch eine Beauftragung einer kantonalen Verwaltungsstelle möglich.

Art. 22 (bisher 21)

Terminologische Anpassungen gemäss den neuen gesetzestechnischen Richtlinien.

2.2 Aufhebung und Änderung bisherigen Rechts

2.2.1 Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur

Das Bundesgesetz 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur vom wird aufgehoben und durch das neue Bundesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate ersetzt.

2.2.2 Verwaltungsverfahrensgesetz vom 20. Dezember 1968 (VwVG)

Art. 21a 2. bei elektronischer Übermittlung

Der Randtitel wird an die heute übliche Terminologie angepasst. «Zustellung» wird für den Weg von der Behörde an den Privaten verwendet, «Übermittlung» ist richtungsneutral.

Beim Erlass der ursprünglichen Regelung wurde davon ausgegangen, dass jedes Gericht oder Behörde ein eigenes Übermittlungssystem entwickelt und einsetzt, welches entsprechende Quittungen ausstellt. Umgesetzt wurde aber in der Praxis ein System mit verschiedenen anerkannten Zustellplattformen, welche die Quittungen ausstellen und die Behörden mit den Eingaben bedienen. Das eigentliche Behördensystem verfügt so lediglich über einen Eingang ohne Quittungsbestätigung. Diese Übermittlungskaskade führt in der Praxis zu Rechtsunsicherheit und soll nun korrigiert werden.

Die neue Formulierung von Artikel 21*a* VwVG stellt den Prototyp für die Regelung der elektronischen Eingabe in allen Prozessordnungen dar und enthält die nachstehenden Elemente:

- Die Eingabe selbst ist von der Partei oder ihrer Vertretung mit einer qualifizierten elektronischen Signatur zu versehen.
- Technologieneutral wird die Art und Weise definiert, wie die Wahrung einer Frist nachgewiesen werden kann.
- Der Bundesrat erhält die Kompetenz, sowohl für die Eingabe selbst als auch für die Beilagen das Format und den technischen Ablauf der Übermittlung zu regeln. Damit kann er auch bestimmen, wie der exakte Zeitpunkt der Ausstellung der Empfangsquittung technisch im Detail festzuhalten ist.

– Der Bundesrat regelt ferner die Voraussetzungen, unter denen bei technischen Problemen die Nachreichung von Dokumenten auf Papier verlangt werden kann.

Mit dieser Lösung kann der Bundesrat die konkreten Bedürfnisse bezüglich Sicherheit und Automatisierbarkeit der Übermittlung im Einzelfall berücksichtigen und flexibel auf die sich ändernden technischen Gegebenheiten bei der elektronischen Übermittlung Rücksicht nehmen.

Art. 34 Abs. 1bis

Die neue Formulierung dieses Artikels stellt den Prototyp für die Regelung der elektronischen Zustellung in allen Prozessordnungen dar und enthält nachstehende Elemente:

– Die elektronische Zustellung bedingt das Einverständnis der Partei.
– Die Verfügung ist elektronisch zu signieren, es ist aber dem Bundesrat überlassen, die Art der Signatur auf Verordnungsstufe festzulegen.
– Der Bundesrat erhält die Kompetenz, die gleichen Gegenstände zu regeln, die er schon bei der Eingabe regeln kann, insbesondere das Format der Verfügung und ihrer Beilagen, die Art und Weise der Übermittlung sowie den Zeitpunkt, zu dem die Verfügung als zugestellt gilt.

2.2.3 Bundesgerichtsgesetz vom 17. Juni 2005

Art. 39 Abs. 2

Die Angabe der Zustelladresse und Erklärung des Einverständnisses mit elektronischen Eröffnungen wird der harmonisierten Terminologie angepasst.

Während der Bundesrat die Ausführungsbestimmungen mit der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV; SR *172.021.2*) respektive der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV; SR *272.1*) erlassen hat, erfolgte dies seitens Bundesgericht durch das Reglement des Bundesgerichts über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen vom 5. Dezember 2006 (ReRBGer; SR *173.110.29*). Alle drei Erlasse werden an die neue Terminologie anzupassen sein (vgl. hinten Ziff. 2.2.8) und basieren auf denselben Grundprinzipien.

Die einzige Ausnahme besteht in der Regelung von Artikel 3 Absatz 2 ReRBGer. Dieser bestimmt, dass der Eintrag auf einer Zustellplattform bereits als Einverständnis gilt, dass Eröffnungen auf elektronischem Weg erfolgen können. Diese Annahme ist weiterhin zulässig und hat sich in der Praxis des Bundesgerichts bewährt. Das Erfordernis einer separaten Erklärung des Einverständnisses würde in solchen Fällen eine administrative Schikane bilden, die nach Ansicht des Bundesgerichts geeignet wäre, die Verbreitung des elektronischen Rechtsverkehrs zu behindern.

Ob diese Regelung auch in den anderen Prozessordnungen übernommen werden soll, ist im Rahmen des Projektes unter dem Titel «Vereinheitlichung der Gesetzgebung über die Zustellung» (vgl. vorne Ziff. 1.2.5) zu prüfen.

Art. 42 Abs. 4, 48 Abs. 2, 60 Abs. 3

Es wird inhaltlich und terminologisch – mutatis mutandis – die gleiche Regelung implementiert, wie sie vorstehend beim VwVG als Prototyp definiert wurde. Die dort dem Bundesrat zukommenden Kompetenzen stehen in diesem Fall dem Bundesgericht zu.

2.2.4 Obligationenrecht

Art. 14 Abs. 2bis

Nachdem nun im Definitionsteil des ZertES (vgl. Art. 2 Bst. d, f und g bzw. Ziff. 1.2.1 vorstehend) die qualifizierte elektronische Signatur neu die Ausstellung des verwendeten Zertifikats durch eine anerkannte Anbieterin voraussetzt, kann Absatz 2bis von Artikel 14 OR stark vereinfacht und damit leserlicher gestaltet werden.

Wie in Ziffer 1.2.3 ausgeführt, geht die Entwicklung immer mehr dahin, nur noch die mit einem Zeitstempel einer unabhängigen Stelle versehene elektronische Signatur als sicher zu betrachten. Für den Begriff der «qualifizierten elektronischen Signatur» im ZertES wurde eine solche zusätzliche Anforderung geprüft und als für zu einschränkend beurteilt.

Da in der Schweiz die rechtliche Anerkennung der elektronischen Signatur im Unterschied zu mehreren Nachbarländern nicht im ZertES selbst geschieht, sondern in der Gesetzgebung der jeweiligen Bereiche, ist es möglich, dass der Zeitstempels für die Anerkennung der elektronischen Signatur selektiv für einem Bereich verlangt wird. Genau dies wird mit der neuen Formulierung des Artikels für die Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift verlangt.

Art. 59a F. Haftung für kryptografische Schlüssel

Die bisherige Haftung des Schlüsselinhabers für qualifizierte Zertifikate soll auch auf geregelte Zertifikate ausgedehnt werden, weil diese Haftung eine wichtige Grundlage für die Akzeptanz und Wertschätzung bei der Empfängerin oder beim Empfänger der signierten oder gesiegelten Erklärung ist. Siehe dazu den Exkurs in Ziffer 1.3.2. Allerdings soll die Haftung auf elektronische Signaturen und elektronische Siegel beschränkt sein und für die Authentisierung oder weitere Anwendungen elektronischer Zertifikate nicht gelten.

Der bisher im Randtitel und in den Absätzen 1 und 2 verwendete Begriff «Signaturschlüssel» ist im Revisionsentwurf nicht mehr definiert, da er für das nunmehr breitere Anwendungsfeld von Zertifikaten zu spezifisch wäre. Er wird hier wie an den meisten Stellen im ZertES selbst durch den Begriff «kryptografischer Schlüssel» ersetzt, zusätzlich muss aber die beabsichtigte Einschränkung auf die Anwendungen für elektronische Signaturen und elektronische Siegel vorgenommen werden.

2.2.5 Zivilprozessordnung

Art. 130, 139, 143 Abs. 2

Es wird inhaltlich und terminologisch – mutatis mutandis – die gleiche Regelung implementiert, wie sie vorstehend beim VwVG als Prototyp definiert wurde.

2.2.6 Bundesgesetz vom 11. April 1889 über Schuldbetreibung und Konkurs

Art. 33a und 34 Abs. 2

Der Randtitel wird an die heute übliche Terminologie angepasst. Es wird inhaltlich und terminologisch – mutatis mutandis – die gleiche Regelung implementiert, wie sie vorstehend beim VwVG als Prototyp definiert wurde.

Darüber hinaus bestimmt Artikel 33*a* Absatz 2, letzter Satz, dass der Bundesrat bei Massenverfahren für die Eingabe vom Erfordernis der qualifizierten elektronischen Signatur absehen kann.

2.2.7 Strafprozessordnung

Art. 86, 91 Abs. 3, 110 Abs. 2

Es wird inhaltlich und terminologisch – mutatis mutandis – die gleiche Regelung implementiert, wie sie vorstehend beim VwVG als Prototyp definiert wurde.

2.2.8 Terminologische Bereinigungen

Die erforderliche terminologische Bereinigung bzw. Vereinfachung bei der Regelung der elektronischen Signatur wird mit Anpassungen von verschiedensten Verordnungen herbeizuführen sein. Benutzt wird der Begriff der elektronischen Signatur insbesondere in folgenden Ausführungsbestimmungen:

- Artikel 14*a* Absatz 2 der Verordnung vom 20. September 2002 über die Ausweise für Schweizer Staatsangehörige (Ausweisverordnung, VAwG; SR *143.11*)
- Artikel 27*k*^{bis} Absatz 2 und 3 sowie Artikel 27*d* Absatz 2 Buchstabe a und b der Verordnung vom 24. Mai 1978 über die politischen Rechte (SR *161.11*)
- Artikel 4 Absatz 2 Buchstabe f, Artikel 6 Absatz 1, 2 und 3, Artikel 9 Absatz 4 und 5 sowie Artikel 12 Absatz 1 Buchstabe c und d der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (SR *172.021.2*)
- Artikel 2 Buchstabe d sowie Artikel 4 Absatz 3 des Reglements des Bundesgerichts vom 5. Dezember 2006 über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen (ReRBGer; SR *173.110.29*)

- Artikel 12*a* Absatz 3 und 4, Artikel 12*c* Absatz 1 Buchstabe b, Artikel 18 Absatz 4, Artikel 20 Absatz 2 und Artikel 21 Absatz. 3 der Handelsregisterverordnung vom 17. Oktober 2007 (HRegV; SR *221.411*)
- Artikel 8 Absatz 2 sowie Artikel 13 Absatz 2 Buchstabe a der Verordnung vom 15. Februar 2006 über das Schweizerische Handelsamtsblatt (Verordnung SHAB; SR *221.415*)
- Artikel 2 Buchstabe a und b, Artikel 5 Absatz 2 Buchstabe c, Artikel 7, Artikel 10 Absatz 3, Artikel 13 Absatz 1 Buchstabe c und d sowie Artikel 14 Absatz 2 der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie Schuldbetreibungs- und Konkursverfahren (SR *272.1*)
- Artikel 4 Absatz 1 der Verordnung des EJPD vom 9. Februar 2011 über die elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs (SR *281.112.1*)
- Artikel 17 Absatz 3 Buchstabe c und Absatz 4 der Registerharmonisierungsverordnung vom 21. November 2007 (RHV; SR *431.021*)
- Artikel 2 Absatz 2 und 3, Artikel 2 Absatz 2 Buchstabe a Ziffer 5, Artikel 2 Absatz 4 sowie Artikel 3 Absatz 1 Buchstabe a, c und d der Verordnung des EFD vom 11. Dezember 2009 über elektronische Daten und Informationen (EIDI-V; SR *641.201.511*)
- Artikel 5 Absatz 4 der Verordnung des UVEK vom 24. November 2006 über den Nachweis der Produktionsart und der Herkunft von Elektrizität (SR *730.010.1*)
- Artikel 63 Absatz 2 Buchstabe c der Verordnung vom 7. Dezember 1998 über die Direktzahlungen an die Landwirtschaft (Direktzahlungsverordnung, DZV; SR *910.13*)
- Artkel 5 Absatz 1bis Buchstabe c der Verordnung vom 7. Dezember 1998 über Flächen- und Verarbeitungsbeiträge im Ackerbau (Ackerbaubeitragsverordnung, ABBV; SR *910.17*)
- Artikel 5 Absatz 3, Artikel 7 Absatz 2 sowie Artikel 9 Absatz 3 der Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES; SR *943.032*)
- Artikel 1 sowie Anhang der Verordnung des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR *943.032.1*)

Zwischen der Verabschiedung der vorliegenden Gesetzesrevision durch die Bundesversammlung und dem Inkrafttreten des neuen ZertES werden die notwendigen Anpassungsarbeiten zu erfolgen haben.

3 Auswirkungen

3.1 Auswirkungen auf den Bund

3.1.1 Finanzielle Auswirkungen

Die Revision hat keine finanziellen Auswirkungen auf den Bund.

3.1.2 Personelle Auswirkungen

Die Rechtsetzung auf Stufe der Verordnung und die Erarbeitung der technischen und administrativen Richtlinien sowie zivilprozessualer Vorlagen erfordern Personal im Umfang von mehreren Personenmonaten. Die Federführung liegt herkömmlicherweise beim BAKOM, zahlreiche weitere Ämter wirken mit.

Es sind keine Einsparungen oder Erhöhungen von Personal als Folge dieser Revision geplant oder absehbar.

3.1.3 Andere Auswirkungen

Verschiedene Bundesstellen werden von den neu geregelten Produkten guten Gebrauch machen können. Mit den Behördenzertifikaten steht nun verschiedenen Registerstellen eine adäquate Lösung für die Signatur von elektronischen Auszügen zur Verfügung. Beispiele hierfür sind Geburtsscheine oder Auszüge aus dem Straf- oder Handelsregister.

3.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Weder das bisherige ZertES noch die Totalrevision bedeuten einen Aufwand für Kantone, Gemeinden oder andere öffentliche Körperschaften.

Sowohl sie als auch andere Organisationen kommen als Kunden der neuen Produkte in Frage.

3.3 Auswirkungen der Harmonisierung der elektronischen Übermittlung in den Prozessordnungen auf Gerichte und Behörden

Da die Harmonisierung im Wesentlichen nur die heute geltende Regelung präziser und einheitlicher formuliert, sollten sich für Gerichte und Behörden kaum Auswirkungen ergeben. Einzig dort, wo bisher bei elektronischer Eingabe gegen den Sinn der heutigen Regelung systematisch eine Nachlieferung auf Papier verlangt wurde, könnte neu nun geringfügig mehr Aufwand für den Ausdruck der elektronischen Eingaben anfallen. Sobald das Gericht oder die Behörde intern auf eine elektronische Geschäftsverwaltung umgestellt hat, entfällt dieser Mehraufwand wieder.

3.4 Auswirkungen auf die Volkswirtschaft

Zertifikatsbasierte Produkte fördern die Sicherheit und das Vertrauen im elektronischen Geschäftsverkehr zwischen Privaten und Behörden. Sie tragen somit dazu bei, dass die Schweiz den Übergang zu einer entwickelten Informationsgesellschaft besser und schneller bewerkstelligt.

3.5 Auswirkungen auf die Gesellschaft

Das Gesetz ermöglicht die staatliche Regelung von starken elektronischen Identifikationsmitteln, was dazu beiträgt, negative Folgen der globalisierten Informationsgesellschaft, beispielsweise Identitätsdiebstahl, zu verhindern.

3.6 Auswirkungen auf die Umwelt

Die Totalrevision hat keine erkennbare Auswirkung auf die Umwelt.

3.7 Andere Auswirkungen

Über das oben Beschriebene hinaus sind keine nennenswerten Auswirkungen der Totalrevision zu erwarten.

4 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrates

4.1 Verhältnis zur Legislaturplanung

Die Vorlage ist in der Botschaft vom 25. Januar 2012[3] zur Legislaturplanung 2011–2015 angekündigt.

4.2 Verhältnis zu nationalen Strategien des Bundesrates

Lange Zeit war die Regelung der elektronischen Signatur ein wichtiger Punkt der jeweiligen Strategien des Bundesrates für eine Informationsgesellschaft in der Schweiz und der E-Government-Strategie des Bundes. Heute ist sie das nicht mehr; seit der Einführung des ZertES geht man davon aus, dass das Problem gelöst ist. Das geregelte Siegel für juristische Personen und Behörden ist in strategischer Hinsicht eine kleine Anpassung eines bestehenden Gesetzes.

Die vorliegende Revision gibt dem Bundesrat aber auch neu die Kompetenz, andere zertifikatsbasierte Anwendungen zu regeln und darunter insbesondere die starke Authentisierung. Die Bereitstellung eines solchen starken elektronischen Identifika-

3 BBl **2012** 481 609

tionsmittels wiederum ist in mehreren Strategien des Bundes enthalten, sei es als direktes Ziel oder als Voraussetzung für die Erreichung anderweitiger Ziele:

- Die Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz vom März 2012 nennt die Erarbeitung «von Lösungen für den Nachweis von Identitäten» als Handlungsschwerpunkt zur Erreichung des Ziels des Schutzes vor Internetkriminalität.
- Die E-Government-Strategie Schweiz nennt im priorisierten B2.07 «Die Bereitstellung der digitalen Identität und Identifikation für die Authentisierung im elektronischen Geschäfts- und Behördenverkehr» einen Eckstein für die künftige Entwicklung des elektronischen Wirtschaftsraums in der Schweiz.
- Die von Bund und Kantonen gemeinsam erarbeitete «Strategie eHealth Schweiz» nennt als Ziel A5 im Handlungsfeld «Elektronisches Patientendossier» die Etablierung der sicheren Authentisierung mit einer Option für die rechtsgültige elektronische Signatur.
- Die Unterbreitung der vorliegenden Totalrevision an das Parlament wurde vom Bundesrat am 19. Dezember 2012 im Rahmen eines umfassenden Gesetzgebungspakets zur Förderung des elektronischen Geschäftsverkehrs beschlossen.

5 Rechtliche Aspekte

5.1 Verfassungs- und Gesetzmässigkeit

Das Gesetz stützt sich weiterhin auf die Artikel 95 Absatz 1 und 122 Absatz 1 der Bundesverfassung (BV), welche dem Bund Gesetzgebungskompetenzen im Bereich der privatwirtschaftlichen Erwerbstätigkeit und des Privatrechts zuweisen.

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Aktuell gibt es vorliegend keine internationalen Verpflichtungen der Schweiz. Die Schweiz ist zwar nicht EU-Mitglied, aber in Anbetracht der engen Verflechtung der Eidgenossenschaft mit vielen EU-Staaten wird in diesem Bereich Konformität und Kompatibilität mit dem europäischen Umfeld angestrebt.

5.3 Erlassform

Nach Artikel 164 BV sind alle wichtigen rechtsetzenden Bestimmungen in Form des Bundesgesetzes zu erlassen.

5.4 Unterstellung unter die Ausgabenbremse

Im Zusammenhang mit diesem Gesetz sind keine Ausgaben verknüpft, die eine Unterstellung unter die Ausgabenbremse bewirken würden.

5.5 Einhaltung der Grundsätze der Subventionsgesetzgebung

Die Grundsätze der Subventionsgesetzgebung sind vorliegend nicht anwendbar.

5.6 Delegation von Rechtsetzungsbefugnissen

Sowohl beim revidierten Gesetz als auch bei der aktuellen Totalrevision geht es hauptsächlich um die Delegation von Rechtsetzungsbefugnissen an den Bundesrat. Die bisherige Kompetenz des Bundesrates zum Erlass von Ausführungsbestimmungen wird mit der Totalrevision auf weitere Produkte ausgeweitet, unter anderem auf eine neue Klasse von elektronischen Zertifikation.

Die regulierten Produkte sind jedoch in keinem Bereich exklusiv. Es steht jeder beliebigen Anbieterin frei, in jeder Produktekategorie auch nicht-regulierte Produkte anzubieten. Die freiwillige Anerkennung von Anbieterinnen mit definierten Anforderungen und die Regulierung der Qualität einiger weniger Produkte durch den Staat schafft aber den Vertrauenscharakter, der von der Wirtschaft gewünscht wird und der in der Welt der Datennetze sonst nur schwer herbeizuführen ist.

5.7 Datenschutz

Elektronische Zertifikate, Signaturen und Authentisierung haben alle direkt mit Personendaten zu tun und erfordern daher unter dem Gesichtspunkt des Datenschutzes hohe Sorgfalt und Aufmerksamkeit.

Dem Anliegen wird in erster Linie Rechnung getragen, indem eine formelle gesetzliche Grundlage existiert. Dem Anliegen des Datenschutzes wird auch Rechnung getragen, indem von den Mitteln zur Erreichung des Ziels «Sicherheit und Vertrauen im elektronischen Geschäftsverkehr» das datenschutzfreundlichste gewählt wurde und indem kein Zwang konstruiert wird, identifizierende und authentisierende Mittel auch dort einzusetzen, wo sie nicht zwingend erforderlich sind.

Artikel 15 zum Datenschutz wird materiell nicht verändert.