Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

Totalrevision des Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)

Erläuternder Bericht zum Vernehmlassungs-Entwurf

1 Allgemeiner Teil

1.1 Ausgangslage

Dem Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES; SR 943.03) wurde bereits beim Erlass vorgeworfen, keine praxistaugliche Lösung für eine anerkannte elektronische Signatur bei Massengeschäften bereitzustellen.

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. Kapitel 3.3.3). Der Bundesrat hat den Bericht am 11. Juni 2010 zur Kenntnis genommen und das EJPD beauftragt, zur Umsetzung der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz den konkreten Regelungsbedarf abzuklären.

Diese Abklärungen ergaben, dass sowohl auf Seiten der Verwaltung als auch auf Seiten der Wirtschaft ein Bedarf besteht nach einer Regelung der elektronischen Signatur für juristische Personen resp. Behörden sowie der Authentifikation. Auch bestehen grössere Rechtsunsicherheiten im Umgang mit elektronisch signierten Dokumenten.

Schliesslich wurde das EJPD mit Beschluss des Bundesrates vom 27. Juni 2011 beauftragt, zum Projekt «elektronische Signatur» bis Anfangs 2012 einen vernehmlassungsreifen Vorentwurf mit erläuterndem Bericht für die erforderlichen Rechtsgrundlagen zu unterbreiten.

Der Bundesrat hat das EJPD am 28. März 2012 weiter damit beauftragt, den Umfang einer umfassenden Gesetzgebung im Anwendungsbereich der elektronischen Signatur abzuklären und dem Bundesrat bis Ende 2012 einen Vorschlag zum weiteren Vorgehen zu unterbreiten. Dabei geht es unter anderem um die Schaffung einer neuen Regelung für die „einfache elek-

tronische Schriftlichkeit“ oder eines elektronischen Zustellrechts und um eine Auslotung der Möglichkeiten, die Anforderungen an die qualifizierte elektronische Unterschrift als Äquivalent zur eigenhändigen Unterschrift zu senken. Verschiedentlich wurde schon moniert, das ganze Verfahren sei zu kompliziert und müsse entschlackt werden. Der entsprechende Bericht wird auch diesen Aspekt behandeln.

1.2 Ziele der Revision

Mit der vorliegenden Revision sollen prioritär drei Ziele erreicht werden.

- Erstens soll als Ergänzung zur bisherigen qualifizierten elektronischen Signatur, die nur natürlichen Personen zugänglich ist, eine weitere geregelte elektronische Signatur definiert werden, welche auch von juristischen Personen und Behörden erstellt werden kann und bei der auf der Stufe der technischen Ausführungsvorschriften allenfalls weitere Detail-Anpassungen an die Anforderungen des geschäftlichen Einsatzes vorgenommen werden können. Der Gesetzgeber, der ein bestimmtes Verfahren zu regeln hat, hätte dann für seine Formvorschriften künftig die Wahl zwischen der bisherigen qualifizierten elektronischen Signatur für spezielle Anforderungen und der neuen geregelten elektronischen Signatur für normale Anforderungen.
- Zweitens soll die gesetzliche Grundlage geschaffen werden, dass nebst der elektronischen Signatur auch die sichere Authentifikation 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 an 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 wurde im Rahmen der Revisionsarbeiten geprüft, ob neu allenfalls ein Zeitstempel obligatorischer Bestandteil einer qualifizierten elektronischen Signatur sein sollte.

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

Bei allen Änderungen soll an den bestehenden Konzepten und Prinzipien der bisherigen Regelung, wie beispielsweise der Freiwilligkeit für die Anbieter und der nicht abschliessenden Regelung von Zertifikatsprodukten, nichts geändert werden, und auch die Kompatibilität der schweizerischen Gesetzgebung mit der europäischen Signaturrichtlinie (RL 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 Begriffs-Definitionen und die europäisch geprägte Terminologie immer beibehalten, wenn nicht aus inhaltlichen Gründen eine Änderung notwendig war.

Wenn man sich das Ergebnis der Revision unter dem Aspekt des Produkte-Sortiments von Anbieterinnen von Zertifizierungsdiensten anschaut, dann soll dieses 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.
- Ein nach ZertES anerkannte Anbieterin kann alle vorstehend genannten Produkte anbieten plus die drei vom ZertES geregelten Produkte:

- Geregelte Zertifikate (neu):
  - Für natürliche und juristische Personen resp. Behörden
  - Für beliebige Anwendungen (ausser für die qualifizierte elektronische Signatur)
- Qualifiziertes Zertifikat (unverändert):
  - Nur für natürliche Personen
  - Nur für die qualifizierte elektronische Signatur
- Qualifizierter Zeitstempel (neu)

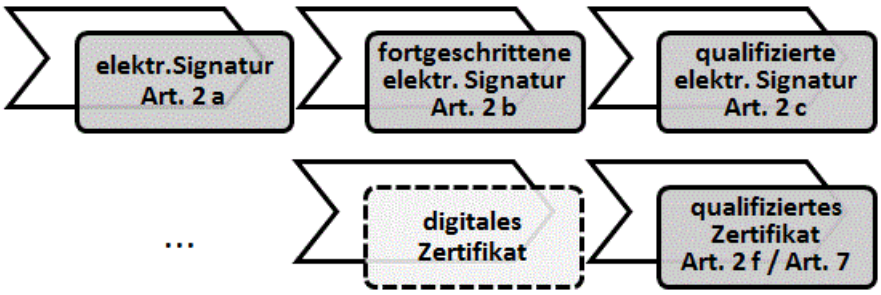
1.3 Grundzüge der Vernehmlassungsvorlage

1.3.1 Geregelte elektronische Signatur basierend auf einem geregelten Zertifikat für natürliche und juristische Personen sowie Behörden

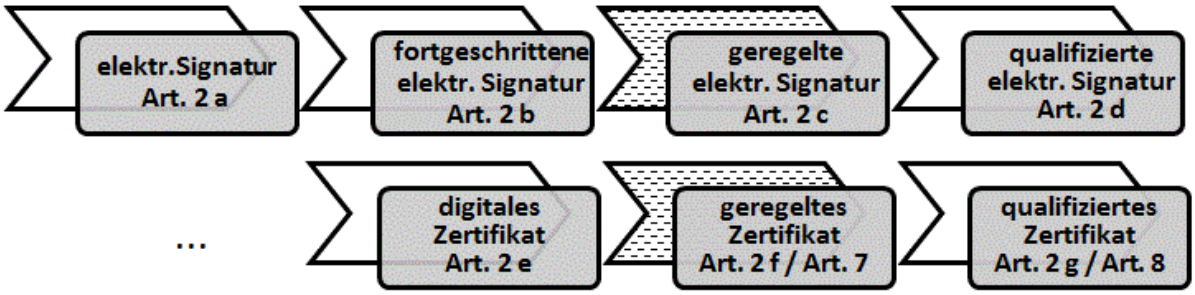
Das bisherige Gesetz definiert – in Übereinstimmung mit der EU-Richtlinie – die qualifizierte elektronische Signatur unter Verwendung eines qualifizierten Zertifikats und gibt dem Bundesrat im Artikel 6 die Kompetenz, die dazu verwendete Schlüsselgenerierung sowie die zugehörigen Signaturerstellungseinheiten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

Dies bleibt in der revidierten Version genau so, es wird jedoch zusätzlich zwischen der fortgeschrittenen und der qualifizierten elektronischen Signatur die neue «geregelte elektronische Signatur» und das dazu zu verwendende «geregelte Zertifikat» definiert. Der Bundesrat erhält die Kompetenz, auch die Generierung und Anwendung der zu diesen Zertifikaten gehörigen Schlüssel zu regeln und die Formate der Zertifikate festzulegen.

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

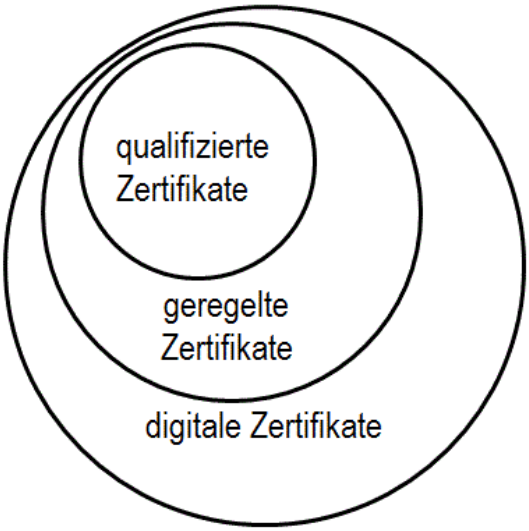


Neu sieht die Kaskade wie folgt aus: Basis für die Signaturen bleibt die elektronische Signatur (Art. 2 Bst. a; unverändert) und die auf ihr basierende fortgeschrittene elektronische Signatur (Art. 2 Bst. b) als zweite Stufe. Neu wird als dritte Spezialisierungs-Stufe die geregelte elektronische Signatur (Art. 2 Bst. c) eingeführt und erst als vierte Stufe die qualifizierte elektronische Signatur (Art. 2 Bst. d). Die qualifizierte elektronische Signatur hat alle Anforderungen an die geregelte elektronische Signatur zu erfüllen und diese wiederum alle Vorgaben der fortgeschrittenen elektronischen Signatur.



Das geregelte Zertifikat ist 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. Artikel 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 – neu – geregelte nebst natürlichen auch juristischen Personen oder Behörden als Inhaber aufweisen kann. Hingegen kann auch das geregelte Zertifikat kein reines Maschinen-Zertifikat sein, also einzig auf eine Maschine wie z.B. einen Server ausgestellt sein.



Mit Hinblick auf das Ziel der terminologischen Vereinfachung wird bei beiden geregelten Zertifikaten schon in der Definition 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 würde 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 einen Typ von Zertifikat 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, die qualifizierte elektronische Signatur, die nachstehend beschriebene Authentifikation und u.U. weitere – 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 nicht mehr für eine bestimmte Anwendung der beiden geregelten Zertifikats-Typen, sondern für beliebige Anwendungen. Die bisherigen Kompetenzen bezüglich qualifizierter elektronischer Signatur bleiben die gleichen und damit bleibt auch die Kompatibilität zur EU-Richtlinie erhalten,

einzig erhält der Bundesrat die gleiche Kompetenz auch für einen zweiten, landesspezifischen Typ von Zertifikaten und für weitere Anwendungen dieser Zertifikate.

1.3.2 Exkurs zur Problematik von Unternehmens-Zertifikaten

Während der ganzen Entstehungsgeschichte des ZertES war umstritten, ob die qualifizierten Zertifikate den natürlichen Personen vorbehalten oder auch für juristische Personen möglich sein sollen. Noch in der Botschafts-Version 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 Unternehmens-Zertifikat entgegengebracht werden. Es könnte nämlich zur Annahme verleiten, dass der jeweilige Benutzer des Unternehmens-Zertifikats rein aus der Tatsache des Zugriffs auf dieses Zertifikat eine Vertretungskompetenz für diese juristische Person hätte. Zum Schutz vor einer Untergrabung fundamentaler Prinzipien im Vertretungsrecht wurde daher schliesslich das qualifizierte Zertifikat auf natürliche Personen eingeschränkt.

Die Praxis seit Inkrafttreten des ZertES hat gezeigt, dass im realen elektronischen Geschäfts- und Behördenverkehr halt trotzdem ein grosser Bedarf nach Unternehmens-Zertifikaten besteht. Gerade bei Massengeschäften ist es seltsam anmutend und auch kaum praktikabel, wenn die Meldungen mit persönlichen Zertifikaten signiert werden und u.U. sogar alle paar Geschäfte der PIN neu eingegeben werden muss.
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 – vertraglich Form-Einreden 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.
Ein Zeichen für einen echten Mangel in diesem Bereich ist die Tatsache, dass ausgerechnet im einzigen Fall von hochvolumigem Verkehr mit Behörden, nämlich bei der Übermittlung der Rechnungen an die MWST-Verwaltung für das geltend machen des Vorsteuerabzug, vom Finanzdepartement auf dem Verordnungsweg ein eigenes Unternehmenszertifikat geregelt und durchgesetzt wurde. Dieses Vorgehen gab ja dann auch den Anlass für die eingangs erwähnte Motion Baumann und teilweise für diese Revision.

Das gleiche Problem stellt sich nicht nur für private Unternehmen, sondern auch für Behörden, so beispielsweise bei der automatisierten Produktion von Register-Auszügen, wie Strafregister-, Handelsregister- oder Grundbuchauszügen. 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 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.

Auch in der Schweiz sind heute schon verschiedene Varianten von Zertifikaten im Einsatz, die sich auf die eine oder andere Art auf juristische Personen beziehen. Nebst dem schon erwähnten MWST-Zertifikat sind das SSL-Zertifikate für vertrauenswürdige (HTTPS-)Server, z.B. für E-Banking und schliesslich gibt es auch in den qualifizierten Zertifikaten die Möglichkeit, den Inhaber oder die Inhaberin als Mitarbeitende oder gar als Vertreter einer juristischen Person zu definieren. Alle diese Fälle gaben bisher keinen Anlass zu falschen Schlüssen über die Vertretungsbefugnisse.

Die vorliegende Revision hat ausdrücklich zum Ziel, die Probleme die sich aus dem Fehlen eines geregelten Unternehmens-Zertifikats ergeben, zu beheben. Sie wählt dazu nun aber nicht die ursprünglich vorgesehene Ausweitung des qualifizierten Zertifikats, sondern kreiert ein neues geregeltes Zertifikat eigener Art, das auch ein fortgeschrittenes Zertifikat ist, aber

kein qualifiziertes, da es etwas weniger weitgehende Anforderungen erfüllen muss und eben direkt auf juristischen Personen und Behörden lauten kann.
Dieses neu geregelte Unternehmens- oder Behördenzertifikat profitiert nicht vom privilegierten Status des qualifizierten Zertifikats. Generell regelt das ZertES ja nur die Qualität gewisser Zertifizierungsprodukte und die Pflichten, die den Anbietern solcher Produkte obliegen. Die Bedeutung bestimmter Produkte oder Verfahren im Rechtsverkehr wird ausserhalb des ZertES geregelt. Im Falle der Anerkennung der qualifizierten elektronischen Signatur als Ersatz für die handschriftliche Unterschrift, geschieht dies in Artikel 14 Absatz 2^{bis} OR (SR 220). Für das neue geregelte Zertifikat und die geregelte elektronische Signatur steht es dem jeweils zuständigen Gesetzgeber frei, diese für bestimmte Funktionen zuzulassen oder eben nicht, genauso wie beispielsweise bisher die Mehrwertsteuer-Behörden für die Einreichung von Rechnungen für den Vorsteuerabzug ein von ihnen definiertes Zertifikat akzeptiert haben. Ebenso können Geschäftspartner eine gewillkürte Form wählen, für welche ein geregeltes Zertifikat genügt, wie sie das mit den EDI-Agreements im elektronischen Massen-Geschäftsverkehr bisher auch getan hatten. Im Unterschied zu bisher stehen für solche Zwecke nun aber ein einheitlich geregeltes Zertifikat und Signatur-Verfahren zur Verfügung.

Wird diese Betrachtungsweise sauber eingehalten, besteht keine Gefahr, dass aus dem Unternehmenszertifikat auf eine nicht vorhandene Vertretungsbefugnis geschlossen wird. Als zusätzliche Absicherung gegen eine diesbezügliche Fehlinterpretation wird diese Einschränkung auch noch in einem neuen Absatz 2 des Zweckartikels (Artikel 1) formuliert.

Solange das qualifizierte Zertifikat und die qualifizierte elektronische Signatur, sowie ihre Kompatibilität mit der EU-Richtlinie nicht tangiert werden und keine Einschränkungen des freien Marktes, weder bezüglich Produkte, noch bezüglich Anbieter gemacht werden, besteht kein Grund, nicht zusätzliche ausgewählte Zertifizierungsprodukte im Sinne einer Dienstleistung für die Wirtschaft staatlich zu regeln. Die vorgeschlagene Regelung stellt in gewissem Sinne für ganze Anwendungsfelder einen staatlich geregelten «Vertrauens-Anker» auf der technisch/organisatorischen Ebene bereit und fördert bzw. schafft damit Märkte in diesem Bereich. Welche juristische Bedeutung den auf diesen standardisierten Produkten basierenden Anwendungen beigemessen wird, bleibt dem Parteiwillen, weiterer Rechtsetzung und der Doktrin überlassen.

1.3.3 Authentifikation

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 gut 10 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 Web-Dienst 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 die gleichen Zertifikate wie für die elektronische Signatur verwendet,

allerdings nicht das gleiche Zertifikat für beide Anwendungen, weil sonst Angriffe durch Dritte und somit Missbräuche möglich wären. Die einschlägige Wirtschaft wünscht sich daher schon lange auch für bestimmte Fälle der Authentifikation ein vom Staat geregeltes Zertifikat, das durch seinen offiziellen Charakter und eine geregelte Qualität eine Art «Vertrauens-Anker» und damit zusätzliche Sicherheit in die Verhältnisse bringen könnte.

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 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 aller Art wie auch für die Authentifikation oder auch andere Sicherheits-Anwendungen wie das SSL-Zertifikat verwenden.

Gesetzgebungstechnisch werden daher neu alle Formulierungen, die bisher auf die Anwendung des Zertifikats für die Signatur ausgerichtet waren, anwendungs-neutral 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 Signatur-Zwecken eingesetzt wird, sich materiell nichts ändert.

1.3.4 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 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, bzw. dass eine Signatur zu einem bestimmten Zeitpunkt erstellt worden ist. Ohne Zeitstempel hat der Zeitpunkt bzw. das Datum einer Signatur streng genommen nur den Wert einer unbestätigten Behauptung. Gewisse Angriffe, bzw. Betrugsszenarien lassen sich nur mit der Integration eines Zeitstempels in die elektronische Signatur verhindern. Im Hinblick auf diesen Sachverhalt sind schon heute nach Artikel 12 des geltenden ZertES die anerkannten Anbieterinnen von Zertifizierungsdienstleistungen verpflichtet, einen Zeitstempel-Dienst anzubieten.

Heutige Signatur-Programme bieten normalerweise die Integration eines Zeitstempels in die Signatur an. Meist kann diese Variante auch als Standard-Vorgabe eingestellt werden.

Für die Einbettung eines Zeitstempels in die elektronische Signatur muss man zum Zeitpunkt des Signierens mit dem Internet verbunden sein. Dies war zum Entstehungszeitpunkt des heutigen ZertES ganz klar noch eine zu hohe Hürde. 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:

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 nicht für die qualifizierte elektronische Signatur im ZertES vorgeschrieben. Diese Frage wird erst für die Anerkennung dieser Signatur im OR als Ersatz für die eigenhändige Unterschrift geregelt.

Die strengste Lösungsvariante wurde von Branchen-Vertretern und Spezialisten mehrheitlich als zu einschränkend abgelehnt und schliesslich, nicht zuletzt auch aufgrund der Tatsache, dass eine solche Verpflichtung in der EU-Richtlinie und in den Nachbarländern nicht vorgesehen ist, fallen gelassen.

Vorgeschlagen wird im vorliegenden Entwurf die dritte Variante, bei der sich das ZertES selbst zu dieser Frage nicht äussert und erst die konkrete Anwendung bei Bedarf dieses Erfordernis anstellt, z.B. das OR für die Verwendung der elektronischen Signatur als Ersatz der eigenhändigen Unterschrift.

1.3.5 Terminologische Anpassungen

Die Basis für eine wichtige terminologische Vereinfachung wurde schon im Kapitel 1.3.1 bei den Ausführungen zu den neuen Definitionen für die Zertifikate beschrieben. Danach kann nun in einem Erlass die typischerweise für den Ersatz der Schriftform benötigte Signatur wesentlich kürzer einfach als «qualifizierte Signatur des 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 «qualifizierte 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, wie z.B. einer Buchhaltung, genannt, wodurch später zusammen mit der elektronischen Signatur 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 «qualifizierte Zeitstempel nach ZertES» referenziert werden.

1.3.6 Zur Revisionstechnik

Die vorliegende Revision war ursprünglich als Teilrevision geplant. Von den relativ begrenzten Zielen her (siehe vorstehend, Kapitel 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 anwendungs-neutral genannt werden – z.B. «kryptografischer Schlüssel» statt Prüfschlüssel – ist die Mehrzahl der Artikel von der Revision betroffen wodurch sie nach den üblichen Kriterien zu einer Totalrevision wurde.

1.3.7 Weitere Revisionen

Mehrere Gesetze und Verordnungen nehmen inzwischen Bezug auf die Konzepte des ZertES, insbesondere natürlich die qualifizierte elektronische Signatur. Neu soll in diesen Erlassen nun im Normalfall auf die geregelte elektronische Signatur verwiesen werden, womit auch Signaturen von juristischen Personen und Behörden zugelassen wären. Die qualifizierte elektronische Signatur soll nur in Spezialfällen, wenn die direkte Zuordnung zu einer natürlichen Person unabdingbar ist, verlangt werden. Dies entspricht der generellen Strategie, die Hürden für den elektronischen Geschäftsverkehr nicht höher zu stellen, als es sachlich unbedingt notwendig ist.

2 Erläuterung der einzelnen Bestimmungen

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 steht dabei in erster Linie 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 wurde und wird von seinem Gegenstand der Regelung her oft über-interpretiert, 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 Zertifikats-Produkte, indem es gewisse Anforderungen an die Produkte selbst aber 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 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 Buchstabe a) und Absatz 3 Buchstabe b (bisher Absatz 2 Buchstabe b) weiter als bisher formuliert.

Der neue Absatz 2 nimmt die im vorstehenden Kapitel 1.3.2 abgehandelten Bedenken auf, ein auf eine juristische Person oder eine Behörde ausgestelltes 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 auch nur 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 Buchstage a harmonisiert die Terminologie zum Absatz 1 und Buchstabe b passt die Formulierung der schon mehrfach erwähnten Ausweitung im Zweck an.

Art. 2 Begriffe

Es werden die neu geregelten Begriffe an ihrem systematischen Platz eingefügt, was auch eine Neunummerierung der bisherigen Buchstaben d ff. 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 Buchstabe c 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).
- Bst. d: 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. e: 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, weicht auch vom Grundsatz ab, dass bei dieser Revision nur geändert werden soll, was für die Zielsetzung (siehe Kapitel 1.2) zwingend notwendig ist, 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, wie 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 wenige verständlich eingeschätzt.
- Bst. f: geregeltes Zertifikat
  Das neu geregelte Zertifikat wird nach dem Bespiel des bisher unter Buchstabe f definierten qualifizierten Zertifikat definiert. Gemäss den Anforderungen des Artikels 7 ist es ein etwas einfacheres, bzw. allgemeineres digitales Zertifikat als das qualifizierte Zertifikat und bildet neu nun 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. g: qualifiziertes Zertifikat
  Das bisher in Buchstabe f definierte qualifizierte Zertifikat. Nach neuer Systematik ist es ein Spezialfall des in Buchstabe f neu eingeführten, geregelten Zertifikats, mit ein paar zusätzlichen Anforderungen. In der Summe sind es aber die bisherigen Anforderungen, ausser der hier – via das geregelte Zertifikat – ebenfalls neu hinzugekommenen Anforderung, dass es immer von einer anerkannten Anbieterin ausgestellt sein muss.

2.1.3 2. Abschnitt: Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Am bisherigen System der Anerkennung soll grundsätzlich nichts geändert werden. 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 Artikel 14) und die Haftung (neu Artikel 17) im Artikel 3 Absatz 1 Buchstabe f.

2.1.4 3. Abschnitt: Generierung, Speicherung und Anwendung 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 Authentifikation 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 Signatur-Anwendung gesprochen. Neu soll – wie in Kapitel 1.3.1 beschrieben – der Bundesrat auch die Kompetenz erhalten, andere Anwendungen von Zertifikaten und zugehörigen Schlüsseln zu regeln, insbesondere die Authentifikation. Daher spricht der Artikel neu nicht mehr von Signatur und Signaturprüfung, sondern von der Anwendung von Schlüsseln generell.

Der bisherige Absatz 3 des Artikels 6 wurde beinahe 1:1 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. 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 (einfache) geregelte Zertifikate sowohl an natürliche wie 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 Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010 (UIDG, SR 431.03) 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 Identitäts-Feststellung durch die Zertifizierungsdienste-Anbieterin könnte sich aufwändig gestalten. Wenn eine solche Person trotzdem am elektronischen Geschäftsverkehr teilnehmen wollen sollte, was eher unwahrscheinlich ist, kann sie das durch eine natürliche Person, die sie vertritt.

Der Buchstabe b wird wie überall auf geregelte Zertifikate allgemein ausgeweitet.

Der 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 b 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) 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 Authentifikation 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 der neuen geregelten Signatur 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. Die geregelte elektronische Signatur unter Verwendung des geregelten Zertifikats deckt genau dieses Bedürfnis ab.

Im Absatz 3 (bisher 2) 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 regelt 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 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 des 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 verwendet werden darf. Dies wieder als 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 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 2 erhöht werden müssen.

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

Art. 12 (bisher 11) Verzeichnisdienst für geregelte Zertifikate

Die neue Formulierung von Absatz 2 beseitigt eine bisherige Unklarheit.

Art. 13 (bisher 12) Qualifizierte Zeitstempel

Der neue Titel des Artikels ermöglicht es, dass mit einem einzigen Begriff der im Vergleich zu irgendeinem Zeitstempel besonders vertrauenswürdige Zeitstempel einer anerkannten Anbieterin von Zertifizierungsdiensten referenziert werden kann.

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. 20 (bisher 19)

‚digitaler Zertifikate' statt ‚Zertifikate' als terminologische Präzisierung.

2.1.7 Verschiedene Anpassungen in den Abschnitten 5 bis 9

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

Anpassung der Artikel-Nummer

Bis auf den letzten Artikel werden alle Artikelnummern um 1 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, 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. Ausnahmsweise wird mit dem gleichen Zweck einer eleganteren Formulierung der Vorzug gegeben.
Diese Anpassung betrifft die (neuen) Artikel 9, 10, 11, 12, 13, 14, 17, 18 und 21.

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

Da neu nicht mehr nur die Signatur sondern auch andere Anwendungen von digitalen Zertifikaten 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, Art. 17 Abs. 3, Art. 18).

2.2 Änderung weiterer Erlasse

2.2.1 Obligationenrecht

Art. 14 Unterschrift

Nachdem nun im Definitions-Teil des ZertES (vgl. Art. 2 Bst. d, f und g bzw. Kap. 1.3.1 vorstehend) die qualifizierte elektronische Signatur neu die Ausstellung des verwendeten Zertifikats durch eine anerkannte Anbieterin voraussetzt, kann Abs. 2^{bis} von Art. 14 OR stark vereinfacht und damit leserlicher gestaltet werden.

Variante: qualifizierte elektronische Signatur mit obligatorischem Zeitstempel

Wie in Kapitel 1.3.4 ausgeführt, gibt es Tendenzen, 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 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 in einen bestimmten Bereich verlangt wird. Genau dies könnte man nun z.B. für die Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift in Artikel 14 Absatz 2bis verlangen, wozu in der Vorlage eine Variante formuliert ist.

Art. 59a Haftung für Signaturschlüssel

Die bisherige Haftung des Schlüsselinhabers für qualifizierte Zertifikate soll auch auf geregelte Zertifikate ausgedehnt werden, weil diese Haftung eine der essentiellen Grundlagen für die Akzeptanz beim Dritten ist; ohne diese Haftung wäre das geregelte Zertifikat in den Augen dessen, der sich darauf verlassen soll, wenig wert. Allerdings soll die Haftung auf Signatur-Anwendungen beschränkt sein und für Authentisierung oder weitere Anwendungen nicht gelten. Aus diesem Grund wird hier der Begriff «Signaturschlüssel» nicht durch den generellen Begriff «kryptografischer Schlüssel» ersetzt.

2.2.2 Erweiterung der Delegationskompetenz

In verschiedenen Verfahrensgesetzen des Bundes wird jeweils bestimmt, dass eine Eingabe mit einer anerkannten elektronischen Signatur zu versehen sei. Mit der Einführung der geregelten elektronischen Signatur steht in Zukunft neben der bisherigen qualifizierten elektronischen Signatur eine zweite anerkannte elektronische Signatur gemäss ZertES zur Verfügung. Somit muss neu auf Verordnungsstufe geregelt werden, welche elektronische Signatur zu verwenden ist. Dazu braucht es eine Erweiterung der Delegationskompetenz an den Bundesrat.

Betroffen sind
- Art. 21*a* Abs. 2 und Art. 34 Abs. 1bis des Verwaltungsverfahrensgesetzes vom 20.12.1968;
- Art. 130 Abs. 2 der Zivilprozessordnung vom 19. Dezember 2008; und
- Art. 110 Abs. 2 der Strafprozessordnung vom 5. Oktober 2007.

Während die Delegationskompetenz an den Bundesrat in Art. 33*a* Abs. 2 des Bundesgesetzes über die Schuldbetreibung und Konkurs vom 11. April 1889 bereits genügt, muss die entsprechende Kompetenz in Art. 42 Abs. 4 des Bundesgerichtsgesetzes vom 17. Juni 2005 an das Bundesgericht delegiert werden.

Die erforderliche terminologische Bereinigung bzw. Vereinfachung bei der Regelung der elektronischen Signatur wird dann mit Anpassungen von verschiedensten Verordnungen herbeizuführen sein. Benutzt wird der Begriff der elektronischen Signatur insbesondere in folgenden Ausführungsbestimmungen:
- Art. 14a Abs. 2 der Verordnung über die Ausweise für Schweizer Staatsangehörige vom 20. September 2002 (Ausweisverordnung, VAwG; SR 143.11)
- Art. 27*k*^{bis} Abs. 2 und 3 sowie Art. 27*d* Abs. 2 Bst. a und b der Verordnung über die politischen Rechte vom 24. Mai 1978 (SR 161.11)
- Art. 4 Abs. 2 Bst. f, Art. 6 Abs. 1, 2 und 3, Art. 9 Abs. 4 und 5 sowie Art. 12 Abs. 1 Bst. c und d der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens vom 18. Juni 2010 (SR 172.021.2)
- Art. 2 Bst. d sowie Art. 4 Abs. 3 des Reglementes des Bundesgerichts über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen vom 5. Dezember 2006 (ReRBGer; SR 173.110.29):
- Art. 11 Abs. 3 der Handelsregisterverordnung vom 17. Oktober 2007 (HRegV; SR 221.411)

- Art. 8 Abs. 2 sowie Art. 13 Abs. 2 Bst. a der Verordnung über das Schweizerische Handelsamtsblatt vom 15. Februar 2006 (Verordnung SHAB; SR 221.415)
- Art. 2 Bst. a und b, Art. 5 Abs. 2 Bst. c, Art. 7, Art. 10 Abs. 3, Art. 13 Abs. 1 Bst. c und d sowie Art. 14 Abs. 2 Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie Schuldbetreibungs- und Konkursverfahren vom 18. Juni 2010 (SR 272.1)
- Art. 4 Abs. 1 der Verordnung des EJPD über die elektronische Übermittlung im Bereich Schuldbetreibung und Konkurs vom 9. Februar 2011 (SR 281.112.1)
- Art. 17 Abs. 3 Bst. c und Abs. 4 der Registerharmonisierungsverordnung vom 21. November 2007 (RHV; SR 431.021)
- Art. 2 Abs. 2 und 3, Art. 2 Abs. 2 Bst. a Ziff. 5, Art. 2 Abs. 4 sowie Art. 3 Abs. 1 Bst. a, c und d der Verordnung des EFD über elektronische Daten und Informationen vom 11. Dezember 2009 (EIDI-V; SR 641.201.511)
- Art. 5 Abs. 4 der Verordnung des UVEK über den Nachweis der Produktionsart und der Herkunft von Elektrizität vom 24. November 2006 (SR 730.010.1)
- Art. 63 Abs. 2 Bst. c der Verordnung über die Direktzahlungen an die Landwirtschaft vom 7. Dezember 1998 (Direktzahlungsverordnung, DZV; SR 910.13)
- Art. 20 Abs. 1^{bis} Bst. c der Verordnung über Sömmerungsbeiträge vom 14. November 2007 (Sömmerungsbeitragsverordnung, SöBV; SR 910.133)
- Art. 8 Abs. 1^{bis} Bst. c der Verordnung über die regionale Förderung der Qualität und der Vernetzung von ökologischen Ausgleichsflächen in der Landwirtschaft vom 4. April 2001 (Öko-Qualitätsverordnung, ÖQV; SR 910.14)
- Art. 5 Abs. 1^{bis} Bst. c der Verordnung über Flächen- und Verarbeitungsbeiträge im Ackerbau vom 7. Dezember 1998 (Ackerbaubeitragsverordnung, ABBV; SR 910.17)
- Art. 5 Abs. 3, Art. 7 Abs. 2 sowie Art. 9 Abs. 3 der Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 3. Dezember 2004 (Verordnung über die elektronische Signatur, VZertES; SR 943.032)
- Art. 1 sowie Anhang der Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 6. Dezember 2004 (SR 943.032.1)