Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

(Bundesgesetz über die elektronische Signatur, ZertES)

vom 18. März 2016 (Stand am 1. Januar 2017)

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,

gestützt auf die Artikel 95 Absatz 1 und 122 Absatz 1 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom 15. Januar 2014[2],

beschliesst:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand und Zweck

[1] Dieses Gesetz regelt:

a. die Anforderungen an die Qualität bestimmter digitaler Zertifikate und an ihre Verwendung;

b. die Voraussetzungen, unter denen sich Anbieterinnen von Zertifizierungsdiensten im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Zertifizierungsdienste) anerkennen lassen können;

c. die Rechte und Pflichten der anerkannten Anbieterinnen von Zertifizierungsdiensten.

[2] Es regelt mit Ausnahme der Haftung nach den Artikeln 17 und 18 nicht die Rechtswirkungen der Verwendung digitaler Zertifikate.

[3] Es hat zum Zweck:

a. ein breites Angebot an sicheren Zertifizierungsdiensten zu fördern;

b. die Verwendung digitaler Zertifikate, elektronischer Signaturen und elektronischer Siegel zu begünstigen;

c. die internationale Anerkennung der Anbieterinnen von Zertifizierungsdiensten und ihrer Leistungen zu ermöglichen.

Art. 2 Begriffe

In diesem Gesetz bedeuten:

AS **2016** 4651
1 SR **101**
2 BBl **2014** 1001

a. *elektronische Signatur*: Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen;

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

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

d. *geregeltes elektronisches Siegel*: eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelerstellungseinheit nach Artikel 6 erstellt wurde und auf einem geregelten, auf eine UID-Einheit nach Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010[3] über die Unternehmens-Identifikationsnummer (UIDG) ausgestellten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat beruht;

e. *qualifizierte elektronische Signatur*: eine geregelte elektronische Signatur, die auf einem qualifizierten Zertifikat beruht;

f. *digitales Zertifikat*: eine digitale Bescheinigung, die den öffentlichen Schlüssel eines asymmetrischen kryptografischen Schlüsselpaars seinem Inhaber oder seiner Inhaberin zuordnet;

g. *geregeltes Zertifikat*: ein digitales Zertifikat, das die Anforderungen nach Artikel 7 erfüllt und von einer nach diesem Gesetz anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt wurde;

h. *qualifiziertes Zertifikat*: ein geregeltes Zertifikat, das die Anforderungen nach Artikel 8 erfüllt;

i. *elektronischer Zeitstempel*: Bestätigung, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen;

j. *qualifizierter elektronischer Zeitstempel*: elektronischer Zeitstempel, der von einer nach diesem Gesetz anerkannten Anbieterin von Zertifizierungsdiensten ausgestellt und mit einem geregelten elektronischen Siegel versehen wurde;

3 SR **431.03**

k. *Anbieterin von Zertifizierungsdiensten*: Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt;

l. *Anerkennungsstelle*: Stelle, die nach der Bundesgesetzgebung über die technischen Handelshemmnisse[4] für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist.

2. Abschnitt: Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Art. 3 Anerkennungsvoraussetzungen

1 Als Anbieterinnen von Zertifizierungsdiensten anerkannt werden können natürliche oder juristische Personen, die:

a. im Handelsregister eingetragen sind;

b. in der Lage sind, qualifizierte Zertifikate gemäss den Anforderungen dieses Gesetzes auszustellen und zu verwalten;

c. Personal mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen;

d. Informatiksysteme und -produkte, insbesondere Signatur- und Siegelerstellungseinheiten verwenden, die verlässlich und vertrauenswürdig sind;

e. über ausreichende Finanzmittel oder -garantien verfügen;

f. die notwendigen Versicherungen zur Deckung von Haftungsansprüchen aus Artikel 17 und der Kosten, welche aus den in Artikel 14 Absätze 2 und 3 vorgesehenen Massnahmen erwachsen könnten, abschliessen;

g. die Einhaltung des anwendbaren Rechts, namentlich dieses Gesetzes und seiner Ausführungsbestimmungen, gewährleisten.

2 Die Voraussetzungen nach Absatz 1 gelten auch für ausländische Anbieterinnen von Zertifizierungsdiensten. Ist eine ausländische Anbieterin bereits von einer ausländischen Anerkennungsstelle anerkannt worden, so kann die schweizerische Anerkennungsstelle sie anerkennen, wenn erwiesen ist, dass:

a. sie die Anerkennung nach ausländischem Recht erworben hat;

b. die für die Anerkennung massgebenden Vorschriften des ausländischen Rechts den schweizerischen Vorschriften gleichwertig sind;

c. die ausländische Anerkennungsstelle über Qualifikationen verfügt, die denen, die von schweizerischen Anerkennungsstellen gefordert werden, gleichwertig sind;

4 SR **946.51**, **946.511**, **946.512**, **946.513.7**

d. die ausländische Anerkennungsstelle die Zusammenarbeit mit der schweizerischen Anerkennungsstelle zur Überwachung der Anbieterin in der Schweiz gewährleistet.

3 Verwaltungseinheiten von Bund, Kantonen und Gemeinden dürfen als Anbieterinnen von Zertifizierungsdiensten anerkannt werden, ohne im Handelsregister eingetragen zu sein.

Art. 4 Bezeichnung der Akkreditierungsstelle

1 Der Bundesrat bezeichnet die für die Akkreditierung der Anerkennungsstellen zuständige Stelle (Akkreditierungsstelle).

2 Ist keine Stelle für die Anerkennung akkreditiert, so bezeichnet der Bundesrat die Akkreditierungsstelle oder eine andere geeignete Stelle als Anerkennungsstelle.

Art. 5 Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten

1 Die Anerkennungsstellen melden der Akkreditierungsstelle die von ihnen anerkannten Anbieterinnen von Zertifizierungsdiensten.

2 Die Akkreditierungsstelle stellt der Öffentlichkeit die Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten zur Verfügung.

3. Abschnitt: Generierung, Speicherung und Verwendung kryptografischer Schlüssel

Art. 6

1 Der Bundesrat regelt die Generierung, Speicherung und Verwendung kryptografischer Schlüssel, für die geregelte Zertifikate im Sinne dieses Gesetzes ausgestellt werden können; er sorgt dabei für ein der technischen Entwicklung entsprechendes hohes Sicherheitsniveau.

2 Bei Systemen zur Generierung, Speicherung und Verwendung privater kryptografischer Schlüssel, insbesondere bei Signatur- und Siegelerstellungseinheiten, muss zumindest gewährleistet werden, dass diese Schlüssel:

a. praktisch nur einmal auftreten können und ihre Geheimhaltung hinreichend gewährleistet ist;

b. mit hinreichender Sicherheit nicht abgeleitet werden können und ihre Verwendung bei Einsatz der jeweils verfügbaren Technologie vor Fälschungen geschützt ist;

c. von der rechtmässigen Inhaberin oder vom rechtmässigen Inhaber vor der missbräuchlichen Verwendung durch andere verlässlich geschützt werden können.

4. Abschnitt: Geregelte Zertifikate

Art. 7 Anforderungen an alle geregelten Zertifikate

[1] Ein geregeltes Zertifikat kann auf natürliche Personen und UID-Einheiten ausgestellt werden.

[2] Es muss folgende Angaben enthalten:

a. die Seriennummer;

b. den Hinweis, dass es sich um ein geregeltes Zertifikat handelt;

c. den Namen oder die Bezeichnung der Inhaberin oder des Inhabers des zugehörigen privaten kryptografischen Schlüssels; besteht eine Verwechslungsmöglichkeit, so ist der Name oder die Bezeichnung mit einem unterscheidenden Zusatz zu versehen;

d. bei natürlichen Personen gegebenenfalls das als solches gekennzeichnete Pseudonym anstelle des Namens;

e. bei UID-Einheiten die Unternehmens-Identifikationsnummer nach dem UIDG[5];

f. den öffentlichen kryptografischen Schlüssel;

g. die Gültigkeitsdauer;

h. den Namen, den Niederlassungsstaat und das geregelte elektronische Siegel der Anbieterin von Zertifizierungsdiensten, die das Zertifikat ausstellt.

[3] Das Zertifikat kann zudem die folgenden Elemente enthalten:

a. spezifische Attribute der Inhaberin oder des Inhabers des zugehörigen privaten kryptografischen Schlüssels, beispielsweise berufliche Qualifikationen;

b. bei natürlichen Personen den Hinweis, dass sie zur Vertretung einer bestimmten UID-Einheit berechtigt ist;

c. den Geltungsbereich, für den das Zertifikat bestimmt ist;

d. die Obergrenze der Transaktionen, für die das Zertifikat bestimmt ist.

[4] Der Bundesrat bestimmt das Format der geregelten Zertifikate.

Art. 8 Zusätzliche Anforderungen an qualifizierte Zertifikate

[1] Ein qualifiziertes Zertifikat darf nur auf eine natürliche Person ausgestellt werden.

[2] Es enthält einen Eintrag, wonach es nur für die elektronische Signatur bestimmt ist.

[3] Anstelle des Hinweises nach Artikel 7 Absatz 2 Buchstabe b ist der Hinweis ins Zertifikat aufzunehmen, dass es sich um ein qualifiziertes Zertifikat handelt.

5 SR **431.03**

5. Abschnitt:
Pflichten anerkannter Anbieterinnen von Zertifizierungsdiensten

Art. 9 Ausstellung geregelter Zertifikate

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die einen Antrag auf Ausstellung eines geregelten Zertifikats stellen, verlangen:

a. bei natürlichen Personen: dass sie persönlich erscheinen und den Nachweis ihrer Identität erbringen;

b. bei UID-Einheiten, die nicht natürliche Personen sind: dass eine Vertretung persönlich erscheint und den Nachweis sowohl für die eigene Identität als auch für die Vertretungsmacht erbringt.

2 Für Attribute zu berufsbezogenen oder sonstigen Angaben zur Person (Art. 7 Abs. 3 Bst. a) müssen sie überprüfen, ob die zuständige Stelle diese Angaben bestätigt hat.

3 Für Hinweise auf die Vertretungsbefugnis (Art. 7 Abs. 3 Bst. b) müssen sie überprüfen, ob die vertretene UID-Einheit zugestimmt hat.

4 Der Bundesrat bezeichnet die Dokumente, mit denen die antragstellende Person ihre Identität und allfällige Attribute nachweisen kann. Er kann vorsehen, dass unter bestimmten Voraussetzungen auf das persönliche Erscheinen der antragstellenden Person verzichtet wird.

5 Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen sich ferner vergewissern, dass die Person, die ein geregeltes Zertifikat verlangt, im Besitz des entsprechenden privaten kryptografischen Schlüssels ist.

6 Die anerkannten Anbieterinnen von Zertifizierungsdiensten können die Identifikation von Antragstellerinnen oder Antragstellern an Dritte delegieren (Registrierungsstellen). Sie haften für die korrekte Ausführung der Aufgabe durch die Registrierungsstelle.

Art. 10 Informations- und Dokumentationspflicht

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen ihre allgemeinen Vertragsbedingungen sowie Informationen über ihre Zertifizierungspolitik allgemein zugänglich machen.

2 Sie müssen ihre Kundinnen und Kunden spätestens bei der Ausstellung der geregelten Zertifikate auf die Folgen eines möglichen Missbrauchs des privaten kryptografischen Schlüssels und auf die nach den Umständen notwendigen Vorkehrungen zur Geheimhaltung aufmerksam machen.

3 Sie führen ein Tätigkeitsjournal. Der Bundesrat regelt, wie lange das Tätigkeitsjournal und die dazugehörenden Belege aufzubewahren sind.

Art. 11 Ungültigerklärung geregelter Zertifikate

[1] Die anerkannten Anbieterinnen von Zertifizierungsdiensten erklären ein geregeltes Zertifikat unverzüglich für ungültig, wenn:

a. die Inhaberin oder der Inhaber oder die Person, die sie oder ihn vertritt, einen entsprechenden Antrag stellt;

b. sich herausstellt, dass dieses unrechtmässig erlangt worden ist oder dass Angaben nach Artikel 7 Absatz 3 nicht oder nicht mehr richtig sind;

c. es keine Gewähr mehr bietet für die Zuordnung zur Inhaberin oder zum Inhaber.

[2] Bei der Ungültigerklärung nach Absatz 1 Buchstabe a müssen sie sich vergewissern, dass die Person, welche die Ungültigerklärung beantragt, dazu berechtigt ist.

[3] Sie informieren die Inhaberinnen und Inhaber unverzüglich über die erfolgte Ungültigerklärung.

Art. 12 Verzeichnisdienste für geregelte Zertifikate

[1] Jede anerkannte Anbieterin von Zertifizierungsdiensten stellt sicher, dass die Gültigkeit aller geregelten Zertifikate, die sie ausgestellt hat, mit einem gebräuchlichen Verfahren jederzeit zuverlässig überprüft werden kann.

[2] Sie kann zudem einen Verzeichnisdienst anbieten, über den jedermann die von ihr ausgestellten geregelten Zertifikate suchen und abrufen kann. In dieses Verzeichnis wird ein Zertifikat nur auf Verlangen des Inhabers beziehungsweise der Inhaberin eingetragen.

[3] Abfragen der öffentlichen Hand sind unentgeltlich.

[4] Der Bundesrat bestimmt die Mindestdauer, während der die Überprüfung von nicht mehr gültigen geregelten Zertifikaten möglich bleiben muss.

Art. 13 Qualifizierte elektronische Zeitstempel

Auf entsprechendes Begehren müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten qualifizierte elektronische Zeitstempel ausgeben.

Art. 14 Einstellung der Geschäftstätigkeit

[1] Die anerkannten Anbieterinnen von Zertifizierungsdiensten melden der Akkreditierungsstelle die Einstellung ihrer Geschäftstätigkeit rechtzeitig. Eine gegen sie gerichtete Konkursandrohung melden sie unverzüglich.

[2] Die Akkreditierungsstelle beauftragt eine andere anerkannte Anbieterin von Zertifizierungsdiensten, das Verzeichnis der gültigen, der abgelaufenen und der für ungültig erklärten geregelten Zertifikate zu führen und das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren. Der Bundesrat bezeichnet eine geeignete Stelle zur Übernahme der Aufgabe, wenn es an einer anerkannten Anbieterin von Zertifizierungsdiensten fehlt. Die anerkannte Anbieterin von Zertifizierungsdiensten, die ihre Tätigkeit aufgibt, trägt die daraus entstehenden Kosten.

3 Absatz 2 gilt auch dann, wenn eine anerkannte Anbieterin von Zertifizierungsdiensten in Konkurs fällt.

Art. 15 Datenschutz

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten und die von ihnen beauftragten Registrierungsstellen dürfen nur diejenigen Personendaten bearbeiten, die zur Erfüllung ihrer Aufgaben erforderlich sind. Sie dürfen mit diesen Daten keinen Handel treiben.

2 Im Übrigen gilt die Datenschutzgesetzgebung.

6. Abschnitt: Aufsicht über die anerkannten Anbieterinnen von Zertifizierungsdiensten

Art. 16

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten werden nach den Regeln der Bundesgesetzgebung über die technischen Handelshemmnisse[6] von den Anerkennungsstellen beaufsichtigt.

2 Eine Anerkennungsstelle meldet der Akkreditierungsstelle unverzüglich den Entzug der Anerkennung einer Anbieterin von Zertifizierungsdiensten. Artikel 14 Absatz 2 findet Anwendung.

7. Abschnitt: Haftung

Art. 17 Haftung der Anbieterin von Zertifizierungsdiensten

1 Die anerkannte Anbieterin von Zertifizierungsdiensten haftet der Inhaberin oder dem Inhaber eines gültigen geregelten Zertifikats und Drittpersonen, die sich auf ein solches Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anbieterin den Pflichten aus diesem Gesetz und den entsprechenden Ausführungsbestimmungen nicht nachgekommen ist.

2 Sie trägt die Beweislast dafür, den Pflichten aus diesem Gesetz und den Ausführungsbestimmungen nachgekommen zu sein.

3 Sie kann ihre Haftung aus diesem Gesetz weder für eigenes Verhalten noch für jenes ihrer Hilfspersonen wegbedingen. Sie haftet jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 7 Abs. 3 Bst. c und d) ergeben.

6 SR **946.51**, **946.511**, **946.512**, **946.513.7**

Art. 18 Haftung der Anerkennungsstelle

Die Anerkennungsstelle haftet der Inhaberin oder dem Inhaber eines gültigen geregelten Zertifikats und Drittpersonen, die sich auf ein solches Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anerkennungsstelle ihren Pflichten aus diesem Gesetz und den Ausführungsbestimmungen nicht nachgekommen ist. Artikel 17 Absätze 2 und 3 gilt sinngemäss.

Art. 19 Verjährung

Die auf dieses Gesetz gestützten Ansprüche verjähren ein Jahr, nachdem die oder der Berechtigte vom Schaden und von der Person der oder des Ersatzpflichtigen Kenntnis hat, spätestens aber zehn Jahre nach der schädigenden Handlung. Vorbehalten bleiben vertragliche Ansprüche.

8. Abschnitt: Internationale Abkommen

Art. 20

1 Um die internationale Verwendung elektronischer Signaturen und anderer Anwendungen kryptografischer Schlüssel sowie deren rechtliche Anerkennung zu erleichtern, kann der Bundesrat internationale Abkommen schliessen, namentlich über:

a. die Anerkennung elektronischer Signaturen, elektronischer Siegel und digitaler Zertifikate;

b. die Anerkennung von Anbieterinnen von Zertifizierungsdiensten und von Anerkennungsstellen;

c. die Anerkennung von Prüfungen und Konformitätsbewertungen;

d. die Anerkennung von Konformitätszeichen;

e. die Anerkennung von Akkreditierungssystemen und akkreditierten Stellen;

f. die Erteilung von Normungsaufträgen an internationale Normungsorganisationen, soweit in der Gesetzgebung auf bestimmte technische Normen verwiesen wird oder verwiesen werden soll;

g. die Information und Konsultation bezüglich Vorbereitung, Erlass, Änderung und Anwendung solcher Vorschriften oder Normen.

2 Zur Ausführung internationaler Abkommen über Gegenstände nach Absatz 1 erlässt der Bundesrat die erforderlichen Bestimmungen.

3 Er kann Aufgaben im Zusammenhang mit der Information und der Konsultation bezüglich Vorbereitung, Erlass und Änderung von Vorschriften oder von technischen Normen Privaten übertragen und dafür eine Abgeltung vorsehen.

9. Abschnitt: Schlussbestimmungen

Art. 21 Vollzug

1 Der Bundesrat erlässt die Ausführungsbestimmungen. Er berücksichtigt dabei das entsprechende internationale Recht und kann internationale technische Normen für anwendbar erklären.

2 Er kann den Erlass administrativer und technischer Vorschriften dem Bundesamt für Kommunikation übertragen.

3 Um den Gesetzeszweck zu erfüllen, kann er eine Verwaltungseinheit des Bundes oder eines Kantons beauftragen, geregelte Zertifikate auch für den Privatrechtsverkehr auszustellen oder sich an einer privaten Anbieterin von Zertifizierungsdiensten zu beteiligen.

Art. 22 Aufhebung und Änderung anderer Erlasse

Die Aufhebung und die Änderung anderer Erlasse werden im Anhang geregelt.

Art. 23 Referendum und Inkrafttreten

1 Dieses Gesetz untersteht dem fakultativen Referendum.

2 Der Bundesrat bestimmt das Inkrafttreten.

Datum des Inkrafttretens: 1. Januar 2017[7]

7 BRB vom 23. Nov. 2016

Anhang
(Art. 22)

Aufhebung und Änderung anderer Erlasse

I

Das Bundesgesetz vom 19. Dezember 2003[8] über die elektronische Signatur wird aufgehoben.

II

Die nachstehenden Bundesgesetze werden wie folgt geändert:

…[9]

8 [AS **2004** 5085, **2008** 3437 Ziff. II 55]
9 Die Änd. können unter AS **2016** 4651 konsultiert werden.