

**Bundesgesetz
über Zertifizierungsdienste im Bereich
der elektronischen Signatur
(Bundesgesetz über die elektronische Signatur, ZertES)**

vom 19. Dezember 2003 (Stand am 1. August 2008)

*Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 95 Absatz 1 und 122 Absatz 1 der Bundesverfassung¹,
nach Einsicht in die Botschaft des Bundesrates vom 3. Juli 2001²,
beschliesst:*

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand und Zweck

¹ Dieses Gesetz regelt:

- a. die Voraussetzungen, unter denen sich Anbieterinnen von Zertifizierungsdiensten im Bereich der elektronischen Signatur anerkennen lassen können;
- b. die Rechte und Pflichten der anerkannten Anbieterinnen von Zertifizierungsdiensten.

² Es hat zum Zweck:

- a. ein breites Angebot an sicheren Diensten der elektronischen Zertifizierung zu fördern;
- b. die Verwendung qualifizierter elektronischer Signaturen zu begünstigen;
- c. die internationale Anerkennung der Anbieterinnen von Zertifizierungsdiensten und ihrer Leistungen zu ermöglichen.

Art. 2 Begriffe

In diesem Gesetz bedeuten:

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

AS 2004 5085

¹ SR 101

² BBl 2001 5679

- 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. *qualifizierte elektronische Signatur*: eine fortgeschrittene elektronische Signatur, die auf einer sicheren Signaturerstellungseinheit nach Artikel 6 Absätze 1 und 2 und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht;
- d. *Signatur Schlüssel*: einmalige Daten wie Codes oder private kryptografische Schlüssel, die von der Inhaberin oder vom Inhaber zur Erstellung einer elektronischen Signatur verwendet werden;
- e. *Signaturprüf Schlüssel*: Daten wie Codes oder öffentliche kryptografische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
- f. *qualifiziertes Zertifikat*: ein digitales Zertifikat, das die Anforderungen des Artikels 7 erfüllt;
- g. *Anbieterin von Zertifizierungsdiensten*: Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt;
- h. *Anerkennungsstelle*: Stelle, die nach dem Akkreditierungsrecht³ für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert ist.

2. Abschnitt:

Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Art. 3 Anerkennungs Voraussetzungen

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;

³ BG vom 6. Okt. 1995 über die technischen Handelshemmnisse, THG (SR 946.51) und die dazugehörigen Ausführungsvorschriften.

- d. Informatiksysteme und -produkte, insbesondere Signaturerstellungseinheiten verwenden, die verlässlich und vertrauenswürdig sind;
- e. über ausreichende Finanzmittel oder -garantien verfügen;
- f. die notwendigen Versicherungen zur Deckung allfälliger Haftungsansprüche aus Artikel 16 und der Kosten, welche aus den in Artikel 13 Absätze 2 und 3 vorgesehenen Massnahmen erwachsen könnten, abschliessen;
- g. die Einhaltung des anwendbaren Rechts, namentlich dieses Gesetzes und seiner Ausführungsvorschriften, 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;
- 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 Wird 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 und Verwendung von Signatur- und Signaturprüfsschlüsseln

Art. 6

¹ Der Bundesrat regelt die Generierung von Signatur- und Signaturprüfsschlüsseln, für die qualifizierte Zertifikate im Sinne dieses Gesetzes ausgestellt werden können. Er sorgt dabei für ein der technischen Entwicklung entsprechendes hohes Sicherheitsniveau.

² Die Signaturerstellungseinheiten müssen zumindest gewährleisten, dass die für die Erzeugung der Signatur verwendeten Signaturschlüssel:

- a. praktisch nur einmal auftreten können und ihre Geheimhaltung hinreichend gewährleistet ist;
- b. mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur bei Verwendung 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.

³ Bei der Gestaltung des Signaturprüfungsvorgangs ist darauf zu achten, dass folgende Anforderungen mit hinreichender Sicherheit gewährleistet sind:

- a. Die zur Überprüfung der Signatur verwendeten Daten entsprechen den Daten, die der Überprüferin oder dem Überprüfer angezeigt werden.
- b. Die Signatur wird zuverlässig überprüft und das Ergebnis dieser Überprüfung wird korrekt angezeigt.
- c. Die Überprüferin oder der Überprüfer kann bei Bedarf den Inhalt der unterzeichneten Daten zuverlässig feststellen.
- d. Die Echtheit und die Gültigkeit des zum Zeitpunkt der Überprüfung der Signatur verlangten Zertifikats werden zuverlässig überprüft und das Ergebnis der Überprüfung wird korrekt angezeigt.
- e. Die Identität der Inhaberin oder des Inhabers des Signaturschlüssels wird korrekt angezeigt.
- f. Die Verwendung eines Pseudonyms wird eindeutig angegeben.
- g. Die sicherheitsrelevanten Veränderungen können erkannt werden.

4. Abschnitt: Qualifizierte Zertifikate

Art. 7

¹ Ein qualifiziertes Zertifikat muss mindestens folgende Angaben enthalten:

- a. die Seriennummer;
- b. den Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt;
- c. den Namen oder das Pseudonym der natürlichen Person, die den Signaturprüf Schlüssel innehat; im Falle einer Verwechslungsmöglichkeit ist der Name mit einem unterscheidenden Zusatz zu versehen;
- d. den Signaturprüf Schlüssel;
- e. die Gültigkeitsdauer;
- f. den Namen, den Niederlassungsstaat und die qualifizierte elektronische Signatur der Anbieterin von Zertifizierungsdiensten, die das Zertifikat ausstellt;
- g. den Hinweis darauf, ob die Anbieterin von Zertifizierungsdiensten anerkannt ist oder nicht und bei allfälliger Anerkennung den Namen der Anerkennungsstelle.

² Ins Zertifikat aufzunehmen sind ferner:

- a. spezifische Attribute der Inhaberin oder des Inhabers des Signaturschlüssels, wie die Tatsache, dass sie oder er zur Vertretung einer bestimmten juristischen Person berechtigt ist;
- b. der Geltungsbereich des Zertifikats;
- c. der Wert der Transaktionen, für die das Zertifikat verwendet werden kann.

³ Der Bundesrat regelt das Format der Zertifikate.

5. Abschnitt: Pflichten anerkannter Anbieterinnen von Zertifizierungsdiensten

Art. 8 Ausstellung qualifizierter Zertifikate

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die einen Antrag auf Ausstellung eines qualifizierten Zertifikats stellen, verlangen, dass sie persönlich erscheinen und den Nachweis ihrer Identität erbringen. Im Falle von Artikel 7 Absatz 2 Buchstabe a ist die Einwilligung der vertretenen Person nachzuweisen; berufsbezogene oder sonstige Angaben zur Person sind durch die zuständige Stelle zu bestätigen.

² 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.

³ Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen sich ferner vergewissern, dass die Person, die ein qualifiziertes Zertifikat verlangt, im Besitz des entsprechenden Signaturschlüssels ist.

⁴ Die anerkannten Anbieterinnen von Zertifizierungsdiensten können ihre Aufgabe zur Identifikation einer Antragstellerin oder eines Antragstellers an Dritte delegieren (Registrierungsstellen). Sie haften für die korrekte Ausführung der Aufgabe durch die Registrierungsstelle.

Art. 9 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 qualifizierten Zertifikate auf die Folgen eines möglichen Missbrauchs des Signaturschlüssels und auf die nach den Umständen notwendigen Vorkehrungen zur Geheimhaltung des Signaturschlüssels aufmerksam machen.

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

Art. 10 Ungültigerklärung qualifizierter Zertifikate

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten erklären ein qualifiziertes 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;
- c. es keine Gewähr mehr bietet für die Zuordnung eines Signaturprüfchlüssels zu einer bestimmten Person.

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 qualifizierter Zertifikate unverzüglich über die erfolgte Ungültigerklärung.

Art. 11 Verzeichnisdienste für qualifizierte Zertifikate

¹ Jede anerkannte Anbieterin von Zertifizierungsdiensten stellt sicher, dass die Gültigkeit aller qualifizierten 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 qualifizierten Zertifikate dieser Anbieterin 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 qualifizierten Zertifikaten möglich bleiben muss.

Art. 12 Zeitstempel

Auf entsprechendes Begehren müssen die anerkannten Anbieterinnen von Zertifizierungsdiensten eine mit ihrer qualifizierten elektronischen Signatur versehene Bescheinigung abgeben, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorliegen.

Art. 13 Einstellung der Geschäftstätigkeit

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten melden der Akkreditierungsstelle die Aufgabe 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 qualifizierten 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. 14 Datenschutz

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten und die von ihnen beauftragten Registrierungsstellen dürfen nur diejenigen Personendaten bearbeiten, die zur Erfüllung ihrer Aufgaben notwendig 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. 15

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten werden nach den Regeln des Akkreditierungsrechts⁴ von den Anerkennungsstellen beaufsichtigt.

² Eine Anerkennungsstelle meldet der Akkreditierungsstelle unverzüglich den Entzug der Anerkennung einer Anbieterin von Zertifizierungsdiensten. Artikel 13 Absatz 2 findet Anwendung.

7. Abschnitt: Haftung

Art. 16 Haftung der Anbieterin von Zertifizierungsdiensten

¹ Die Anbieterin von Zertifizierungsdiensten haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anbieterin den Pflichten aus diesem Gesetz und den entsprechenden Ausführungsvorschriften nicht nachgekommen ist.

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

³ Sie kann ihre Haftung aus diesem Gesetz weder für sich noch für Hilfspersonen wegbedingen. Sie haftet jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 7 Abs. 2) ergeben.

Art. 17 Haftung der Anerkennungsstelle

Die Anerkennungsstelle nach Artikel 2 Buchstabe h haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualifiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anerkennungsstelle ihren Pflichten aus diesem Gesetz und den Ausführungsvorschriften nicht nachgekommen ist. Artikel 16 Absätze 2 und 3 gilt sinngemäss.

Art. 18 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.

⁴ BG vom 6. Okt. 1995 über die technischen Handelshemmnisse, THG (SR 946.51) und die dazugehörigen Ausführungsvorschriften.

8. Abschnitt: Internationale Abkommen

Art. 19

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

- a. die Anerkennung elektronischer Signaturen und 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 Vorschriften über elektronische Signaturen 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 Durchführung internationaler Abkommen über Gegenstände nach Absatz 1 erlässt der Bundesrat die erforderlichen Vorschriften.

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

9. Abschnitt: Schlussbestimmungen

Art. 20 Vollzug

¹ Der Bundesrat erlässt die Ausführungsvorschriften. 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 beauftragen, qualifizierte Zertifikate auch für den Privatrechtsverkehr auszustellen oder sich an einer privaten Anbieterin von Zertifizierungsdiensten zu beteiligen.

Art. 21 Änderung bisherigen Rechts

Die Änderung bisherigen Rechts wird im Anhang geregelt.

Art. 22⁵**Art. 23** Referendum und Inkrafttreten

¹ Dieses Gesetz untersteht dem fakultativen Referendum.

² Der Bundesrat bestimmt das Inkrafttreten.

Datum des Inkrafttretens: 1. Januar 2005⁶

⁵ Aufgehoben durch Ziff. II 55 des BG vom 20. März 2008 zur formellen Bereinigung des Bundesrechts, mit Wirkung seit 1. Aug. 2008 (AS **2008** 3437 3452; BBl **2007** 6121).

⁶ BRB vom 3. Dez. 2004 (AS **2004** 5094)

Anhang
(Art. 21)

Änderung bisherigen Rechts

Die nachstehenden Bundesgesetze werden wie folgt geändert:

...⁷

⁷ Die Änderungen können unter AS **2004** 5085 konsultiert werden

