



Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES)

vom 23. November 2016

Der Schweizerische Bundesrat,

gestützt auf die Artikel 4, 6 Absatz 1, 7 Absatz 4, 9 Absatz 4, 10 Absatz 3, 12 Absatz 4, 14 Absatz 2 und 21 des Bundesgesetzes vom 18. März 2016¹ über die elektronische Signatur (ZertES),

gestützt auf Artikel 59a Absatz 3 des Obligationenrechts²,

verordnet:

Art. 1 Anerkennungsstellen

¹ Die Schweizerische Akkreditierungsstelle (SAS) des Staatssekretariats für Wirtschaft akkreditiert gemäss den Bestimmungen der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996³ die Stellen, die die Anbieterinnen von Zertifizierungsdiensten anerkennen.

² Besteht keine akkreditierte Anerkennungsstelle, so anerkennt das Bundesamt für Kommunikation (BAKOM) die Anbieterinnen von Zertifizierungsdiensten (Anbieterinnen).

Art. 2 Versicherung

¹ Eine Anbieterin, die anerkannt werden will, muss zur Deckung ihrer Haftung eine Versicherung von mindestens 2 Millionen Franken pro Versicherungsfall und 8 Millionen Franken pro Versicherungsjahr abschliessen.

² Sie kann anstelle einer Versicherung eine gleichwertige Garantie vorlegen.

SR 943.032

¹ SR 943.03

² SR 220

³ SR 946.512

Art. 3 Generierung, Speicherung und Verwendung kryptografischer Schlüssel

¹ Die Länge der Schlüssel und der verwendete Algorithmus müssen während der Gültigkeitsdauer des geregelten Zertifikats kryptografischen Angriffen standhalten können.

² Das BAKOM regelt die Einzelheiten in den technischen und administrativen Vorschriften und legt die Anforderungen fest, die für die Systeme zur Generierung, Speicherung und Verwendung privater kryptografischer Schlüssel gelten.

Art. 4 Geregelte Zertifikate

¹ Das BAKOM regelt das Format der geregelten Zertifikate für die folgenden Anwendungen:

- a. die elektronische Signatur einer natürlichen Person oder das elektronische Siegel einer UID-Einheit im Sinne von Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010⁴ über die Unternehmens-Identifikationsnummer (UIDG);
- b. die elektronische Identifikation einer solchen Person oder Einheit;
- c. die Verschlüsselung elektronischer Daten.

² Geregelte Zertifikate mit dem Hinweis, dass deren Inhaberin oder deren Inhaber sich selber oder die UID-Einheit, die sie oder er vertritt, durch ihre oder seine elektronische Signatur verpflichten kann, dürfen nur auf natürliche Personen ausgestellt werden.

Art. 5 Ausstellung geregelter Zertifikate auf natürliche Personen

¹ Die anerkannten Anbieterinnen müssen von den Personen, die ein geregeltes Zertifikat anfordern, verlangen, dass sie einen Pass, eine Schweizer Identitätskarte oder eine für die Einreise in die Schweiz anerkannte Identitätskarte persönlich vorweisen.

² Sind spezifische Attribute (Art. 7 Abs. 3 Bst. a ZertES), Vertretungsbefugnisse oder die vertretene UID-Einheit (Art. 7 Abs. 3 Bst. b ZertES) im Handelsregister eingetragen, so müssen die anerkannten Anbieterinnen einen aktuellen beglaubigten Handelsregisterauszug verlangen. Die im Auszug aufgeführten spezifischen Attribute und Vertretungsbefugnisse bedürfen weder einer Bestätigung durch die zuständige Stelle noch der Zustimmung der vertretenen UID-Einheit im Sinne von Artikel 9 Absätze 2 und 3 ZertES.

³ Die anerkannten Anbieterinnen müssen sicherstellen, dass die Einträge im Zertifikat dem Handelsregister nicht widersprechen. Insbesondere dürfen sie für eine Person, die laut Handelsregister zur Vertretung einer Rechtseinheit befugt ist oder in ihr eine Funktion hat, in Bezug auf die betreffende Rechtseinheit nur dieselben Vertretungsbefugnisse oder dieselbe Funktion in das Zertifikat aufnehmen.

⁴ SR 431.03

⁴ Ist die vertretene UID-Einheit im Handelsregister eingetragen, muss die Zustimmung zur Aufnahme von nicht im Handelsregister eingetragenen Vertretungsbefugnissen in das Zertifikat von einer Person, die laut Handelsregister zur Vertretung der UID-Einheit befugt ist, unterzeichnet werden.

⁵ Die anerkannten Anbieterinnen überprüfen ausserdem die Daten zu den Kernmerkmalen der vertretenen UID-Einheiten anhand des UID-Registers (Art. 11 Abs. 1 UIDG⁵). Hat die UID-Einheit der Veröffentlichung ihrer Daten zu den Kernmerkmalen nicht zugestimmt (Art. 11 Abs. 3 UIDG), müssen sie einen aktuellen beglaubigten Auszug aus dem UID-Register verlangen.

⁶ Die Absätze 1–5 gelten auch für die Ausstellung eines geregelten Zertifikats auf eine natürliche Person, die ein Pseudonym verwendet.

Art. 6 Ausstellung geregelter Zertifikate auf UID-Einheiten,
die keine natürlichen Personen sind

¹ Die Identität einer Person, die ein geregeltes Zertifikat für eine UID-Einheit beantragt, die keine natürliche Person ist, muss nach Artikel 5 Absatz 1 überprüft werden. Die Vertretungsbefugnisse dieser Person müssen mit einer schriftlichen Vollmacht begründet werden, sofern sie nicht im Handelsregister eingetragen sind.

² Die anerkannten Anbieterinnen müssen die Daten zu den Kernmerkmalen der UID-Einheiten anhand des UID-Registers überprüfen (Art. 11 Abs. 1 UIDG⁶). Hat die UID-Einheit der Veröffentlichung ihrer Daten zu den Kernmerkmalen nicht zugestimmt (Art. 11 Abs. 3 UIDG), müssen sie einen aktuellen beglaubigten Auszug aus dem UID-Register verlangen.

³ Ist die UID-Einheit im Handelsregister eingetragen, muss ein aktueller beglaubigter Auszug verlangt werden.

Art. 7 Befreiung von der Pflicht des persönlichen Erscheinens

¹ Die Identität einer Person, die ein geregeltes Zertifikat beantragt, kann auf Distanz festgestellt werden, sofern eine Konformitätsbewertungsstelle bestätigt hat, dass das verwendete Verfahren zur Personenidentifikation eine gleichwertige Sicherheit zum persönlichen Erscheinen bietet.

² Die anerkannten Anbieterinnen können geregelte Zertifikate im Rahmen eines Verfahrens zur Personenidentifikation mittels audiovisueller Kommunikation in Echtzeit ausstellen, wenn das Verfahren den Anforderungen des Geldwäschereigesetzes vom 10. Oktober 1997⁷ entspricht. Die so ausgestellten Zertifikate dürfen nur im Rahmen der Beziehungen zwischen deren Inhaberinnen und Inhabern und den Finanzintermediären, die ihre Identität überprüft haben, verwendet werden.

³ Die anerkannten Anbieterinnen können einen mit einer qualifizierten elektronischen Signatur versehenen Antrag entgegennehmen, der die Ausstellung eines geregelten Zertifikats an die folgende Einheit oder Person betrifft:

⁵ SR 431.03

⁶ SR 431.03

⁷ SR 955.0

- a. an eine UID-Einheit, die keine natürliche Person ist, sofern die Vertretungsbefugnisse der antragstellenden Person in einem öffentlichen Register eingetragen sind;
- b. an eine natürliche Person ohne spezifische Attribute und Vertretungsbefugnisse, sofern deren Identität bereits von der Anbieterin nach Artikel 5 oder nach den Absätzen 1 und 2 dieses Artikels festgestellt worden ist.

Art. 8 Kopieren der Schlüssel und Aufbewahren von Doppeln

Die anerkannten Anbieterinnen dürfen die privaten kryptografischen Schlüssel ihrer Kundinnen und Kunden kopieren und die Doppel aufbewahren, ausser wenn diese für die elektronische Signatur verwendet werden und in Signaturerstellungseinheiten gespeichert sind, die sich im Besitz der Kundinnen und Kunden befinden.

Art. 9 Ungültigerklärung geregelter Zertifikate

¹ Die anerkannten Anbieterinnen informieren ihre Kundinnen und Kunden darüber, wie letztere die Ungültigerklärung von geregelten Zertifikaten verlangen können. Sie müssen in der Lage sein, die Anträge zur Ungültigerklärung jederzeit entgegenzunehmen.

² Sie müssen Dritten bis zum Ablauf der Gültigkeit eines geregelten Zertifikats Online-Zugang zu den Informationen zur Ungültigerklärung desselben gewähren. Diese Informationen umfassen die Seriennummer des Zertifikats, den Hinweis auf die Ungültigerklärung sowie das Datum und die Uhrzeit der Ungültigerklärung. Sie müssen durch das geregelte elektronische Siegel der anerkannten Anbieterin authentifiziert werden.

³ Die anerkannten Anbieterinnen müssen die Informationen zur Überprüfung von nicht mehr gültigen geregelten Zertifikaten während elf Jahren ab Ablauf der Zertifikate angeben können.

Art. 10 Qualifizierte elektronische Zeitstempel

Das BAKOM legt die Anforderungen fest, die anerkannte Anbieterinnen erfüllen müssen, um qualifizierte elektronische Zeitstempel auszugeben.

Art. 11 Tätigkeitsjournal

¹ Die anerkannten Anbieterinnen bewahren die Eintragungen betreffend ihre Tätigkeiten sowie die dazugehörenden Belege während elf Jahren auf.

² Für die Tätigkeiten im Zusammenhang mit den Zertifikaten beginnt die Frist mit dem Ablauf der Zertifikate.

³ Für die in Anwendung von Artikel 7 Absatz 3 Buchstabe b ausgestellten Zertifikate müssen die Eintragungen und die Belege zur Identifizierung ihrer Inhaberinnen oder Inhaber gemäss den Artikeln 5 und 7 Absätze 1 und 2 so lange aufbewahrt werden, bis die Elfjahresfrist für das letzte der so ausgestellten Zertifikate abgelaufen ist.

Art. 12 Einstellung der Geschäftstätigkeit

¹ Die anerkannten Anbieterinnen melden der SAS und der Anerkennungsstelle unverzüglich, mindestens aber 30 Tage im Voraus, die Aufgabe ihrer Geschäftstätigkeit.

² Gibt es keine andere anerkannte Anbieterin, der die SAS die Aufgaben nach Artikel 14 Absatz 2 ZertES übertragen kann, so übernimmt das BAKOM folgende Aufgaben:

- a. Es bearbeitet die Anträge auf Ungültigerklärung der geregelten Zertifikate weiter.
- b. Es stellt sicher, dass Dritte die Informationen zur Ungültigerklärung der geregelten Zertifikate bis zu deren Ablauf elektronisch abrufen können.
- c. Es führt das Tätigkeitsjournal nach und bewahrt dieses sowie die dazugehörenden Belege auf.

³ Es kann die noch gültigen Zertifikate von sich aus für ungültig erklären.

Art. 13 Sicherheitsvorkehrungen

¹ Die Inhaberin oder der Inhaber eines geregelten Zertifikats muss den ausschliesslichen Zugang zum kryptografischen Schlüssel, der zur Generierung elektronischer Signaturen oder Siegel eingesetzt wird, behalten. Soweit zumutbar, muss sie oder er die Signatur- oder Siegelerstellungseinheit auf sich tragen oder wegschliessen.

² Bei Verlust oder Diebstahl der Signatur- oder Siegelerstellungseinheit muss die Inhaberin oder der Inhaber eines geregelten Zertifikats so rasch wie möglich dessen Ungültigerklärung beantragen. Das Gleiche gilt, wenn die Inhaberin oder der Inhaber weiss oder den begründeten Verdacht hat, dass eine Drittperson Zugang zum kryptografischen Schlüssel, der zur Generierung elektronischer Signaturen oder Siegel eingesetzt wird, haben konnte.

³ Die Daten zur Aktivierung der Signatur- oder Siegelerstellungseinheit dürfen sich nicht auf Daten zur Person oder zur UID-Einheit, die Inhaberin eines geregelten Zertifikats ist, beziehen.

⁴ Aufzeichnungen der Aktivierungsdaten sind sicher und getrennt von der Signatur- oder Siegelerstellungseinheit aufzubewahren.

⁵ Die Inhaberin oder der Inhaber eines geregelten Zertifikats muss die Aktivierungsdaten der Signatur- oder Siegelerstellungseinheit ändern, wenn sie oder er weiss oder den begründeten Verdacht hat, dass eine Drittperson Kenntnis davon erlangt hat. Wenn sie oder er die Aktivierungsdaten nicht selbst ändern kann, muss sie oder er so rasch wie möglich die Ungültigerklärung des Zertifikates beantragen.

Art. 14 Handelsregister

¹ Was die Aufbewahrung der Belege betrifft, die zur Ausstellung eines geregelten Zertifikats für Personen mit im Handelsregister eingetragenen spezifischen Attributen oder Vertretungsbefugnissen vorgelegt werden müssen, so bleiben die Artikel 8

Absatz 5, 9 Absatz 4 und 166 der Handelsregisterverordnung vom 17. Oktober 2007⁸ vorbehalten.

² Der Handelsregistereintrag ist für den Beweis der spezifischen Attribute und Vertretungsbefugnisse der Inhaberinnen oder Inhaber geregelter Zertifikate allein massgebend.

Art. 15 Vollzug

Das BAKOM erlässt die notwendigen technischen und administrativen Vorschriften. Es berücksichtigt dabei das entsprechende internationale Recht und kann internationale technische Normen für anwendbar erklären.

Art. 16 Aufhebung und Änderung anderer Erlasse

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

Art. 17 Übergangsbestimmungen

¹ Vor dem 1. Januar 2017 ausgestellte qualifizierte Zertifikate bleiben bis zu ihrem Ablauf, jedoch längstens bis am 31. Dezember 2019 gültig.

² Die nach altem Recht anerkannten Anbieterinnen können geregelte Zertifikate im Sinne des neuen Rechts ausstellen, bis sie nach dem neuen Recht anerkannt worden sind oder ihnen die Anerkennung entzogen worden ist, jedoch längstens bis am 31. Dezember 2018. Bis zur Erlangung der neuen Anerkennung sind die von ihnen ausgestellten geregelten Zertifikate längstens bis zum 31. Dezember 2019 gültig.

Art. 18 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2017 in Kraft.

23. November 2016

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Johann N. Schneider-Ammann

Der Bundeskanzler: Walter Thurnherr

Anhang
(Art. 16)

Aufhebung und Änderung anderer Erlasse

I

Die Verordnung vom 3. Dezember 2004⁹ über die elektronische Signatur wird aufgehoben.

II

Die nachstehenden Verordnungen werden wie folgt geändert:

1. Publikationsverordnung vom 7. Oktober 2015¹⁰

Anhang Ziff. 2

2 Elektronische Signatur

- 2.1 Die elektronische Signatur gemäss Artikel 30 ist ein geregeltes elektronisches Siegel nach Artikel 2 Buchstabe d des Bundesgesetzes vom 18. März 2016¹¹ über die elektronische Signatur (ZertES).
- 2.2 Die Gültigkeit des Zertifikats muss beim Anbringen des Siegels geprüft werden.
- 2.3 Dem Siegel muss ein qualifizierter elektronischer Zeitstempel nach Artikel 2 Buchstabe j ZertES beigefügt werden.

2. Verordnung vom 18. Juni 2010¹² über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens

Ingress

gestützt auf die Artikel 11b Absatz 2, 21a Absatz 4 und 34 Absatz 1^{bis} des Bundesgesetzes vom 20. Dezember 1968¹³ über das Verwaltungsverfahren (VwVG),

⁹ AS 2004 5101, 2011 3457

¹⁰ SR 170.512.1

¹¹ SR 943.03

¹² SR 172.021.2

¹³ SR 172.021

Art. 4 Abs. 2 Bst. f

² Das Verzeichnis führt für jede Behörde auf:

- f. die Adresse der Zertifikate, die die öffentlichen kryptografischen Schlüssel enthalten, die für die Verschlüsselung von Eingaben an die Behörde und für die Überprüfung der elektronischen Signatur der Behörde zu verwenden sind;

Art. 5a Wahrung einer Frist

¹ Für die Wahrung einer Frist ist der Zeitpunkt massgebend, in dem die von den Verfahrensbeteiligten verwendete Zustellplattform die Quittung ausstellt, dass sie die Eingabe zuhanden der Behörde erhalten hat (Abgabequittung).

² Das Eidgenössische Justiz- und Polizeidepartement bestimmt, wie dieser Zeitpunkt auf der Abgabequittung festgehalten wird.

Art. 6 Signatur

¹ Eine qualifizierte elektronische Signatur (Art. 21a Abs. 2 VwVG) ist nicht erforderlich, wenn die Identifizierung der Absenderin oder des Absenders und die Integrität der Übermittlung in anderer geeigneter Weise sichergestellt sind. Ausgenommen bleiben die Fälle, in denen das Bundesrecht vorschreibt, dass ein bestimmtes Dokument unterschrieben wird.

² Fehlt eine vorgeschriebene elektronische Signatur, so kann die Behörde der Partei eine Frist zur Korrektur einräumen. Die Partei kann die Eingabe zusammen mit einer qualifizierten elektronischen Signatur wiederholen oder nach den Regeln von Artikel 21 VwVG mit handschriftlicher Unterschrift einreichen.

Art. 7 Zertifikat

Ist das qualifizierte Zertifikat mit dem öffentlichen kryptografischen Schlüssel weder auf der von der Behörde verwendeten Zustellplattform zugänglich noch im Verzeichnis der anerkannten Anbieterin von Zertifizierungsdiensten (Art. 12 Abs. 2 des Bundesgesetzes vom 18. März 2016¹⁴ über die elektronische Signatur [ZertES]) aufgeführt, so muss es der Sendung beigelegt werden.

Art. 9 Abs. 4 und 5

⁴ Die Verfügungen werden mit einer qualifizierten elektronischen Signatur versehen (Art. 2 Bst. e ZertES¹⁵).

⁵ Mit einem geregelten elektronischen Siegel (Art. 2 Bst. d ZertES) dürfen versehen werden:

¹⁴ SR 943.03

¹⁵ SR 943.03

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

Art. 15a Übergangsbestimmung zur Änderung vom 23. November 2016

Für Massenverfügungen und E-Rechnungen mit Verfügungscharakter (Art. 9 Abs. 5) genügt bis 31. Dezember 2018 das Anbringen einer fortgeschrittenen elektronischen Signatur (Art. 2 Bst. b ZertES¹⁶), die auf einem Zertifikat einer anerkannten Anbieterin basiert.

3. Grundbuchverordnung vom 23. September 2011¹⁷

Art. 40 Abs. 1 Bst. b

¹ Elektronische Eingaben an die Grundbuchämter können über die Zustellplattformen nach den Artikeln 2 und 4 der Verordnung vom 18. Juni 2010¹⁸ über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren oder über Internetseiten des Bundes oder der Kantone erfolgen, sofern diese:

- b. eine mit einem geregelten elektronischen Siegel und einem elektronischen Zeitstempel nach Artikel 2 Buchstaben d und i des Bundesgesetzes vom 18. März 2016¹⁹ über die elektronische Signatur (ZertES) versehene Quittung über die Eingabe ausstellen.

Art. 44 Abs. 1 und 2 Einleitungssatz

¹ Zustellungen des Grundbuchamts müssen mit einer qualifizierten elektronischen Signatur mit qualifiziertem elektronischem Zeitstempel nach Artikel 2 Buchstaben e und j ZertES²⁰ unterzeichnet sein.

² Die Zertifikate müssen folgende Attribute enthalten:

¹⁶ SR 943.03
¹⁷ SR 211.432.1
¹⁸ SR 272.1
¹⁹ SR 943.03
²⁰ SR 943.03

4. Handelsregisterverordnung vom 17. Oktober 2007²¹

Art. 12a Abs. 3

³ Die elektronischen Kopien müssen mit einer qualifizierten elektronischen Signatur mit qualifiziertem elektronischem Zeitstempel nach Artikel 2 Buchstaben e und j des Bundesgesetzes vom 18. März 2016²² über die elektronische Signatur (ZertES) unterzeichnet sein.

Art. 12c Abs. 1 Bst. b

¹ Elektronische Eingaben an die Handelsregisterämter können neben den Zustellplattformen gemäss den Artikeln 2 und 4 der Verordnung vom 18. Juni 2010²³ über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren auch über entsprechende Internetseiten des Bundes oder der Kantone erfolgen, sofern diese:

- b. eine mit einem geregelten elektronischen Siegel und einem elektronischen Zeitstempel nach Artikel 2 Buchstaben d und i ZertES²⁴ versehene Quittung über die Eingabe ausstellen.

Art. 12d Abs. 1 und 2 Einleitungssatz

¹ Qualifizierte Zertifikate mit einem Pseudonym dürfen weder bei Eingaben an noch bei Zustellungen durch die Handelsregisterämter verwendet werden.

² Die für Beglaubigungen und für den elektronischen Geschäftsverkehr von den Handelsregisterämtern verwendeten qualifizierten Zertifikate müssen folgende Elemente enthalten:

Art. 18 Abs. 4

⁴ Elektronische Anmeldungen müssen mit einer qualifizierten elektronischen Signatur mit qualifiziertem elektronischem Zeitstempel nach Artikel 2 Buchstaben e und j ZertES²⁵ unterzeichnet sein. Unter Vorbehalt von Artikel 21 müssen die eigenhändigen Unterschriften der Personen, welche die Anmeldung unterzeichnen, nicht hinterlegt werden.

Art. 20 Abs. 2

² Die Belege müssen rechtskonform unterzeichnet sein. Belege in elektronischer Form müssen mit einer qualifizierten elektronischen Signatur mit qualifiziertem elektronischem Zeitstempel nach Artikel 2 Buchstaben e und j ZertES²⁶ unterzeichnet sein.

²¹ SR 221.411

²² SR 943.03

²³ SR 272.1

²⁴ SR 943.03

²⁵ SR 943.03

²⁶ SR 943.03

Art. 21 Abs. 3

³ Um die elektronisch eingeleseene Unterschrift selbst zu bestätigen, versteht die zeichnungsberechtigte Person diese mit einer Erklärung, dass sie diese als ihre eigene anerkennt, und signiert sie mit einer qualifizierten elektronischen Signatur mit qualifiziertem elektronischem Zeitstempel nach Artikel 2 Buchstaben e und j ZertES²⁷.

5. Verordnung vom 15. Februar 2006²⁸ über das Schweizerische Handelsamtsblatt

Art. 8 Abs. 2

² Die SHAB-Daten werden vom Herausgeber mit einer elektronischen Signatur oder einem elektronischen Siegel nach Artikel 2 Buchstabe c, d oder e des Bundesgesetzes vom 18. März 2016²⁹ über die elektronische Signatur (ZertES) versehen.

Art. 13 Abs. 2 Einleitungssatz und Bst. a

² Für die Verwertung von Daten, die nicht mit einer elektronischen Signatur oder einem elektronischen Siegel nach Artikel 2 Buchstabe c, d oder e ZertES³⁰ versehen sind, gelten zusätzlich folgende Auflagen:

- a. Die Daten sind mit folgendem Hinweis zu versehen: «Dies ist keine amtliche Veröffentlichung. Massgebend sind die vom SECO mit einer elektronischen Signatur oder einem elektronischen Siegel versehenen SHAB-Daten.»

6. Verordnung vom 18. Juni 2010³¹ über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren

Ingress

gestützt auf die Artikel 130 Absatz 2, 139 Absatz 2 und 400 Absatz 1 der Zivilprozessordnung (ZPO)³²,
auf die Artikel 15 Absatz 2, 33a Absätze 2 und 4 sowie 34 Absatz 2 des Bundesgesetzes vom 11. April 1889³³ über Schuldbetreibung und Konkurs (SchKG) und auf die Artikel 86 Absatz 2, 110 Absatz 2 und 445 der Strafprozessordnung (StPO)³⁴,

- 27 SR 943.03
- 28 SR 221.415
- 29 SR 943.03
- 30 SR 943.03
- 31 SR 272.1
- 32 SR 272
- 33 SR 281.1
- 34 SR 312.0

Art. 2 Bst. a und b

Eine Plattform für die sichere Zustellung (Zustellplattform) wird anerkannt, wenn sie:

- a. für Signatur und Verschlüsselung kryptografische Schlüssel einsetzt, die auf Zertifikaten einer nach dem Bundesgesetz vom 18. März 2016³⁵ über die elektronische Signatur (ZertES) anerkannten Anbieterin von Zertifizierungsdiensten (anerkannte Anbieterin) basieren;
- b. unverzüglich eine Quittung ausstellt mit dem Zeitpunkt des Eingangs einer Eingabe auf der Zustellplattform oder der Übergabe durch die Plattform an die Adressatin oder den Adressaten; diese Quittung und der von einem synchronisierten Zeitstempeldienst bestätigte Zeitpunkt ist mit einem geregelten elektronischen Siegel (Art. 2 Bst. d ZertES) zu versehen;

*Art. 7**Aufgehoben**Art. 8a und 8b einfügen vor dem Gliederungstitel des 3. Abschnitts**Art. 8a* Nachreichung auf Papier

¹ Eine Behörde kann die Nachreichung von Eingaben und Beilagen auf Papier verlangen, wenn diese aufgrund von technischen Problemen:

- a. von der Behörde nicht geöffnet werden können; oder
- b. für die Behörde beim Anzeigen am Bildschirm oder in gedruckter Form nicht lesbar sind.

² Sie gewährt den betroffenen Verfahrensbeteiligten unter Angabe des Grundes eine angemessene Frist für die Nachreichung.

Art. 8b Wahrung einer Frist

¹ Für die Wahrung einer Frist ist der Zeitpunkt massgebend, in dem die von den Verfahrensbeteiligten verwendete Zustellplattform die Quittung ausstellt, dass sie die Eingabe zuhanden der Behörde erhalten hat (Abgabequittung).

² Das EJPD bestimmt, wie dieser Zeitpunkt auf der Abgabequittung festgehalten wird.

Art. 10 Abs. 3 und 4

³ Die Mitteilungen werden mit einer qualifizierten elektronischen Signatur versehen (Art. 2 Bst. e ZertES³⁶).

³⁵ SR 943.03

³⁶ SR 943.03

⁴ Elektronische Kopien von Mitteilungen können mit einem geregelten elektronischen Siegel (Art. 2 Bst. d ZertES) der Behörde versehen werden.

Art. 15a Übergangsbestimmung zur Änderung vom 23. November 2016

Für Quittungen nach Artikel 2 Buchstabe b genügt bis 31. Dezember 2018 das Anbringen einer fortgeschrittenen elektronischen Signatur (Art. 2 Bst. b ZertES³⁷), die auf einem Zertifikat einer anerkannten Anbieterin basiert.

7. Registerharmonisierungsverordnung vom 21. November 2007³⁸

Art. 17 Abs. 3 und 4

³ Das Bundesamt für Informatik und Telekommunikation erteilt für jede dieser Stellen sowie für jede weitere Benutzerin oder jeden weiteren Benutzer von Sedex ein Zertifikat:

- a. zur Überprüfung ihrer elektronischen Signatur;
- b. zu ihrer Authentifizierung;
- c. zur Verschlüsselung von für sie bestimmten elektronischen Daten.

⁴ *Aufgehoben*

8. Fortpflanzungsmedizinverordnung vom 4. Dezember 2000³⁹

Art. 16b Abs. 3

³ Das Formular muss mit einer qualifizierten elektronischen Signatur nach Artikel 2 Buchstabe e des Bundesgesetzes vom 18. März 2016⁴⁰ über die elektronische Signatur versehen sein.

9. Direktzahlungsverordnung vom 23. Oktober 2013⁴¹

Art. 98 Abs. 6 Bst. b

⁶ Der Kanton bestimmt:

- b. ob Gesuche, die elektronisch eingereicht werden, mit einer qualifizierten elektronischen Signatur nach Artikel 2 Buchstabe e des Bundesgesetzes vom 18. März 2016⁴² über die elektronische Signatur versehen werden können.

³⁷ SR 943.03

³⁸ SR 431.021

³⁹ SR 810.112.2

⁴⁰ SR 943.03

⁴¹ SR 910.13

⁴² SR 943.03

10. Einzelkulturbeitragsverordnung vom 23. Oktober 2013⁴³

Art. 7 Abs. 6 Bst. b

⁶ Der Kanton bestimmt:

- b. ob Gesuche, die elektronisch eingereicht werden, mit einer qualifizierten elektronischen Signatur nach Artikel 2 Buchstabe e des Bundesgesetzes vom 18. März 2016⁴⁴ über die elektronische Signatur versehen werden können.

11. Verordnung vom 23. September 2011⁴⁵ über die elektronische öffentliche Beurkundung

Ingress

gestützt auf Artikel 55a Absatz 4 des Schlusstitels des Zivilgesetzbuches⁴⁶ und die Artikel 7 Absatz 4 und 9 Absatz 4 des Bundesgesetzes vom 18. März 2016⁴⁷ über die elektronische Signatur (ZertES),

Art. 3 Abs. 1 Bst. d

¹ Zur Erstellung einer elektronischen öffentlichen Urkunde oder Beglaubigung geht die Urkundsperson wie folgt vor:

- d. Sie signiert das Dokument mit einer qualifizierten elektronischen Signatur mit qualifiziertem elektronischem Zeitstempel nach Artikel 2 Buchstaben e und j ZertES, zusammen mit dem Nachweis der Berechtigung zur Beurkundung.

Art. 12 Abst. 3 Bst. d

³ Ist das zu beglaubigende Dokument digital signiert, so überprüft die Urkundsperson die Signatur und dokumentiert auf dem Papierausdruck das Prüfungsergebnis hinsichtlich:

- d. Zeitpunkt der Signatur und Angabe, ob das Dokument mit einem qualifizierten elektronischen Zeitstempel nach Artikel 2 Buchstabe j ZertES versehen ist.

⁴³ SR 910.17

⁴⁴ SR 943.03

⁴⁵ SR 943.033

⁴⁶ SR 210

⁴⁷ SR 943.03