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

(Verordnung über die elektronische Signatur, VZertES)

vom 23. November 2016 (Stand am 1. Januar 2017)

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 2016[1] über die elektronische Signatur (ZertES),
gestützt auf Artikel 59*a* Absatz 3 des Obligationenrechts[2],

verordnet:

Art. 1 Anerkennungsstellen

[1] Die Schweizerische Akkreditierungsstelle (SAS) des Staatssekretariats für Wirtschaft akkreditiert gemäss den Bestimmungen der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[3] 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.

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.

AS **2016** 4667

1 SR **943.03**
2 SR **220**
3 SR **946.512**

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 2010[4] 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 zuständigen 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 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.

4 SR **431.03**

5 Die anerkannten Anbieterinnen überprüfen ausserdem die Daten zu den Kernmerkmalen der vertretenen UID-Einheiten anhand des UID-Registers (Art. 11 Abs. 1 UIDG[5]). Hat die UID-Einheit der Veröffentlichung ihrer Daten zu den Kernmerkmalen nicht zugstimmt (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 UIDG[6]). 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 1997[7] 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 Sicherheitsvorkehren

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 2007[8] 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.

8 SR **221.411**

Anhang
(Art. 16)

Aufhebung und Änderung anderer Erlasse

I

Die Verordnung vom 3. Dezember 2004[9] über die elektronische Signatur wird aufgehoben.

II

Die nachstehenden Verordnungen werden wie folgt geändert:

…[10]

9 [AS **2004** 5101, **2011** 3457]
10 Die Änd. können unter AS **2016** 4667 konsultiert werden.