

Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur

(Verordnung über die elektronische Signatur, VZertES)

vom ... [Entwurf vom 1. Juni 2004]

Der Schweizerische Bundesrat,

gestützt auf die Artikel 4 Absatz 1 und 2, 6 Absatz 1, 7 Absatz 3, 8 Absatz 2, 9 Absatz 3, 11 Absatz 4, 13 Absatz 2 und 20 des Bundesgesetzes vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES)¹;

verordnet:

1. Abschnitt: Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Art. 1 Anerkennung

¹ Die Schweizerische Akkreditierungsstelle (SAS) des Bundesamtes für Metrologie und Akkreditierung (metas) akkreditiert die Stellen, die für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten gemäss den Bestimmungen der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996 (AkkBV)² zuständig sind.

² Besteht keine akkreditierte Anerkennungsstelle, anerkennt die SAS die Anbieterinnen von Zertifizierungsdiensten.

Art. 2 Anerkennungsvoraussetzungen

¹ Die Versicherung zur Deckung der Haftung der Anbieterin von Zertifizierungsdiensten, die eine Anerkennung anstrebt, muss für einen Betrag von mindestens 2,5 Millionen Franken pro Versicherungsfall oder 10 Millionen Franken pro Versicherungsjahr abgeschlossen werden.

² Anstelle einer Versicherung kann die Anbieterin von Zertifizierungsdiensten eine gleichwertige Garantie vorlegen.

2. Abschnitt: Generierung und Verwendung von Signatur- und Signaturprüfchlüsseln

Artikel 3

¹ Signatur- und Signaturprüfchlüssel, für die qualifizierte Zertifikate ausgestellt werden können, müssen eine ausreichende Länge aufweisen und einen anerkannten Algorithmus umsetzen, um während der ganzen Lebensdauer des qualifizierten Zertifikats kryptografischen Angriffen standhalten zu können.

² Das Bundesamt für Kommunikation (das Bundesamt) regelt die Einzelheiten in den technischen und administrativen Vorschriften und legt die Anforderungen fest, die für die Signaturerstellungseinheiten gelten. Es kann zudem die Anforderungen für den Signaturprüfungsvorgang festlegen.

3. Abschnitt: Qualifizierte Zertifikate

Artikel 4

Das Bundesamt regelt das Format der qualifizierten Zertifikate.

4. Abschnitt: Pflichten der anerkannten Anbieterinnen

Art. 5 Ausstellung qualifizierter Zertifikate

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die ein qualifiziertes Zertifikat anfordern, den Nachweis ihrer Identität und ihrer Befugnisse durch persönliche Vorweisung der folgenden Dokumente verlangen:

- a. Identitätskarte oder Pass;
- b. bei Signaturschlüsselinhaberinnen und Signaturschlüsselinhabern mit spezifischen Attributen zudem den Nachweis für diese Attribute, wie Vollmacht oder Handelsregisterauszug.

² Beantragt eine vor weniger als sechs Jahren gemäss Absatz 1 identifizierte Person ein neues elektronisches Zertifikat, können die anerkannten Anbieterinnen von Zertifizierungsdiensten einen Antrag entgegennehmen, der mit einer elektronischen Signatur versehen ist, die anhand des Signaturschlüssels erzeugt wurde, der dem Signaturprüfchlüssel zugeordnet werden kann, dessen Zertifikat erneuert werden soll.

³ Die Identität einer Person, die ein Pseudonym verwendet, muss nach den Absätzen 1 und 2 festgestellt werden.

¹ SR 943.03

² SR 946.512

Art. 6 Aufbewahrung der Signaturschlüssel

Die anerkannten Anbieterinnen von Zertifizierungsdiensten dürfen keine Kopien der Signaturschlüssel ihrer Kundschaft aufbewahren.

Art. 7 Ungültigerklärung qualifizierter Zertifikate

¹ Die anerkannten Anbieterinnen müssen sich vergewissern, dass die Person, welche die Ungültigerklärung der qualifizierten Zertifikate verlangt, dazu berechtigt ist. Diese Anforderung gilt als erfüllt, wenn der Antrag mit der elektronischen Signatur versehen ist, die anhand des Signaturschlüssels erzeugt wurde, der dem Signaturprüfsschlüssel entspricht, dessen Zertifikat für ungültig erklärt werden soll.

² Die anerkannten Anbieterinnen sind verpflichtet, die Seriennummer des Zertifikats, den Hinweis auf die Ungültigerklärung sowie das Datum und die Uhrzeit der Ungültigerklärung aufzuzeichnen. Diese Informationen müssen durch die qualifizierte elektronische Signatur der anerkannten Anbieterin authentifiziert werden.

³ Die anerkannten Anbieterinnen sind verpflichtet, Dritten mindestens bis zum Ablauf der Gültigkeit des Zertifikats den Online-Zugang zu den in Absatz 2 verlangten Informationen zu gewähren.

Art. 8 Verzeichnisdienste für qualifizierte Zertifikate

¹ Das Bundesamt legt die Anforderungen fest, die für anerkannte Anbieterinnen gelten, wenn sie einen Verzeichnisdienst anbieten.

² Die anerkannten Anbieterinnen von Zertifizierungsdiensten sind verpflichtet, die Informationen betreffend die abgelaufenen oder für ungültig erklärten qualifizierten Zertifikate während elf Jahren ab Ablauf oder Ungültigerklärung der Zertifikate aufzubewahren.

Art. 9 Tätigkeitsjournal

Die anerkannten Anbieterinnen von Zertifizierungsdiensten bewahren die Eintragungen betreffend ihre Tätigkeiten sowie die dazugehörigen Belege elf Jahre lang auf.

Art. 10 Einstellung der Geschäftstätigkeit

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten melden der SAS die Aufgabe ihrer Geschäftstätigkeit 30 Tage im Voraus.

² Existiert keine andere anerkannte Anbieterin von Zertifizierungsdiensten, führt die Stelle, welche die ihre Geschäftstätigkeit einstellende Anbieterin anerkannt hat, die Liste der gültigen, abgelaufenen oder für ungültig erklärten qualifizierten Zertifikate und bewahrt das Tätigkeitsjournal sowie die dazugehörigen Belege auf.

5. Abschnitt: Haftung für Signaturschlüssel: Sicherheitsvorkehrungen**Art. 11** Signaturschlüssel

Die Inhaberin oder der Inhaber des Signaturschlüssels darf diesen keiner anderen Person anvertrauen. Sie oder er muss den Signaturschlüssel, soweit zumutbar, auf sich tragen oder diesen wegschliessen.

Art. 12 Passwort

¹ Passwörter, die Zugang zum Signaturschlüssel verschaffen, müssen eine Länge von mindestens vier Zeichen (Zahlen oder Buchstaben) aufweisen.

² Das Passwort darf sich nicht auf persönliche Daten der Inhaberin oder des Inhabers des Signaturschlüssels beziehen.

³ Zeichnet die Inhaberin oder der Inhaber das Passwort auf, so muss sie oder er auch diese Aufzeichnung unter Verschluss halten.

⁴ Auf einen Passwortschutz kann verzichtet werden, wenn geeignete biometrische Verfahren garantieren, dass der Signaturschlüssel nur von der Inhaberin oder vom Inhaber verwendet wird.

⁵ Der Signaturschlüssel und die Passwörter sind getrennt voneinander aufzubewahren.

Art. 13 Meldung bei Verlust

¹ Hat die Inhaberin oder der Inhaber den eigenen Signaturschlüssel verloren oder ist dieser abhanden gekommen, muss sie oder er innerhalb von 24 Stunden die Ungültigerklärung des eigenen Zertifikats veranlassen.

² Das Gleiche gilt für die Inhaberin oder den Inhaber des Signaturschlüssels, der weiss oder den begründeten Verdacht hat, dass ein Dritter Kenntnis des Passworts erlangt hat.

³ Die Frist verlängert sich, wenn eine Meldung anfänglich nicht möglich oder zumutbar ist.

6. Abschnitt: Schlussbestimmungen**Art. 14** Vollzug

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

Art. 15 Aufhebung bisherigen Rechts

Die Verordnung vom 12. April 2000 über Dienste der elektronischen Zertifizierung (ZertDV)³ wird aufgehoben.

Art. 16 Inkrafttreten

Diese Verordnung tritt am 1. Januar 2005 in Kraft.

