Verordnung über Dienste der elektronischen Zertifizierung

(Zertifizierungsdiensteverordnung, ZertDV)

vom 12. April 2000

Der Schweizerische Bundesrat,

gestützt auf die Artikel 28, 62 und 64 des Fernmeldegesetzes vom 30. April 1997[1] (FMG)
und auf die Artikel 10, 14 und 15 des Bundesgesetzes vom 6. Oktober 1995[2] über die technischen Handelshemmnisse (THG),

verordnet:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Zweck und Gegenstand

[1] Diese Verordnung legt im Sinne einer Versuchsregelung die Voraussetzungen für die freiwillige Anerkennung der Anbieterinnen von Zertifizierungsdiensten fest und regelt ihre Tätigkeiten im Zusammenhang mit der Ausstellung von elektronischen Zertifikaten.

[2] Sie hat zum Zweck, ein breites Angebot an sicheren Diensten im Zusammenhang mit der elektronischen Zertifizierung zu fördern, die Verwendung und die rechtliche Anerkennung der digitalen Signaturen zu begünstigen und die internationale Anerkennung der Anbieterinnen von Zertifizierungsdiensten und ihrer Dienste zu ermöglichen.

[3] Die privatrechtlichen Vorschriften über den Abschluss von Verträgen und die Vertretung juristischer Personen bleiben vorbehalten.

Art. 2 Begriffe

In dieser Verordnung bedeuten:

a. *Anbieterin von Zertifizierungsdiensten*: eine natürliche oder juristische Person oder eine Verwaltungseinheit des Bundes, der Kantone oder der Gemeinden, die Daten im Rahmen einer elektronischen Umgebung beglaubigt und zu diesem Zweck elektronische Zertifikate ausstellt;

b. *elektronisches Zertifikat*: Gesamtheit von elektronischen Daten, welche die Zuordnung eines öffentlichen Schlüssels zu einer natürlichen oder juristischen Person oder einer Verwaltungseinheit ermöglichen und durch die

SR **784.103**

1 SR **784.10**
2 SR **946.51**

digitale Signatur einer Anbieterin von Zertifizierungsdiensten authentifiziert werden;

c. *privater Schlüssel*: ein geheim gehaltener kryptografischer Schlüssel;

d. *öffentlicher Schlüssel*: ein kryptografischer Schlüssel, der einem privaten Schlüssel zugeordnet werden kann und allgemein zugänglich ist;

e. *kryptografischer Schlüssel*: ein Parameter, der mit einem mathematischen Algorithmus zur Umwandlung, Bestätigung, Authentifizierung, Verschlüsselung oder Entschlüsselung von Daten verwendet wird;

f. *digitale Signatur*: ein elektronischer Code, der elektronischen Daten beigefügt wird oder logisch mit ihnen verknüpft ist und mit Hilfe eines privaten Schlüssels verschlüsselt wird, und anhand dessen nach Entschlüsselung mit Hilfe des entsprechenden öffentlichen Schlüssels festgestellt werden kann, dass die Daten dem Inhaber des privaten Schlüssels zugeordnet werden können und seit ihrer Signatur nicht verändert worden sind;

g. *Anerkennungsstelle*: eine nach der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[3] akkreditierte Zertifizierungsstelle, die für die Prüfung und Anerkennung der Anbieterinnen von Zertifizierungsdiensten zuständig ist.

2. Kapitel: Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Art. 3 Anerkennung

1 Anerkannt werden können Anbieterinnen von Zertifizierungsdiensten, welche in der Lage sind, die elektronischen Zertifikate gemäss den Anforderungen dieser Verordnung auszustellen und zu verwalten.

2 Die für die Umsetzung der vorliegenden Verordnung akkreditierten Anerkennungsstellen sind für die Anerkennung der Anbieterinnen von Zertifizierungsdiensten zuständig.

3 Existiert keine Anerkennungsstelle, werden die Anbieterinnen von Zertifizierungsdiensten von der Schweizerischen Akkreditierungsstelle (SAS) des Eidgenössischen Amtes für Messwesen anerkannt.

Art. 4 Voraussetzungen für die Anerkennung

1 Um anerkannt zu werden, müssen die Anbieterinnen von Zertifizierungsdiensten folgende Voraussetzungen erfüllen:

a. im Handelsregister eingetragen oder Teil einer Verwaltungseinheit des Bundes, der Kantone oder Gemeinden sein;

3 SR **946.512**

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

c. zuverlässige Informatiksysteme und -produkte verwenden;

d. über ausreichende Finanzmittel und -garantien verfügen;

e. die notwendigen Versicherungen zur Deckung allfälliger Haftungsansprüche und der Kosten, welche aus den in Artikel 15 Absätze 2 und 3 vorgesehenen Massnahmen erwachsen könnten, abschliessen;

f. sich in ihren allgemeinen Geschäftsbedingungen verpflichten, dass sie für Schäden, die infolge eines fehlerhaften elektronischen Zertifikats oder wegen Missachtung von Publikationspflichten entstehen, auch gegenüber Dritten haften, sofern sie nicht nachweisen können, dass sie kein Verschulden trifft;

g. die Einhaltung des anwendbaren Rechts, namentlich dieser Verordnung und ihrer Ausführungsvorschriften, gewährleisten.

2 Die Voraussetzungen werden in den Ausführungsvorschriften näher festgelegt.

Art. 5 Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten

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

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

3 Jede anerkannte Anbieterin von Zertifizierungsdiensten veröffentlicht die Liste aller anderen anerkannten Anbieterinnen von Zertifizierungsdiensten sowie ihren öffentlichen Schlüssel. Sie authentifiziert die Liste, indem sie sie mit ihrer digitalen Signatur versieht. Die weiteren Einzelheiten zu Art und Umfang der Veröffentlichung sind in den Ausführungsvorschriften geregelt.

3. Kapitel: Grundlegende Anforderungen

1. Abschnitt: Generierung und Verwendung der kryptografischen Schlüssel

Art. 6

Die Fragen im Zusammenhang mit der Generierung der kryptografischen Schlüssel, für die elektronische Zertifikate im Sinne dieser Verordnung ausgestellt werden können, sowie mit der Erzeugung und Prüfung der digitalen Signatur sind in den Ausführungsvorschriften geregelt. Diese bezwecken die Gewährleistung eines der technischen Entwicklung entsprechenden hohen Sicherheitsniveaus.

2. Abschnitt: Elektronische Zertifikate

Art. 7

1 Jedes gestützt auf dieser Verordnung ausgestellte elektronische Zertifikat muss mindestens folgende Angaben enthalten:

a. seine Seriennummer;

b. den Hinweis, dass es in Anwendung dieser Verordnung ausgestellt wurde;

c. den Hinweis auf mögliche Nutzungsbeschränkungen;

d. den Namen des Inhabers des beglaubigten öffentlichen Schlüssels sowie den Hinweis, dass es sich um eine natürliche Person, eine juristische Person, eine Verwaltungseinheit oder gegebenenfalls um ein Pseudonym handelt;

e. den beglaubigten öffentlichen Schlüssel;

f. seine Gültigkeitsdauer;

g. den Namen und die digitale Signatur der Anbieterin von Zertifizierungsdiensten, die es ausstellt.

2 Das Format der Zertifikate ist in den Ausführungsvorschriften geregelt.

3. Abschnitt: Anbieterinnen von Zertifizierungsdiensten

Art. 8 Ausstellung der elektronischen Zertifikate

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die einen Antrag auf Ausstellung eines elektronisches Zertifikat stellen, den Nachweis ihrer Identität und ihrer Vertretungsmacht durch persönliche Vorweisung der folgenden Dokumente verlangen:

a. Identitätskarte oder Pass bei natürlichen Personen;

b. Vollmacht und Identitätskarte oder Pass bei Personen, die für Verwaltungseinheiten handeln;

c. Handelsregisterauszug und Identitätskarte oder Pass der Handlungsbevollmächtigten bei juristischen Personen.

2 Beantragt eine vor weniger als zehn Jahren gemäss Absatz 1 identifizierte Person oder Verwaltungseinheit ein neues elektronisches Zertifikat, können die anerkannten Anbieterinnen von Zertifizierungsdiensten einen Antrag entgegennehmen, welcher mit der anhand des privaten Schlüssels erzeugten digitalen Signatur versehen ist, der dem öffentlichen Schlüssel zugeordnet werden kann, dessen Zertifikat erneuert werden soll.

3 Auf Antrag führen sie im elektronischen Zertifikat anstelle des Namens des Inhabers des beglaubigten öffentlichen Schlüssels ein Pseudonym auf. Die Identität muss nach den Absätzen 1 und 2 festgestellt werden.

Art. 9 Informationspflicht

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

[2] Sie müssen ihre Kunden spätestens bei der Ausstellung der elektronischen Zertifikate auf die Folgen eines möglichen Missbrauchs oder Verlusts des privaten Schlüssels aufmerksam machen. Sie müssen ihnen geeignete Massnahmen zur Geheimhaltung des privaten Schlüssels vorschlagen.

Art. 10 Aufbewahrung der privaten Schlüssel

Die anerkannten Anbieterinnen von Zertifizierungsdiensten dürfen keine Kopien der privaten Schlüssel ihrer Kunden aufbewahren.

Art. 11 Ungültigerklärung der elektronischen Zertifikate

[1] Die anerkannten Anbieterinnen von Zertifizierungsdiensten erklären elektronische Zertifikate auf Antrag ihrer Inhaber unverzüglich für ungültig.

[2] Sie müssen sich versichern, dass die Person, welche die Ungültigerklärung verlangt, dazu berechtigt ist. Diese Anforderung gilt als erfüllt, wenn der Antrag mit der anhand des privaten Schlüssels erzeugten digitalen Signatur versehen ist, der dem öffentlichen Schlüssel zugeordnet werden kann, dessen Zertifikat für ungültig erklärt werden soll.

[3] Die anerkannten Anbieterinnen von Zertifizierungsdiensten sind verpflichtet, von ihnen ausgestellte elektronische Zertifikate unverzüglich für ungültig zu erklären, wenn sich herausstellt, dass diese unrechtmässig erlangt worden sind oder keine Gewähr mehr für die Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person oder Verwaltungseinheit bieten.

[4] Sie können die elektronischen Zertifikate vorübergehend für eine Dauer von maximal drei Tagen suspendieren. Nach Ablauf dieser Frist erklären sie die Zertifikate definitiv für ungültig oder erneut für gültig. Im ersten Fall wird die Ungültigerklärung im Zeitpunkt der Suspendierung des Zertifikats wirksam; im zweiten Fall hat die Suspendierung keine Wirkung auf die Gültigkeit des Zertifikats.

[5] Die anerkannten Anbieterinnen von Zertifizierungsdiensten informieren die Inhaber von elektronischen Zertifikaten unverzüglich über deren Ungültigerklärung oder Suspendierung.

Art. 12 Verzeichnis der elektronischen Zertifikate und Liste der für ungültig erklärten oder suspendierten Zertifikate

[1] Die anerkannten Anbieterinnen von Zertifizierungsdiensten führen ein Verzeichnis der von ihnen ausgestellten elektronischen Zertifikate, in das die Kunden ihre elektronischen Zertifikate eintragen lassen können.

2 Sie sind verpflichtet, eine Liste aller für ungültig erklärten oder suspendierten Zertifikate zu führen, auch wenn diese nicht im Verzeichnis eingetragen worden sind. Diese Liste enthält ausschliesslich die Seriennummer des elektronischen Zertifikats, den Hinweis auf die Ungültigerklärung oder Suspendierung sowie das Datum und die Uhrzeit der Ungültigerklärung oder Suspendierung. Sie wird durch die digitale Signatur der anerkannten Anbieterin von Zertifizierungsdiensten authentifiziert.

3 Die anerkannten Anbieterinnen von Zertifizierungsdiensten sind verpflichtet, Dritten den Online-Zugang zum Verzeichnis der elektronischen Zertifikate und zur Liste der für ungültig erklärten oder suspendierten Zertifikate jederzeit und ohne zusätzliche Kosten neben jenen für die Nutzung der öffentlichen Telekommunikationsmittel zu gewährleisten.

4 Die Modalitäten betreffend die Führung der Verzeichnisse der elektronischen Zertifikate und der Listen der für ungültig erklärten oder suspendierten Zertifikate sowie den Zugang zu den Verzeichnissen und den Listen sind in den Ausführungsvorschriften geregelt.

Art. 13 Aufbewahrung der elektronischen Zertifikate

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten sind verpflichtet, die abgelaufenen oder für ungültig erklärten elektronischen Zertifikate sowie die Listen der für ungültig erklärten Zertifikate aufzubewahren und die Einsicht in Zertifikate und die Listen während mindestens elf Jahren nach Ablauf oder Ungültigerklärung der Zertifikate zu gewährleisten.

2 Während der ersten sechs Jahre ist die entsprechende Einsicht jederzeit und ohne andere Kosten als diejenigen für die Nutzung der öffentlichen Telekommunikationsmitteln online zu gewähren.

Art. 14 Tätigkeitsjournal

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten vermerken ihre Aktivitäten im Zusammenhang mit der Ausstellung, der Ungültigerklärung und der Suspendierung der elektronischen Zertifikate in einem Tätigkeitsjournal.

2 Sie bewahren die Eintragungen in diesem Journal sowie die entsprechenden Belege während derselben Frist auf, wie sie das letzte gemäss Artikel 8 Absatz 2 erneuerte Zertifikat aufbewahren müssen.

Art. 15 Einstellung der Geschäftstätigkeit

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten melden der SAS die Aufgabe ihrer Geschäftstätigkeit 30 Tage im Voraus. Eine gegen sie gerichtete Konkursandrohung ist der SAS unverzüglich zu melden.

2 Bei freiwilliger Einstellung der Geschäftstätigkeit sind die anerkannten Anbieterinnen von Zertifizierungsdiensten verpflichtet, die von ihnen ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären. Die SAS beauftragt eine andere anerkannte Anbieterin von Zertifizierungsdiensten, die Liste der für ungültig

erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren.

3 Fällt eine anerkannte Anbieterin von Zertifizierungsdiensten in Konkurs, so beauftragt die SAS eine andere anerkannte Anbieterin von Zertifizierungsdiensten, die von jener ausgestellten, noch gültigen elektronischen Zertifikate für ungültig zu erklären, die Liste der für ungültig erklärten Zertifikate zu führen und die abgelaufenen oder für ungültig erklärten Zertifikate, das Tätigkeitsjournal sowie die entsprechenden Belege aufzubewahren.

Art. 16 Datenschutz

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten dürfen nur diejenigen Personendaten erheben und weiterbearbeiten, die zur Erfüllung ihrer Aufgaben notwendig sind.

2 Im Übrigen gilt die Datenschutzgesetzgebung.

4. Kapitel: Aufsicht über die anerkannten Anbieterinnen von Zertifizierungsdiensten

Art. 17

1 Die anerkannten Anbieterinnen von Zertifizierungsdiensten werden gemäss den Regeln des Akkreditierungsrechts von den Anerkennungsstellen beaufsichtigt.

2 Eine Anerkennungsstelle meldet den Entzug der Anerkennung einer Anbieterin von Zertifizierungsdiensten unverzüglich der SAS. Artikel 15 Absatz 3 findet Anwendung.

5. Kapitel: Anerkennung der ausländischen Anbieterinnen von Zertifizierungsdiensten

Art. 18

Die SAS stellt der Öffentlichkeit die Liste der ausländischen Anbieterinnen von Zertifizierungsdiensten zur Verfügung, die im Rahmen der vom Bundesrat gemäss Artikel 14 THG abgeschlossenen internationalen Abkommen anerkannt wurden.

6. Kapitel: Bestätigung der Konformität einer digitalen Signatur mit dieser Verordnung

Art. 19

1 Gegen Bezahlung einer Gebühr bestätigt die SAS auf Antrag schriftlich, dass die auf einem elektronischen Dokument vorhandene digitale Signatur mit Hilfe des privaten Schlüssels angebracht wurde, der einem öffentlichen Schlüssel zugeordnet werden kann, für den eine anerkannte Anbieterin von Zertifizierungsdiensten ein elektronisches Zertifikat ausgestellt hat, und dass dieses Zertifikat zu einem bestimmten Zeitpunkt gültig war.

2 Das Eidgenössische Justiz- und Polizeidepartement legt die Höhe der Gebühr fest.

3 Die Bestätigungen im Sinne von Absatz 1 können auch von anderen Stellen ausgestellt werden, sofern diese die erforderlichen Voraussetzungen erfüllen.

7. Kapitel: Schlussbestimmungen

Art. 20 Vollzug

Das Bundesamt für Kommunikation erlässt die in dieser Verordnung vorgesehenen Ausführungsvorschriften in Zusammenarbeit mit dem Informatikstrategieorgan Bund und der SAS. Es berücksichtigt dabei die internationalen Normen und Vorschriften in diesem Bereich.

Art. 21 Inkrafttreten und Geltungsdauer

1 Diese Verordnung tritt am 1. Mai 2000 in Kraft.

2 Sie gilt bis zum Inkrafttreten einer entsprechenden gesetzlichen Regelung, längstens aber bis zum 31. Dezember 2009.

12. April 2000

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Adolf Ogi

10942

Die Bundeskanzlerin: Annemarie Huber-Hotz