Entwurf der Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES)

Erläuterungen

Allgemeines

Das Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES; BBl 2003 8221) übernimmt im Wesentlichen die Bestimmungen der Verordnung vom 12. April 2000 über Dienste der elektronischen Zertifizierung (ZertDV; SR 784.103). Der vorliegende Entwurf für die neue Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES) behält im Allgemeinen die Bestimmungen bei, die nicht im Gesetz übernommen wurden, regelt die vom Gesetzgeber delegierten Bereiche und präzisiert bei Bedarf die gesetzlichen Bestimmungen. Die Struktur der Verordnung folgt weitgehend derjenigen des Gesetzes.

Anerkennung der Anbieterinnen von Zertifizierungsdiensten

Art. 1 Anerkennung

In Ausführung von Artikel 4 ZertES übernimmt diese Bestimmung das aktuelle System. Die SAS akkreditiert die Stellen, die befugt sind, die Anbieterinnen von Zertifizierungsdiensten (CSP) gemäss dem allgemeinen Akkreditierungssystem anzuerkennen. Wie bei der heutigen Regelung in der ZertDV (Art. 3 Abs. 3) ist es Aufgabe der SAS, die CSP anzuerkennen, wenn es keine akkreditierte Anerkennungsstelle gibt. Bei dieser Lösung können aber Kompetenzkonflikte innerhalb der SAS entstehen, da die SAS sowohl eine Akkreditierungs- als auch eine Anerkennungsfunktion ausübt. Aus diesem Grund wird in Erwägung gezogen, Art. 1 Abs. 2 zu ändern und eine andere Behörde – z.B. das BAKOM – mit der Anerkennungsfunktion zu betrauen.

Art. 2 Anerkennungsvoraussetzungen

Die CSP haften für den verursachten Schaden, wenn sie ihren gesetzlichen Pflichten nicht nachkommen (Art. 16 ZertES). Sie können zwar ihre Haftung nicht ausschliessen, haften aber höchstens für den Betrag des auf dem Zertifikat angegebenen Transaktionswerts (Art. 16 Abs. 3, in Verbindung mit Art. 7 Abs. 2 Bst. c ZertES). Das gleiche Zertifikat kann eine Vielzahl von Schäden verursachen, die kumuliert einen grossen Betrag ausmachen können. Daher sind ausreichende Finanzgarantien zur Deckung der Haftung der CSP unabdingbar.

Ergänzend zu den Bestimmungen des ZertES legt die Verordnung den Mindestbetrag fest, der von der Versicherung der CSP sowohl pro Fall als auch pro Versicherungsjahr gedeckt werden muss. Dies sollte dazu beitragen, dass ein Markt für Versicherungen im Bereich der elektronischen Zertifizierungen entstehen kann und gleichzeitig die Inhaberinnen und Inhaber wie auch die Nutzerinnen und Nutzer von elektronischen Zertifikaten genügend geschützt sind. Unter Versicherungsfall ist die Gesamtheit der Schäden zu verstehen, die aufgrund der Verletzung einer oder mehrer Pflichten durch die CSP entstanden sind. Ein Versicherungsfall kann daher mehrere Schadensfälle umfassen. Der ausschlaggebende Schadensfall ist derjenige, der im Rahmen einer Transaktion im Sinne von Artikel 7 Absatz 2 Buchstabe c ZertES erlitten wird.

Im Übrigen erlaubt die Verordnung der CSP, die eine Anerkennung anstrebt, eine gleichwertige Finanzgarantie vorzulegen, anstatt eine Versicherung abzuschliessen. Diese Garantie zur Deckung der Haftung der CSP muss mindestens die Beträge decken, die auch für die Versicherung vorgesehen sind. Es kann sich um eine Bankgarantie oder eine äquivalente andere Art von Finanzgarantie handeln.

Generierung und Verwendung von Signatur- und Signaturprüfschlüsseln

Artikel 3

Gestützt auf Art. 6 Abs. 1 ZertES regelt der Bundesrat die Generierung von Signatur- und Signaturprüfschlüsseln, für die qualifizierte Zertifikate ausgestellt werden können. Die vorliegende Bestimmung legt die entscheidenden Kriterien fest, namentlich die Länge der Schlüssel und den für ihre Generierung verwendeten Algorithmus. Das BAKOM wird beauftragt, die Einzelheiten unter Berücksichtigung der technischen Entwicklung zu regeln. In Anwendung von Artikel 20 Absatz 2 ZertES erhält es zudem den Auftrag, Artikel 6 Absatz 2 ZertES umzusetzen (Anforderungen betreffend die Signaturerstellungseinheiten). Weiter kann es bei Bedarf die in Artikel 6 Absatz 3 ZertES genannten Anforderungen betreffend den Signaturprüfvorgang präzisieren.

Qualifizierte Zertifikate

Artikel 4

Gemäss Artikel 7 Absatz 3 ZertES regelt der Bundesrat das Format der Zertifikate. Da es sich hierbei um eine rein technische Frage handelt, übertägt er diese Aufgabe gestützt auf Artikel 20 Absatz 2 ZertES dem BAKOM (Subdelegation).

Pflichten der anerkannten Anbieterinnen

Art. 5 Ausstellung qualifizierter Zertifikate

Gemäss Artikel 8 Absatz 2 ZertES bezeichnet der Bundesrat die Dokumente, mit denen die antragstellende Person ihre Identität und allfällige Attribute nachweisen kann. Er bestimmt zudem, unter welchen Voraussetzungen auf das persönliche Erscheinen der antragstellenden Person verzichtet werden kann. Der Verordnungsentwurf übernimmt im Wesentlichen die geltende Regelung. Da juristische Personen nicht mehr Inhaberinnen von qualifizierten Zertifikaten sein können, ist zu präzisieren, welche Art von Dokumenten die Inhaberinnen und Inhaber von Signaturschlüsseln mit besonderen Attributen vorlegen müssen, z. B. die Berechtigung, eine bestimmte juristische Person zu vertreten (vgl. Abs. 1 Bst. b).

Absatz 2 entspricht Artikel 8 Absatz 2 ZertDV, mit Ausnahme der Tatsache, dass die Frist betreffend den Verzicht auf das persönliche Erscheinen von zehn auf sechs Jahre reduziert wurde. Absatz 3 präzisiert wie bisher, dass die Identität einer Person, die im Zertifikat ein Pseudonym anstelle ihres Namens aufführen lässt, gemäss den Absätzen 1 und 2 festgestellt werden muss.

Art. 6 Aufbewahrung der Signaturschlüssel

Diese Bestimmung entspricht der geltenden Regelung (vgl. Art. 10 ZertDV). Sie entspricht einem anerkannten Sicherheitsbedürfnis.

Art. 7 Ungültigerklärung qualifizierter Zertifikate

Absatz 1 übernimmt Artikel 11 Absatz 2 ZertDV. Die Überprüfung der Gültigkeit der qualifizierten Zertifikate muss zudem durch einen Online-Zugang zu den Informationen betreffend die ungültig erklärten Zertifikate möglich sein, welche die CSP veröffentlichen müssen (Abs. 2 und 3).

Art. 8 Verzeichnisdienste für qualifizierte Zertifikate

Das Anbieten eines Verzeichnisdienstes für die qualifizierten Zertifikate ist nicht mehr vorgeschrieben (vgl. Art. 11 Abs. 2 ZertES). Wird eine solche Dienstleistung freiwillig angeboten, muss sie aber die vom BAKOM festgelegten Anforderungen erfüllen (Abs. 1).

Gemäss Artikel 11 Absatz 4 ZertES bestimmt der Bundesrat die Mindestdauer, während der die Überprüfung von nicht mehr gültigen Zertifikaten möglich bleiben muss. Die vorgeschlagene Regelung (Abs. 2) übernimmt die in Artikel 13 ZertDV festgelegte Frist von elf Jahren, die der allgemeinen Verjährungsfrist gemäss Artikel 127 des Obligationenrechts (OR) und der Frist für die Aufbewahrung der Geschäftsbücher gemäss Artikel 962 OR entspricht.

Art. 9 Tätigkeitsjournal

Gemäss Artikel 9 Absatz 3 ZertES legt der Bundesrat fest, wie lange das Journal und die dazugehörenden Dokumente aufbewahrt werden müssen. Auch hier drängt sich die Frist von elf Jahren entsprechend Artikel 8 Absatz 2 auf.

Art. 10 Einstellung der Geschäftstätigkeit

Absatz 1 präzisiert gegenüber dem Gesetz, dass die Meldung einer Aufgabe der Geschäftstätigkeit 30 Tage im Voraus stattfinden muss. Absatz 2 regelt in Anwendung von Art. 13 Abs. 2 ZertES den Fall, in dem es keine andere anerkannte CSP gibt, welche die Aufgaben der die Geschäftstätigkeit einstellenden Anbieterin übernehmen kann. Diese Aufgaben gehen an diejenige Stelle über, welche die aufgebende Anbieterin anerkannt hat.

Haftung für Signaturschlüssel: Sicherheitsvorkehrungen

Artikel 59*a* Absatz 3 OR beauftragt den Bundesrat, die Sicherheitsvorkehren zu umschreiben, welche die Inhaberin oder der Inhaber eines Signaturschlüssels einhalten muss, um nicht für den Missbrauch des eigenen Signaturschlüssels zu haften. Zu beachten ist dabei, dass sich dieses Haftungsrisiko nur im Umfeld der im ZertES beschriebenen (fortgeschrittenen) elektronischen Signatur verwirklichen kann. Dies bedeutet, dass die Signaturerstellungseinheit so beschaffen sein muss, dass die Inhaberin oder der Inhaber diese vor der missbräuchlichen Verwendung durch andere verlässlich schützen kann (Art. 6 Abs. 2 Bst. c ZertES). Nach heutigem Stand der Diskussion bedeutet dies, dass der Signaturschlüssel hardwaremässig abgelegt sein muss (Smartcard, Token) - Hardware, welche die Inhaberin oder der Inhaber mehr oder weniger leicht unter Verschluss halten kann.

Hinzuweisen ist ferner auf den Sinn von Artikel 59*a* Absatz 3 OR. Der Gesetzgeber hat sich für diese Lösung entschieden, damit die von der Inhaberin oder vom Inhaber des Signaturschlüssels verlangten Sicherheitsvorkehren in einem vernünftigen Rahmen bleiben. Wäre die Umschreibung der Sicherheitsvorkehrungen den Anbieterinnen von Zertifizierungsdiensten überlassen worden, hätte dieses Ziel kaum erreicht werden können. Dem Anliegen des Gesetzgebers ist bei der Redaktion der Verordnung Rechnung zu tragen.

Art. 11 Signaturschlüssel

Im einen Extremfall vertraut die Inhaberin oder der Inhaber des Signaturschlüssels diesen einem Dritten an. Dass sie oder er in der Folge haftet, ist unbestritten. Im anderen Extremfall lässt sich die Inhaberin oder der Inhaber den Signaturschlüssel nur gewaltsam abnehmen. Dass sie oder er in diesem Fall nicht haftet, ist ebenfalls unbestritten. Wo aber liegt die Grenze?

Von der Inhaberin oder vom Inhaber des Signaturschlüssels wird verlangt, diesen auf sich zu tragen oder wegzuschliessen, allerdings nur soweit dies zumutbar ist. Damit wird der Tatsache Rechnung getragen, dass ein Signaturschlüssel namentlich im familiären Umfeld nicht in jedem Fall dem Zugriff anderer entzogen ist und dass dies der Inhaberin oder dem Inhaber des Signaturschlüssels nicht zum Vorwurf gereicht.

Art. 12 Passwort

Gerade im beruflichen Umfeld ist damit zu rechnen, dass die Hardware, auf welcher der Signaturschlüssel abgelegt ist, relativ einfach zugänglich bleibt, dass aber mittels Passwortschutz sichergestellt wird, dass der Signaturschlüssel nicht missbraucht wird.

Absatz 2 verbietet es, dass eine Person, die Felix Muster heisst, als Passwort felixmuster oder musterfelix verwendet. Auch darf diese Person, falls sie am 30. März 1960 geboren wurde, nicht die Zahlenkombinationen 30031960, 30196003 oder 19603003, 19600330 und 03301960 und 03196003 gebrauchen.

Eine Verpflichtung, das Passwort oder die Zahlenkombination regelmässig zu ändern, wird nicht statuiert. Zum einen ist die Kontrolle der Einhaltung einer solchen Verpflichtung unrealistisch. Zum andern resultiert aus der Änderung eines Passworts nur bedingt ein Mehrwert an Sicherheit: Auch ein am Vortag geändertes Passwort kann ausspioniert und in der Folge missbraucht werden.

Es wird auch kein Verbot aufgestellt, Passworte und Zahlenkombinationen aufzuzeichnen. Bei Aufzeichnung des Passworts bzw. der Zahlenkombination ist aber immer dafür zu sorgen, dass auch die Aufzeichnung unter Verschluss gehalten wird (Absatz 3).

Bei der Diskussion über die Verlässlichkeit elektronischer Signaturen taucht immer wieder die Forderung auf, den Zugang zur elektronischen Signatur biometrisch zu sichern. Dem ist insofern Rechnung zu tragen, als der Zugang zur Hardware und damit zum Signaturschlüssel mittels biometrischer Verfahren gesichert werden kann. Die Biometrie übernimmt in diesem Fall die Funktion, die andernfalls ein Passwortschutz hat. Die Verordnung begnügt sich mit dem Grundsatz und lässt sich auf keine Diskussion darüber ein, wann biometrische Verfahren als ausreichend verlässlich gelten können (Absatz 4).

Die getrennte Aufbewahrung ist wohl die wirksamste Massnahme zur Verhinderung des Missbrauchs einer elektronischen Signatur (Abs. 5). Respektiert die Inhaberin oder der Inhaber des Signaturschlüssels diese Vorkehren, ist ein Missbrauch praktisch ausgeschlossen; selbstverständlich kann auch in diesem Fall darüber diskutiert werden, was getrennte Aufbewahrung heisst. Sicher keine getrennte Aufbewahrung liegt vor, wenn Signaturschlüssel und Passwort bzw. Zahlenkombination im gleichen Portemonnaie oder in der gleichen Schublade eines Pults abgelegt sind.

Art. 13 Meldung bei Verlust

Die Meldung eines verlustig gegangenen Signaturschlüssels bzw. die Notwendigkeit, das Zertifikat deswegen für ungültig zu erklären, ist im Grundsatz unbestritten. Klar ist auch, dass eine solche Meldung nur verlangt werden kann, soweit eine solche möglich und zumutbar ist. Dies ist beispielsweise nicht der Fall, wenn das Opfer nach einem Unfall im Spital liegt und andere Sorgen hat, als das auf ihn lautende Zertifikat für ungültig erklären zu lassen. Umstritten dürfte sein, ob man sich mit dem blossen Grundsatz "umgehende Meldung" begnügt oder ob man zusätzlich eine minimale Frist setzt. Im Sinne einer grösseren Rechtssicherheit drängt sich eine solche letztlich auf. Sie wird auf 24 Stunden seit Bemerken des Verlustes festgelegt.

Schlussbestimmungen

Art. 14 Vollzug

In Anwendung von Artikel 20 Absatz 2 ZertES wird das BAKOM beauftragt, die notwendigen technischen und administrativen Vorschriften zu erlassen. Die aktuellen Vorschriften (SR 784.103.1) müssen überarbeitet werden, um den Entwicklungen der letzten Jahre im Bereich der Normierung Rechnung zu tragen.

Art. 15 Aufhebung bisherigen Rechts

Die aktuelle Verordnung, die nur eine begrenzte Geltungsdauer hat (vgl. Art. 21 Abs. 2 ZertDV) wird formell aufgehoben.

Art. 16 Inkrafttreten

Das Gesetz, die Verordnung und die technischen und administrativen Vorschriften werden gleichzeitig per 1. Januar 2005 in Kraft gesetzt.

BAKOM/01.06.2004