BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2004 **Ausgegeben am 15. April 2004** **Teil II**

159. Verordnung des Bundeskanzlers, mit der die sicherheitstechnischen und organisationsrelevanten Voraussetzungen für Verwaltungssignaturen geregelt werden (VerwSigV)

Auf Grund des § 25 des Bundesgesetzes über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl. I Nr. 10/2004, und auf Grund des § 9 des Signaturgesetzes, BGBl. I Nr. 190/1999, wird – hinsichtlich des § 9 im Einvernehmen mit dem Bundesminister für Justiz – verordnet:

Signaturerstellungsdaten

§ 1. (1) Die Signaturerstellungsdaten der Verwaltungssignatur müssen hinsichtlich ihrer Schlüssellänge und ihrer Verwendbarkeit in Algorithmen den Signaturerstellungsdaten der sicheren Signatur im Sinne des § 2 Z 3 SigG entsprechen.

(2) Die Erzeugung der Signaturerstellungsdaten muss auf zufälligen Werten beruhen und es muss ausgeschlossen sein, dass sich Signaturerstellungsdaten eines Signators aus den Signaturerstellungsdaten anderer Signatoren errechnen lassen. Der eingesetzte Zufall muss auch mit hinreichend hoher Sicherheit ausschließen, dass es bei der Grundmenge an erwartbaren Zertifikaten zu zwei Zertifikaten mit gleichen Signaturerstellungsdaten kommen kann. Dazu müssen mindestens 128 Bit Zufall in die Erzeugung der Signaturerstellungsdaten eingehen und diese so gestaltet sein, dass die gesamten Signaturerstellungsdaten vom Zufall abhängig sind.

(3) Der Erzeugungsvorgang darf nicht die Freisetzung der Signaturerstellungsdaten außerhalb der Signaturerstellungseinheit bewirken. Spezielle Hardwareelemente für die Erzeugung der Signaturerstellungsdaten sind jedoch nicht vorgeschrieben

Authorisierungscode

§ 2. (1) Der Authorisierungscode des Benutzers einer Verwaltungssignatur darf in keiner der für die Verwaltungssignatur eingesetzten Systemkomponenten gespeichert sein und darf nach seiner Erstellung nur für den Benutzer verfügbar sein. Das System muss so ausgelegt sein, dass ein für Zwecke des Signierens eingegebener Authorisierungscode ausschließlich zur Erstellung von Signaturen und zum Ändern des Codes an einen allenfalls beteiligten Sicherheitsserver übermittelt werden kann. Dabei darf der Code weder im Eingabegerät**,** noch auf dem Weg zur Signaturerstellungseinheit, noch in der Signaturerstellungseinheit selbst über den Vorgang der Signaturerstellung oder Code-Änderung hinaus gespeichert bleiben.

(2) Sofern der Authorisierungscode nicht frei durch den Signator gewählt wird, muss seine Erstellung auf Zufallselementen beruhen, sodass ein Errechnen des Codes aus den Schlüsselwerten oder aus anderen Authorisierungscodes nicht möglich ist. Die Länge des Codes muss mindestens sechs Dezimalziffern entsprechen.

Signaturerstellungseinheit

§ 3. Signaturerstellungseinheit für die Verwaltungssignatur können entweder Signaturerstellungsgeräte (einschließlich der zugehörigen Mechanismen) beim Signator sein, die die Signaturerstellungsdaten hinreichend schützen, oder Signaturdienste, die im Auftrag des Signators auf Sicherheitsservern, die innerhalb eines gesicherten Bereichs betrieben werden, eingerichtet sind. Diese Signaturerstellungseinheiten müssen den nachfolgenden besonderen Sicherheitsbedingungen genügen:

1. Im Falle der Verwendung von Signaturerstellungsgeräten beim Signator:

a) Es sind nur Geräte zugelassen, die auf der Grundlage geeigneter Hardware die Signaturerstellungsdaten vor dem Ausspähen und Auslesen sowie vor der unbefugten Verwendung (ohne Einsatz der korrekten Authorisierungscodes) schützen.

b) Der Schutz vor der unbefugten Verwendung hat auch den Schutz vor dem „wiederholten Ausprobieren“ von Authorisierungscodes zu beinhalten.

c) Die kryptographischen Mechanismen, die von den Signaturerstellungsdaten abhängig sind bzw. Zufallselemente benötigen, müssen zur Gänze auf dem Signaturerstellungsgerät durchgeführt werden. Ein Ermitteln der Hashwerte der zu signierenden Daten außerhalb des Signaturerstellungsgerätes ist jedoch zulässig.

2. Im Falle der Verwendung von Signaturdiensten auf Sicherheitsservern:

a) Das Erfordernis, dass sich die Signaturerstellungsdaten in der ausschließlichen Verfügungsgewalt des Signators befinden müssen, ist dadurch sicherzustellen, dass zusätzlich zum Authorisierungscode ein Einmalcode verwendet wird, der außerhalb des Sicherheitsservers bzw. durch andere Personen als den Signator nicht systematisch ermittelbar ist.

aa) Sofern der Einmalcode in einem Gerät und/oder mit einem Mechanismus beim Signator erzeugt oder vorgehalten wird, dürfen nur solche Geräte oder Mechanismen eingesetzt werden, die den Signator in die Lage versetzen, sich hinreichend vor der missbräuchlichen Verwendung des Einmalcodes schützen zu können.

bb) Es muss sichergestellt sein, dass sowohl verwendete als auch nicht verwendete Einmalcodes aus der Vergangenheit nicht weiter verwendbar bleiben.

b) Die bei der Signatur zum Einsatz kommenden Komponenten (Geräte und Mechanismen) sind auch gegen den Missbrauch durch das eigene Personal des Betreibers des Sicherheitsservers zu schützen (z. B durch alternative Verteilungswege für die Einmalcodes). Es sind jedenfalls die folgenden Komponenten sicherheitskritisch:

aa) der Sicherheitsserver,

bb) die Erzeugung und Verwendung von Authorisierungscodes (Wissenskomponente*)* und

cc) der Mechanismus des Einmalcodes (Besitzkomponente).

c) Als Sicherheitsserver wird jene Komponente bezeichnet, innerhalb der die Signaturerstellungsdaten des Signators zur Verwendung entschlüsselt werden können und auf Verfügung des Signators zur Anwendung gebracht werden. Der Sicherheitsserver darf nur sicherheitskritische Funktionen vergleichbarer Sicherheitsstufen umfassen (Signaturerstellung, Sperre und Widerruf, Vernichten von Signaturerstellungsdaten, Verschlüsselung, Erzeugung von Zufallswerten für die Kryptographie, Zeitstempel, etc.). Die Funktionen müssen vollständig dokumentiert sein und dürfen nicht dynamisch ergänzt werden.

d) Der Zugriff auf den Sicherheitsserver ist auf das absolut notwendige Mindestmaß zu beschränken (z.B. durch eine Firewall, die nur einen Dienst offen hält). Die Art der Beschränkung ist nachprüfbar zu dokumentieren.

e) Signaturerstellungsdaten dürfen – außer zur Verwendung entsprechend der Verfügung des Signators während der Erstellung einer Signatur – auf dem Sicherheitsserver nur in verschlüsselter Form abgelegt sein. Signaturerstellungsdaten können zum Betrieb und zur Sicherung außerhalb des Sicherheitsservers verschlüsselt gespeichert werden, wenn durch „starke“ Verschlüsselung (> 100 Bit symmetrisch).sichergestellt ist, dass sie ausschließlich durch den Sicherheitsserver entschlüsselt werden können. Der hiefür notwendige Schlüssel muss organisatorisch (Vieraugenprinzip und Protokoll) und technisch (Safe) gesichert sein. In den Schlüssel zur verschlüsselten Speicherung ist der Authorisierungscode des Signators oder eine kryptographische Sicherung, die den Zugriffswillen des Benutzers zum gegebenen Zeitpunkt technisch sicherstellt, einzubinden, damit sichergestellt ist, dass ein Zugang zu den Signaturerstellungsdaten selbst dann nicht möglich ist, wenn die Inhalte der Speichermedien freigesetzt würden.

f) Authorisierungscode und Einmalcode sind beim Transport vom Benutzer zum gesicherten Bereich geeignet kryptographisch zu schützen. Vorzugsweise ist eine Verschlüsselung vom Eingabegerät bis zum Sicherheitsserver vorzusehen.

g) Der Sicherheitsserver muss ohne Bedienung arbeiten. Sofern zu Betriebs- oder Wartungszwecken irgendwelcher Art ein Zutritt notwendig ist, ist dieser organisatorisch (Vieraugenprinzip und Protokoll) und technisch (geeignete Absperrung des Raumes) abzusichern.

h) Ein Zugang über Datenübertragung zum gesicherten Bereich ist außer für die definierten Sicherheitsdienste nicht einzurichten (keine Remote Konsole, kein Telnet, usw.).

i) Im Wartungsfall dürfen keine Datenträger aus der Hand gegeben werden. Diese sind, sofern sie nicht mehr verwendet werden oder nicht mehr verwendbar sind, geeignet zu löschen und zu vernichten.

j) Es sind sämtliche Betriebs- und Wartungsarbeiten, soweit das System dies zulässt, auch automatisch zu dokumentieren. Die Dokumentation ist zumindest fünf Jahre aufzubewahren und muss allfälligen Audits zur Verfügung stehen.

Prüfung der Geräte und Mechanismen

§ 4. (1) Eine Prüfung oder Zertifizierung der für Verwaltungssignaturen eingesetzten Geräte und Mechanismen nach einem Schutzprofil wird nicht explizit vorgeschrieben. Geräte oder Mechanismen sind jedenfalls als geeignet anzusehen, wenn sie die Bedingungen der sicheren Signatur bzw. die Bedingungen der Geräte und Mechanismen erfüllen, die bei Zertifizierungsdiensteanbietern für qualifizierte Zertifikate eingesetzt werden.

(2) Liegt keine Evaluierung der zum Einsatz bei Verwaltungssignaturen bestimmten Komponenten (Geräte und Mechanismen) nach einem Schutzprofil vor, so dürfen diese nur eingesetzt werden, nachdem ein Gutachten einer Bestätigungsstelle im Sinne des § 19 SigG mit dem in Absatz 3 bezeichneten Inhalt die Einhaltung der Anforderungen gemäß §§ 1 bis 3 festgestellt hat.

(3) Das Gutachten der Bestätigungsstelle hat auf die einzelnen Punkte der in den §§ 1 bis 3 genannten Anforderungen einzugehen und hat auch festzustellen, in welchen Zeiträumen ein Audit zur Aufrechterhaltung der Sicherheit notwendig ist. Die Schlussaussage des Gutachtens muss „nach den Anforderungen für die Verwaltungssignatur geeignet“ oder „nach den Anforderungen für die Verwaltungssignatur nicht geeignet“ lauten. Notwendige Betriebsbedingungen können in einem derartigen Gutachten festgestellt werden.

(4) Im Sicherheitskonzept des Zertifizierungsdiensteanbieters ist auszuweisen, welche der eingesetzten Komponenten die Anforderungen für den Einsatz bei sicheren Signaturen bzw. bei Zertifizierungsdiensteanbietern für qualifizierte Zertifikate erfüllen und für welche Komponenten die Erfüllung der Anforderungen der Verwaltungssignatur in einem Gutachten nach Abs. 3 festgestellt wurde.

Personal

§ 5. Die Anforderungen des § 10 Abs. 4 und 5 SigV an die Fachkunde und Sicherheit des für die Ausstellung und die weitere Verwaltung sicherer Signaturen beim Zertifizierungsdienstanbieter eingesetzten Personals gelten auch hinsichtlich der Verwaltungssignaturen. Die Maßnahmen zur Gewährleistung der Erfüllung dieser Anforderungen sind im Sicherheitskonzept des Zertifizierungsdiensteanbieters darzustellen.

Identifikation

§ 6. Die im Hinblick auf die Bestätigung der Identität im Zertifikat notwendige Identifikation des Signators darf bei der Registrierung für die Verwaltungssignatur nur erfolgen

1. in seiner Anwesenheit und aufgrund der Vorlage eines amtlichen Lichtbildausweises oder
2. ohne sein persönliches Erscheinen beim Zertifizierungsdiensteanbieter
   a) durch Übersendung der für die Freischaltung der Verwaltungssignatur notwendigen Informationen in einer Form, die die Überprüfung der Identität des Empfängers mit jener Verlässlichkeit gewährleistet, die bei der Zustellung zu eigenen Handen (§ 21 ZustellG) eingehalten wird;
   b) elektronisch durch Verwendung einer weiteren Bürgerkarte des Signators.

Verzeichnisdienste

§ 7. Verzeichnisdienste für die Zertifikate der Verwaltungssignatur müssen verfügbar sein. Darüber hinausgehende Auflagen der Verfügbarkeit und Sicherheit dürfen von Behörden nicht gestellt werden, sofern bei den bei ihnen verwendeten Signaturformaten das Zertifikat dem gültig signierten Dokument beigelegt wird.

Widerrufsdienste

§ 8. Der Widerruf eines Zertifikates ist von dem hiezu berufenen Zertifizierungsdiensteanbieter zu veröffentlichen (Widerrufsdienst), es sei denn dass die Signaturerstellungsdaten ausschließlich im Sicherheitsserver verwendbar sind und mit dem Widerruf das Vernichten der Signaturerstellungsdaten sichergestellt ist. Das Vorliegen des letzteren Falles ist im Sicherheitskonzept des Zertifizierungsdiensteanbieters festzuhalten und als „automatischer und impliziter Widerrufsdienst“ zu bezeichnen.

Bürgerkarte

§ 9. (1) Abgesehen von sicheren Signaturen dürfen nur Signaturen, die die für Verwaltungssignaturen nach den vorstehenden Bestimmungen geltenden Anforderungen erfüllen, für die Funktion „Bürgerkarte“ verwendet werden. Die Stammzahlenregisterbehörde darf daher eine Personenbindung nur vornehmen, wenn sie auf ihr Verlangen vom Zertifizierungsdiensteanbieter alle Auskünfte und Nachweise erhält, die sie benötigt, um das Vorliegen einer Verwaltungssignatur beurteilen zu können.

(2) Eine Verwaltungssignatur im Sinne dieser Verordnung liegt nur vor, wenn die Voraussetzungen der §§ 1 bis 8 erfüllt sind. Zertifizierungsdiensteanbieter von Verwaltungssignaturen, die in Bürgerkarten Verwendung finden, haben in geeigneter Weise dafür Vorsorge zu treffen, dass einzelne oder alle Zertifikate durch Widerruf unverzüglich für ungültig erklärt werden, wenn die Stammzahlenregisterbehörde feststellt, dass die Gefahr einer missbräuchlichen Verwendung des Zertifikates besteht.

Inkrafttreten

§ 10. Diese Verordnung tritt mit 16. April 2004 in Kraft.

Schüssel