Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen- und Rechnungswesen der Bayerischen Kommunen (AFS-HKR)

Inhalt

1. Präambel

Auf der Grundlage von § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik werden nachfolgend die Mindest-Anforderungen an fortgeschrittene elektronische Signaturen, die in automatisierten Verfahren für das Haushalts-, Kassen- und Rechnungswesen (HKR-Verfahren) zum Einsatz kommen sollen, näher festgelegt.

2. Zweck und Geltungsbereich

a) Diese Richtlinie gilt für fortgeschrittene elektronische Signaturen im Sinne von § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik.

b) Zweck dieser Richtlinie ist es, gemäß §§ 87 Nr. 12 KommHV-Kameralistik, 98 Nr. 21 KommHV-Doppik ergänzende Merkmale für die fortgeschrittene elektronische Signatur festzulegen, um bei deren Einsatz eine einheitliche Handhabung und ein angemessenes Sicherheitsniveau sicherzustellen.

3. Eigenschaften der fortgeschrittenen elektronischen Signatur

a) Die im Haushalts-, Kassen- und Rechnungswesen verwendete fortgeschrittene elektronische Signatur muss die in Art. 26 eIDAS-VO genannten Anforderungen erfüllen.

b) Für die elektronischen Signaturerstellungsdaten, die Zertifikate und die Signaturvalidierungsdaten gelten Art. 3 Nrn. 13, 14 und 40 eIDAS-VO sinngemäß. Die elektronischen Zertifikate müssen einer natürlichen Person zugeordnet sein und den Namen dieser Person bestätigen.

c) Das Zertifikat für elektronische Signaturen darf nur für den innerdienstlichen Gebrauch verwendet werden.

4. Zertifizierungsstellen

a) Als Zertifizierungsstelle für die fortgeschrittene elektronische Signatur nach dieser Richtlinie ist jede Zertifizierungsstellen zugelassen, die

- ihren Vertrauensdienst nach der Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung für die X.509-Zertifikatshierarchie innerhalb der deutschen Verwaltungs-PKI (Bayerische Verwaltungs-PKI) betreibt (vgl. Anlage 1) oder

- einen vergleichbar sicheren Betrieb des Vertrauensdienstes gewährleistet, dies mit einer Zertifizierungsrichtlinie nach RFC 3647 dokumentiert und in einer entsprechenden Selbsterklärung bestätigt.

b) Diese Voraussetzungen müssen von der Zertifizierungsstelle über die gesamte Zeitdauer des Betriebs des Zertifizierungsdienstes sichergestellt sein.

5. Vergabe fortgeschrittener Zertifikate

a) Der Antrag auf Ausstellung eines Zertifikats für fortgeschrittene elektronische Signaturen ist bei einer durch eine Zertifizierungsstelle nach Nr. 4 Buchst. a zugelassenen und ausreichend eingewiesenen Registrierungsstelle (RA, vgl. Nr. 11 Buchst. c) zu stellen. Im Übrigen wird auf die Nrn. 4.1 u. 4.2 der Zertifizierungsrichtlinie der bayerischen Verwaltungs-PKI verwiesen.

b) Die Zertifizierungsstelle hat die die Verknüpfung der Signaturvalidierungsdaten mit einer natürlichen Person durch ein elektronisches Zertifikat zu bestätigen. Dieses Zertifikat ist jederzeit für jeden über eine öffentlich erreichbare Kommunikationsverbindung (Vertrauensdienst, vgl. Art. 3 Nr. 16 eIDAS-VO) für die Dauer der Aufbewahrungsfrist von Belegen nachprüfbar und abrufbar zu halten. Gleiches gilt für die Informationen über gesperrte Zertifikate (Sperrlisten, vgl. Nr. 11 Buchst. f).

c) Bei der erstmaligen Antragstellung muss die Registrierungsstelle den Unterzeichner (vgl. Art. 3 Nr. 9 eIDAS-VO) zuverlässig identifizieren.

d) Für die Identifizierung, Authentifizierung und Namensgebung ist Nr. 3 der Zertifizierungsrichtlinie der bayerischen Verwaltungs-PKI anzuwenden.

e) Folgezertifikate können vom Unterzeichner entweder bei der ursprünglichen Registrierungsstelle oder mit einem elektronisch signierten Verlängerungsantrag direkt bei der Zertifizierungsstelle beantragt werden. Eine nochmalige Identifizierung des Antragstellers ist hierbei nicht notwendig.

f) Die Zertifizierungsstelle und die Registrierungsstellen haben Vorkehrungen zu treffen, damit die (Antrags-)Daten für die fortgeschrittenen Zertifikate nicht unbemerkt verändert oder unterdrückt werden können.

g) Die Geheimhaltung der Signaturerstellungsdaten ist zu gewährleisten. Die Zertifizierungsstelle hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass diese Daten nicht unbemerkt genutzt, gefälscht oder vervielfältigt werden können.

6. Unterrichtungspflicht

Die Registrierungs- oder Zertifizierungsstelle hat den Signaturschlüssel-Inhaber in schriftlicher oder elektronischer Form über die Maßnahmen zu unterrichten, die für die Sicherheit und die zuverlässige Prüfung der fortgeschrittenen Signaturen notwendig sind.

7. Inhalt und Gültigkeitsdauer fortgeschrittener Zertifikate

a) Ein Zertifikat für fortgeschrittene elektronische Signaturen i.S. von § 87 Nr. 12 KommHV-Kameralistik, § 98 Nr. 21 KommHV-Doppik muss mindestens die in der Anlage 2 beschriebenen Pflichtangaben enthalten.

b) Pseudonyme dürfen in fortgeschrittenen Zertifikaten nicht verwendet werden.

8. Sperrung fortgeschrittener Zertifikate

Für die Sperrung von Zertifikaten gilt Nr. 4.9 der Zertifizierungsrichtlinie der Bayerischen Verwaltungs-PKI.

9. Verfahren zum langfristigen Erhalt der Beweiskraft signierter Dokumente

a) Daten mit einer fortgeschrittenen Signatur sind neu zu signieren, wenn sie in signierter Form länger benötigt werden, als die Eignung der für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter reicht. In diesem Falle sind die Daten vor Ablauf der Eignung mit einer neuen fortgeschrittenen elektronischen Signatur zu versehen. Diese muss frühere Signaturen einschließen.

b) Eine Neusignierung nach Buchst. a ist nicht erforderlich, solange die signierten Daten gemeinsam mit den fortgeschrittenen Signaturen in einer Weise gespeichert werden, die die Unveränderbarkeit dieser Daten während der Dauer der Aufbewahrungsfristen gewährleistet (vgl. § 71 Abs. 2 KommHV-Kameralistik, § 67 Abs. 2 KommHV-Doppik).

c) Werden die signierten Daten in ein anderes Format transformiert, gilt Buchst. a entsprechend.

10. Anforderungen an Produkte für fortgeschrittene elektronische Signaturen

a) Für die Schlüsselerzeugung, Installation, Aufbewahrung und Management der Schlüssel durch die Zertifizierungsstelle gelten die Nrn. 6.1, 6.2 und 6.3 der Zertifizierungsrichtlinie der Bayerischen Verwaltungs-PKI.

b) Für die Speicherung von Signaturerstellungsdaten und die Erzeugung fortgeschrittener elektronischer Signaturen dürfen Software-Token (z.B. PKCS#8- oder PKCS#12-Dateien, Windows PSE) oder Hardware-Token (z.B. TPM, USB-Token oder Chipkarten) verwendet werden.

c) Beim Einsatz von Software-Token ist durch angemessene technische und organisatorische Maßnahmen sicherzustellen, dass die Signaturerstellungsdaten weder exportiert noch unbefugt verwendet werden können. Im Übrigen wird auf Art. 26 Buchst. c eIDAS-VO verwiesen.

d) Werden die Signaturerstellungsdaten auf einem zentralen Serversystem gespeichert, müssen diese in einem kryptographischen Modul (HSM) aufbewahrt werden. Beim Einsatz von Remote- oder Fernsignaturlösungen müssen die fortgeschrittenen Signaturen ebenfalls im kryptographischen Modul erzeugt werden.

e) Die eingesetzten kryptographischen Module müssen über eine dem Schutzbedarf angemessene Sicherheitszertifizierung (z.B. nach FIPS 140-2 Level 3, Common Criteria EAL 4+ oder EN 419221-5) verfügen.

f) Die fortgeschrittenen Signaturerstellungseinheiten müssen die in Anlage 3 genannten Anforderungen erfüllen.

g) Die Erfüllung der in den Buchst. b bis f genannten Anforderungen ist im Rahmen der Freigabe des automatisierten Verfahrens nach § 37 Abs. 1 Nr. 1 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 1 KommHV-Doppik zu bestätigen.

11. Begriffsbestimmungen

a) Personalisierungsprozess
Beim Personalisierungsprozess speichert die Registrierungsstelle das für den Signaturschlüssel-Inhaber generierte Zertifikat sowie den persönlichen Signaturschlüssel auf einer sicheren Signaturerstellungseinheit (SmartCards) und wickelt die damit zusammenhängenden Prozesse (z.B. Bedrucken der SmartCard mit Identifikationsdaten, Generierung von PIN und PUK, Erstellen des PIN-Briefes) ab.

b) Produktionsstelle
Registrierungsstelle mit Personalisierungseinheit, die im Auftrag der originär zuständigen Registrierungsstelle den Personalisierungsprozess übernimmt.

c) Registrierungsstelle (Registration Authority = RA)
Stelle, die den Antrag eines Teilnehmers auf ein Zertifikat entgegennimmt, vor Ort die Identität des Teilnehmers zuverlässig feststellt, die Richtigkeit der Daten im Zertifikatsantrag prüft und den Wunsch auf Schlüsselerzeugung und Zertifizierung an die zuständige Zertifizierungsstelle weiterleitet und den Personalisierungsprozess entweder selbst vornimmt oder eine Produktionsstelle damit beauftragt.

d) Technische Kompromittierung
Die Vertrauenswürdigkeit eines Systems, einer Datenbank oder eines einzelnen Datensatzes ist nicht mehr gegeben, weil Daten manipuliert sein könnten und der Eigentümer bzw. Administrator des Systems über die korrekte Funktionsweise oder den korrekten Inhalt keine Kontrolle mehr hat bzw. ein nicht berechtigter Nutzer ein anderes Ziel der Manipulation erreicht hat.

e) Verzeichnisdienst
Hierarchische Datenbank (z.B. LDAP), die u.a. Zertifikate oder Sperrlisten verwalten kann und die Informationen über den Zertifikatsstatus (z.B. SCVP oder OCSP) dem anfragenden Programm mitteilt.

f) Zertifikatssperrlisten (Certificate Revocation List - CRL)
Liste mit für ungültig erklärten Zertifikaten, die in einem Trustcenter geführt wird.

g) Zertifizierungsstelle (Certification Authority = CA)
Stelle, welche fortgeschrittene Zertifikate oder fortgeschrittene Zeitstempel bereitstellt und die Signatur von Zertifikatsanträgen übernimmt. Hierbei findet eine sichere Zuordnung von öffentlichem Schlüssel und Teilnehmer statt.

12. Anlagen

a) Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung für die X.509-Zertifikatshierarchie innerhalb der deutschen Verwaltungs-PKI (Bayerische Verwaltungs-PKI), Stand 17.12.2015

b) Anforderungen an fortgeschrittene Zertifikate für elektronische Signaturen

c) Anforderungen an fortgeschrittene elektronische Signaturerstellungseinheiten