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

Stand: 10.08.2010

Inhalt

1. Präambel

Auf der Grundlage von § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik werden nachfolgend die Anforderungen an fortgeschrittene elektronische Signaturen, die in automatisierten Verfahren für das Haushalts-, Kassen- und Rechnungswesen (HKR-Verfahren) zum Einsatz kommen sollen, näher festgelegt. Die Regelungen sollen sicherstellen, dass die verwendeten fortgeschrittenen elektronischen Signaturen in Handhabung, Sicherheit, Nachprüfbarkeit und Beweisqualität den Anforderungen des Haushalts-, Kassen- und Rechnungswesens genügen.

2. Zweck und Geltungsbereich

a) Diese Richtlinie gilt für fortgeschrittene 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 Signatur nach dem Signaturgesetz festzulegen, um den Einsatz der fortgeschrittenen elektronischen Signatur in den nach Kommunalhaushaltsrecht zugelassenen Fällen zu ermöglichen.

3. Eigenschaften der fortgeschrittenen Signatur

a) Die fortgeschrittene Signatur (vgl. § 2 Nr. 2 SigG) muss

- auf einem Signaturschlüssel (vgl. § 2 Nr. 4 SigG), einem Signaturprüfschlüssel (vgl. § 2 Nr. 5 SigG) und einem gültigen fortgeschrittenen Zertifikat (vgl. Nr. 7 Buchst. a) beruhen, die von einer Zertifizierungsstelle (vgl. Nr. 11 Buchst. g) aus dem Bereich der öffentlichen Verwaltung (Bund, Länder, Kommunen) erzeugt und ausgegeben wurden, und

- mit einer sicheren Signaturerstellungseinheit (vgl. § 2 Nr. 10 SigG) erzeugt werden.

Grundlage für diese Dienste muss die bundesweit verfügbare zertifikatsbasierte Schlüsselinfrastruktur der öffentlichen Verwaltung (Verwaltungs-PKI – VPKI) sein.

Signaturschlüssel, Signaturprüfschlüssel und fortgeschrittenes Zertifikat müssen einer natürlichen Person zugeordnet sein.

b) Das fortgeschrittene Zertifikat 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

- von der Wurzelzertifizierungsinstanz der deutschen Verwaltungs-PKI (Bundesamt für die Sicherheit in der Informationstechnik - BSI) zertifiziert ist und

- den Betrieb des Zertifizierungsdienstes nach den aktuellen Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung und die weiteren Voraussetzungen für den Betrieb einer Zertifizierungsstelle nach dieser Richtlinie gewährleistet.

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 ist bei einer durch eine Zertifizierungsstelle der VPKI zugelassenen und ausreichend eingewiesenen Registrierungsstelle (RA vgl. Nr. 11 Buchst. c) zu stellen.

b) Die Zertifizierungsstelle hat die Zuordnung eines Signaturprüfschlüssels zu einer identifizierten Person durch ein Zertifikat zu bestätigen. Dieses Zertifikat ist jederzeit für jeden über eine öffentlich erreichbare Kommunikationsverbindung (Verzeichnisdienst vgl. Nr. 11 Buchst. e) 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 Signaturschlüssel-Inhaber (vgl. § 2 Nr. 9 SigG) zuverlässig identifizieren. Die Registrierungsstelle darf dazu mit Einwilligung des Antragstellers personenbezogene Daten nutzen, die die Registrierungsstelle bereits zu einem früheren Zeitpunkt erhoben

hat oder die ihr von einer anderen Stelle auf sicherem Wege übermittelt wurden, sofern diese Daten eine zuverlässige Identifizierung des Antragstellers gewährleisten. Im Übrigen sind die Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung (Anlage 1) entsprechend anzuwenden.

d) Folgezertifikate können vom Signaturschlüssel-Inhaber 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.

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

f) Die Geheimhaltung der Signaturschlüssel ist zu gewährleisten. Eine Speicherung der Signaturschlüssel außerhalb einer sicheren Signaturerstellungseinheit ist unzulässig. Die Zertifizierungsstelle hat Vorkehrungen zu treffen, damit Daten für fortgeschrittene Zertifikate nicht unbemerkt gefälscht oder verfälscht 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. § 6 SigG ist sinngemäß anzuwenden.

7. Inhalt und Gültigkeitsdauer fortgeschrittener Zertifikate

a) Ein fortgeschrittenes Zertifikat muss die in § 7 Abs. 1 Nrn. 1 bis 7 SigG beschriebenen Pflichtangaben enthalten und eine fortgeschrittene elektronische Signatur tragen.

b) Pseudonyme (z.B. im Sinne von § 7 Abs. 1 Nr. 1 SigG) dürfen in fortgeschrittenen Zertifikaten nicht verwendet werden.

8. Sperrung fortgeschrittener Zertifikate

a) Die Zertifizierungsstelle hat ein fortgeschrittenes Zertifikat unverzüglich zu sperren, wenn die in § 8 Abs. 1 Satz 1 SigG genannten Gründe vorliegen.

b) Der Dienstherr bzw. Arbeitgeber oder die Registrierungsstelle kann die sofortige Sperrung des fortgeschrittenen Zertifikats verlangen, wenn

- der Signaturschlüssel-Inhaber aus dem Dienst- oder Arbeitsverhältnis ausscheidet,
- der Signaturschlüssel oder die sichere Signaturerstellungseinheit kompromittiert wurde,
- die PIN für die sichere Signaturerstellungseinheit an andere Personen weitergegeben oder diese auf andere Weise kompromittiert wurde,
- der Dienstherr bzw. Arbeitgeber aus sonstigen wichtigen Gründen dem Signaturschlüssel-Inhaber die Unterschriftsbefugnis entziehen möchte.

c) Weitere Sperrgründe können sich aus den Sicherheitsleitlinen der Wurzelzertifizierungsinstanz der Verwaltung (BSI) ergeben.

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 einem qualifizierten Archivsystem im Sinne von § 71 Abs. 2 KommHV-Kameralistik oder § 67 Abs. 2 KommHV-Doppik aufbewahrt werden.

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

10. Produkte für fortgeschrittene elektronische Signaturen

a) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung fortgeschrittener elektronischer Signaturen gelten § 17 Abs. 1 SigG und § 15 SigV entsprechend. Als sichere Signaturerstellungseinheiten sind ausschließlich solche zugelassen, die auch für qualifizierte Signaturen nach dem SigG verwendet werden dürfen.

b) Für die Darstellung zu signierender Daten gelten § 17 Abs. 2 SigG und § 15 SigV entsprechend.

c) Die in den automatisierten Verfahren im Sinne von § 37 KommHV-Kameralistik/ § 35 KommHV-Doppik verwendeten Signaturanwendungskomponenten (vgl. § 2 Nr. 11 SigG) müssen mindestens die Sicherheitsstufe EAL 4+ nach den Common Criteria (CC) erfüllen.

d) Die Erfüllung der Anforderungen nach Buchst. a ist durch entsprechende Prüfbestätigungen nachzuweisen. Für die Erfüllung der Anforderungen nach den Buchstaben b und c genügt eine Erklärung durch den Hersteller oder Lieferanten des automatisierten Verfahrens, das mit den Signaturanwendungskomponenten zusammenwirkt. Diese ist beim Bayerischen Staatsministerium des Innern (StMI) in schriftlicher oder elektronischer Form (vgl. §§ 126, 126a BGB) zu hinterlegen.

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 u. 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 Zertifizierungsstelle (CA) 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 Zertifikatsstatus über ein Protokoll (z.B. 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 der VPKI bereitstellt und die Signatur von Zertifikatsanträgen übernimmt. Hierbei findet eine sichere Zuordnung von öffentlichem Schlüssel und Teilnehmer statt.

12. Anlagen

a) Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung (VPKI-Richtlinie BSI, Stand: 09.01.2003)

b) Sicherheitsrichtlinien (Policy) der Zertifizierungsinstanz (CA) für das Bayerische Behördennetz (BayPKI-Richtlinie LfStaD, Stand: 09.02.2010)