Begründung zur AFS-HKR

Stand: 10.08.2010

Inhalt

1. Allgemeiner Teil

1.1 Ausgangslage

Mit der Änderung der KommHV-Kameralistik vom 05.10.2007 (GVBl S. 707) und Einführung der neuen KommHV-Doppik vom 05.10.2007 (GVBl S. 678) wurde für bestimmte Vorgänge (z.B. förmliche Kassenanordnung) neben der bisher vorgeschriebenen Schriftform auch die elektronische Form zugelassen. Damit sind die wesentlichen Rahmenbedingungen für die Anwendung von fortgeschrittenen und von qualifizierten elektronischen Signaturen im Bereich des Haushalts-, Kassen- und Rechnungswesens geschaffen.

Während die qualifizierte elektronische Signatur im Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.05.2001 (BGBl I S. 876) und in der Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16.11.2001 (BGBl I S. 3074) abschließend geregelt ist, sind im SigG nur die Merkmale einer fortgeschrittenen elektronischen Signatur im Rahmen einer Legaldefinition näher beschrieben. Dies hat systematische Gründe, da die gesetzlich geregelte qualifizierte Signatur auf den Merkmalen der fortgeschrittenen Signatur aufbaut (vgl. Definition in Art. 2 Abs. 2 EG-Richtlinie 1999/93/EG vom 13.12.1999[1] – EG-Signaturrichtlinie und dessen Umsetzung in § 2 Abs. 2 SigG). Über die gemeinsamen Anforderungen hinaus, dass fortgeschrittene Signaturen dem Signaturschlüssel-Inhaber zugeordnet sein müssen, dessen Identifizierung und alleinige Kontrolle der Mittel für die Signaturerstellung sowie eine Integritätsprüfung der damit signierten elektronischen Daten ermöglichen müssen, enthält das SigG keine weiteren Vorschriften zur fortgeschrittenen Signatur. Insbesondere fehlen Regelungen

– zum Aufbau und Inhalt fortgeschrittener elektronischer Zertifikate,

– zum Schutz der fortgeschrittenen Zertifikate und des persönlichen Signaturschlüssels,

– zur Absicherung des Signaturerstellungsprozesses und

– zum Betrieb der Zertifizierungsdienste.

[1] Die Änderung der EG-Signaturrichtlinie durch EG-Verordnung 1137/2008 vom 22.10.2008 betrifft nur die Qualitätssicherung der sicheren Signaturerstellungseinheiten und ist insoweit nicht relevant.

Die fortgeschrittene Signatur ist damit offen für die technische und organisatorische Ausgestaltung und muss somit an die Bedürfnisse der jeweiligen Anwendung angepasst werden.

Hierbei ist zu berücksichtigen, dass automatisierte Verfahren, die dem Haushalts-, Kassen- und Rechnungswesen dienen, in der Regel in geschlossenen, meist besonders abgesicherten internen Verwaltungsnetzen ablaufen und interne Verwaltungsprozesse unterstützen (z.B. die Ermittlung von Ansprüchen oder Zahlungsverpflichtungen, die Buchführung und den Zahlungsverkehr). Wegen des abgeschlossenen Benutzerkreises und der allgemeinen beamten- und arbeitsrechtlichen Vorgaben bestehen im Regelfall zwar niedrigere Anforderungen als bei einer Kommunikation mit Externen. Gleichwohl sind im Hinblick auf die Ordnungsmäßigkeit und Nachvollziehbarkeit des Haushalts-, Kassen- und Rechnungswesens, die Kassensicherheit und die Aufbewahrungsfristen für Belege und Bücher ergänzende Regelungen notwendig, die den Einsatz von fortgeschrittenen elektronischen Signaturen in diesem Bereich einheitlich regeln und revisionssicher gestalten.

Die vorliegenden Voraussetzungen für den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen- und Rechnungswesen (AFS-HKR) ergänzen deshalb die gesetzlichen Anforderungen an fortgeschrittene elektronische Signaturen mit zusätzlichen Qualitätsmerkmalen, soweit diese aus den vorstehenden Gründen notwendig und zweckmäßig erscheinen. Insbesondere darf auch die fortgeschrittene Signatur vom Verwender nicht abstreitbar sein und muss selbst bei einem unterschiedlichen Qualitätsniveau in der Administration der eingesetzten technischen Systeme und automatisierten Verfahren eine zuverlässige Nachweis- und Beweisführung ermöglichen.

Die festgelegten Anforderungen an den Betrieb der Zertifizierungsdienste orientieren sich aus Gründen der Verwaltungsvereinfachung an den bestehenden Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung (VPKI-Richtlinien), da diese eine solide und sichere Grundlage für eine zertifikatsbasierte Schlüsselinfrastruktur (PKI) und die damit zusammenhängenden Dienste (Authentisierung, Verschlüsselung und Erstellung fortgeschrittener elektronischer Signaturen) innerhalb der Bundes-, Landes- und Kommunalverwaltung darstellen.

1.2 Zielsetzung und Gegenstand

Die AFS-HKR legt die Voraussetzungen für fortgeschrittene Signaturen im Sinne von § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik fest. Mit den in der AFS-HKR beschriebenen Anforderungen soll erreicht werden, dass die verwendeten fortgeschrittenen Signaturen in der Handhabung, Sicherheit, Nachprüfbarkeit und Beweisqualität den qualifizierten Signaturen annähernd gleichwertig sind und als adäquater Ersatz für die kommunalhaushaltsrechtlich vorgeschriebene Schriftform eingesetzt werden können.

Die AFS-HKR dient zugleich der Verwaltungsmodernisierung, da sie einerseits medienbruchfreie elektronische Verwaltungsprozesse gestalten lässt, die bisher wegen der geforderten Schriftform nicht möglich waren. Andererseits sind auf Basis von multifunktionalen Signaturkarten weitere Anwendungen denkbar, bei denen es auf die zuverlässige Authentifizierung und Identifizierung des Signaturkarten-Inhabers ankommt (z.B. elektr. Dienstausweis, Zutritts- und Zugangskontrolle, Zeiterfassung, single-sign-on an IT-Systemen und automatisierten Verfahren).

Die Regelungen in der AFS-HKR stehen auch nicht im Widerspruch zur EG-Signaturrichtlinie oder dem geltenden SigG. Die im Haushalts-, Kassen- und Rechnungswesen verwendeten Zertifikate und Signaturen werden nur verwaltungsintern, also in nicht-öffentlichen, geschlossenen Netzen eingesetzt. Hierdurch ist gewährleistet, dass weder der freie Waren- und Dienstleistungsverkehr im Binnenmarkt noch grenzüberschreitende Dienste für den Bürger behindert werden. Zudem wird in diesem Zusammenhang auf Nr. 16 der Erwägungsgründe der EG-Signaturrichtlinie hingewiesen, der auch bei anderen geschlossenen Systemen von den gesetzlichen Rahmenbedingungen abweichende (z.B. privatrechtliche) Regelungen für elektronische Signaturen zulässt.

1.3 Finanzielle Auswirkungen

Aus der AFS-HKR ergeben sich keine unmittelbaren Kosten für die Kommunen, da der Einsatz von elektronischen Signaturen freigestellt ist. Als technische Rahmenbedingungen sind die Regelungen in erster Linie von den Zertifizierungsdiensteanbietern innerhalb der VPKI und den Herstellern automatisierter Verfahren zu berücksichtigen.

Mittelbar können sich für die Kommunen zwar Kosten bei der Einführung ergeben (z.B. aus der Anschaffung von Signaturkarten, Lesegeräten und dem lfd. Betrieb). Es ist aber davon auszugehen, dass vor der Einführung von zertifikats- oder signaturgestützten elektronischen Verwaltungsprozessen eine Wirtschaftlichkeitsbetrachtung durchgeführt wird und eine Umsetzung erst beim Nachweis der Wirtschaftlichkeit eines solchen Projekts erfolgt.

2. Besonderer Teil

2.1 zu Nr. 1 Vorbemerkung

Die Regelung verdeutlicht, dass nur fortgeschrittene elektronische Signaturen mit bestimmten (erweiterten) Qualitätsmerkmalen die haushaltsrechtlich vorgeschriebene

Schriftform ersetzen können. Diese müssen eine sichere Authentifizierung und Identifizierung der signierenden Person und eine zuverlässige Prüfung der Integrität signierter Daten zulassen. Im Hinblick auf die Kassensicherheit muss außerdem gewährleistet sein, dass elektronische Signaturen, die die sachliche und rechnerische Richtigkeit bestätigen oder mit denen Zahlungen angeordnet werden, nur mit Mitteln erzeugt werden können, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann. Damit die persönlichen Zertifikatsdaten, insbesondere der private Signaturschlüssel, nicht durch Unbefugte ausgelesen oder das bei Signaturvorgängen eingegebene Passwort (PIN) nicht durch Schadprogramme aufgezeichnet werden kann, sind sichere Signaturerstellungseinheiten notwendig, wie sie auch bei der Erzeugung qualifizierter Signaturen vorausgesetzt werden. Eine nur auf Softwarekomponenten beruhende Signaturerstellungseinheit (z.B. im Zertifikatsspeicher des PC-Betriebssystems gespeichertes Zertifikat und Signaturschlüssel) kann dies nicht zuverlässig gewährleisten. Gerade in diesem sicherheitskritischen Bereich können kleine Fehler bei der Administration oder Bedienung der Anwendungs-/Signatursoftware leicht zur Kompromittierung von privaten Signaturschlüsseln führen. Diese Risiken lassen sich bei Einsatz entsprechender Hardware (Chipkarte in Form einer sog. SmartCard mit eigenem Betriebssystem, externes Chipkarten-Lesegerät mind. Klasse 2) vermeiden. Da mit der Feststellungs- und Anordnungsbefugnis auch eine persönliche Haftung oder strafrechtliche Verantwortlichkeit des Signierenden verbunden sein kann, kommt es gerade in diesem Bereich auf die Nicht-Abstreitbarkeit der elektronischen Signaturen und die zuverlässige Zuordnung des Signaturschlüssel-Inhabers zum Zertifikat oder zur Signatur an.

2.2 zu Nr. 2 Zweck und Geltungsbereich

Die gesetzlich vorgeschriebene Schriftform kann nur durch eine elektronische Form mit qualifizierten Signaturen nach dem Signaturgesetz rechtswirksam ersetzt werden (vgl. § 126 Abs. 3 i. V. m. § 126a BGB oder §§ 3a Abs. 2, 37 Abs. 3 VwVfG bzw. Art. 3a Abs. 2, 37 BayVwVfG). Konsequenterweise erleichtert deshalb § 371a ZPO nur für elektronische Dokumente mit qualifizierten Signaturen die prozessuale Beweisführung, indem auf solchermaßen signierte private und öffentliche elektronische Dokumente die Vorschriften über die Beweiskraft und die Echtheit der jeweiligen Urkundsart entsprechend angewandt werden (gesetzliche Beweisregel). Alle elektronischen Dokumente mit anderen elektronischen Signaturen unterliegen dagegen der freien richterlichen Beweiswürdigung und sind Objekte des Beweises durch Augenschein (vgl. § 371 Abs. 1 Satz 2 ZPO).

Elektronische Dokumente mit fortgeschrittenen Signaturen im Sinne von § 2 Nr. 2 SigG sind daher im rechtsgeschäftlichen Verkehr nur dann als Schriftformersatz geeignet, wenn die Schriftform nicht gesetzlich vorgeschrieben ist und die von § 126a BGB abweichende elektronische Form entweder durch ein Rechtsgeschäft (z.B. Vertrag) aus-

drücklich vereinbart wurde oder dem Willen der Vertragsparteien entspricht (vgl. § 127 Abs. 3 BGB).

Auch die öffentlich-rechtlichen Kommunalhaushaltsverordnungen ermöglichen den Ersatz der schriftlichen Form durch die elektronische Form. Gemäß §§ 39 Abs. 1 Satz 2, 41 Abs. 1 Satz 2, 43 Abs. 3 Satz 2 KommHV-Kameralistik oder §§ 35 Abs. 1 Satz 2, 37 Abs. 1 Satz 2, 39 Abs. 3 Satz 2 KommHV-Doppik kann die dort vorgeschriebene Schriftform durch eine elektronische Form mit elektronischen Signaturen ersetzt werden. Die Art und Qualitätsstufe der hierbei zulässigen elektronischen Signaturen wird erst in den jeweiligen Begriffsdefinitionen der Kommunalhaushaltsverordnungen näher bestimmt. Neben der gesetzlich geregelten qualifizierten Signatur lassen § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik die fortgeschrittene Signatur im Sinne von § 2 Nr. 2 SigG zu, wenn diese bestimmte ergänzende Qualitätsmerkmale besitzt. Diese erweiterten Merkmale sind in der AFS-HKR näher bestimmt.

Die Regelungen in Nr. 2 AFS-HKR dienen einerseits zur Klarstellung der vorstehend dargestellten Rechtslage und beschreiben andererseits den speziellen Anwendungsbereich von fortgeschrittenen Signaturen innerhalb des Haushalts-, Kassen- und Rechnungswesens.

2.3 zu Nr. 3 Eigenschaften der fortgeschrittenen Signatur

In Anlehnung an § 2 Nrn. 2 und 3 SigG müssen die fortgeschrittenen Signaturen

– ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein,

– die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,

– mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,

– zum Zeitpunkt ihrer Erzeugung auf einem gültigen Zertifikat der VPKI beruhen und

– mit einer sicheren Signaturerstellungseinheit erzeugt werden.

Die fortgeschrittenen Signaturen unterscheiden sich damit in technischer Hinsicht und in ihrer Anwendung nicht von qualifizierten Signaturen nach dem SigG. In diesem Zusammenhang wird auch auf die in Nr. 10 AFS-HKR getroffenen Regelungen verwiesen. Unterschiede bestehen allerdings hinsichtlich der Anforderungen an die Zertifizierungsstellen und die von diesen Stellen betriebenen Zertifizierungsdienste. Auf ausdrücklichen Wunsch der kommunalen Spitzenverbände wurden hier die besonderen Strukturen der VPKI besonders berücksichtigt. Auf die im SigG und SigV enthaltenen Regelungen zur Betriebsdokumentation, Haftung, Versicherung, Dauer der Nachprüf-

barkeit und zum Datenschutz wurde weitgehend verzichtet, soweit sich nicht aus haushaltsrechtlichen Gründen besondere Anforderungen ergaben (z.B. muss die Nachprüfbarkeit von Signaturen für die Dauer der Aufbewahrungsfristen sichergestellt sein). Statt dessen wird auf die Zuverlässigkeit derjenigen Stellen vertraut, die als Zertifizierungsstellen in der PKI-Infrastruktur der öffentlichen Verwaltung (Bund, Länder, Kommunen) tätig und zugelassen sind, zumal die Maßnahmen für einen ordnungsgemäßen und sicheren Betrieb der zertifikatsbasierten Schlüsselinfrastruktur ohnehin bereits in entsprechenden Sicherheitsleitlinien (BSI) oder Sicherheitsrichtlinien (Zertifizierungs- oder Registrierungsstellen) geregelt sind. Demzufolge lassen Nr. 3 Buchst. a und b AFS-HKR für diesen besonderen Verwendungszweck nur solche Signaturschlüssel, Signaturprüfschlüssel und Zertifikate für die Erzeugung fortgeschrittener Signaturen zu, die von Zertifizierungsstellen der deutschen Verwaltungs-PKI (VPKI) erzeugt und ausgegeben werden. Die hierfür in Betracht kommenden Zertifizierungsstellen können der Homepage des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) entnommen werden. Das BSI als Wurzelzertifizierungsstelle der VPKI gibt mit seinen Sicherheitsleitlinien die technischen und organisatorischen Rahmenbedingungen für alle Diensteanbieter und Teilnehmer der VPKI vor.

Für die Nutzung von elektronischen Signaturen als Unterschriftsersatz ist die eindeutige Zuordnung der Signaturen und Zertifikate zu einer natürlichen Person unabdingbare Voraussetzung. Aus diesem Grund dürfen alle anderen im Rahmen der VPKI möglichen Alternativen (Zertifikate für juristische Personen, Personengruppen, Funktionen oder automatisierte IT-Prozesse) nicht als Ersatz für die haushaltsrechtlich vorgeschriebene Schriftform verwendet werden. Diesem Umstand wird in Nr. 3 Buchst. a letzter Satz AFS-HKR besonders Rechnung getragen.

Da die in der AFS-HKR beschriebenen fortgeschrittenen elektronischen Signaturen nur in verwaltungsinternen Systemen zum Einsatz kommen sollen, ist deren Verwendung ausschließlich auf den innerdienstlichen Gebrauch beschränkt. Insoweit hat Nr. 3 Buchst. b AFS-HKR lediglich deklaratorische Bedeutung und soll eine Kollision mit vorrangigen Rechtsvorschriften (vgl. Ziff. 1.2 der Begründung) ausschließen. Es wird den Kommunen empfohlen, diese Verwendungsbeschränkung im Zertifikat festzuhalten.

2.4 zu Nr. 4 Zertifizierungsstellen

Die Regelung verdeutlicht, dass sich der Betrieb der Zertifizierungsstellen an den Sicherheitsleitlinien des BSI orientieren muss und hiervon nicht abgewichen werden darf. Damit wird ein sicherer und ordnungsgemäßer Betrieb der Zertifizierungsdienste innerhalb der VPKI sichergestellt, da das BSI mit seiner Kompetenz und Erfahrung einen zuverlässigen Garanten für die Qualität und den Umfang der notwendigen Sicherungsmaßnahmen darstellt. Dies trägt erheblich zur Vertrauenswürdigkeit der innerhalb der VPKI ausgestellten Zertifikate und Signaturschlüssel bei. Von wesentlicher Bedeutung für die haushaltsrechtliche Akzeptanz der fortgeschrittenen Signaturen als Schrift-

formersatz ist außerdem die Tatsache, dass das BSI seine Leitlinien für die VPKI (Sicherheitsleitlinien in Verbindung mit einem entsprechenden Zertifikatsprofil) an dem SigG ausrichtet. Die Einhaltung dieser Anforderungen durch die teilnehmenden Zertifizierungsstellen wird vom BSI über entsprechende vertragliche Vereinbarungen sichergestellt.

Weitergehende Anforderungen, wie sie im SigG und in der SigV für die Zertifizierungsdienstanbieter gesetzlich geregelt sind, werden innerhalb der VPKI nicht für erforderlich gehalten.

2.5 zu Nr. 5 Vergabe fortgeschrittener Zertifikate

In Anlehnung an § 5 SigG und die §§ 3, 5 SigV definiert Nr. 5 AFS-HKR Mindestanforderungen, die bei der Vergabe von Zertifikaten für fortgeschrittene Signaturen zu beachten sind. Die Regelungen sollen eine sichere, zugleich aber möglichst einfache Identifikation der Signaturschlüssel-Inhaber durch die jeweiligen Registrierungsstellen sowie eine nachvollziehbare Verfahrensweise bei der Vergabe, Erzeugung und Speicherung der Zertifikate sicherstellen. Wegen der besonderen Struktur der VPKI und den größtenteils bereits eingeführten Prozessen zur Identifizierung von Personen, zum Verfahrensablauf bei der Antragstellung und der Ausstellung von Zertifikaten und Signaturschlüsseln waren einige Abweichungen vom Vergabeverfahren bei qualifizierten Zertifikaten notwendig. Die Registrierungsstellen müssen die Identifizierung des Signaturschlüssel-Inhabers nicht zwangsläufig selbst vornehmen. Die Identifikationsdaten können den Registrierungsstellen auch von einer anderen zuverlässigen Stelle (z.B. Personalbüro) auf sicherem Wege übermittelt werden. Daraus sind jedoch keine Probleme bei der Identifikation der Signaturschlüssel-Inhaber oder der eindeutigen Zuordnung von Zertifikat und Signaturschlüssel zu einer natürlichen Person zu erwarten, zumal diese Prozesse stets innerhalb der geschlossenen Benutzergruppe „öffentliche Verwaltung“ stattfinden. Insoweit kann von einer zuverlässigen und ordnungsgemäßen Abwicklung dieser Prozesse ausgegangen werden.

Eine Registrierungsstelle kann für eine oder mehrere Kommunen und deren Einrichtungen tätig werden.

Im Vorgriff auf die künftige Struktur der bayerischen VPKI wurde in Nr. 11 AFS-HKR auch der Begriff „Produktionsstelle“ eingeführt. Diese Produktionsstellen können, insbesondere bei der erstmaligen Antragstellung, im Auftrag der originär zuständigen Registrierungsstelle den Personalisierungsprozess übernehmen, also die für den Teilnehmer generierten Zertifikate (sog. Teilnehmer-Zertifikate) sowie die dazugehörigen persönlichen Signaturschlüssel auf sichere Signaturerstellungseinheiten (SmartCards) übertragen und die damit zusammenhängenden Prozesse (z.B. Generierung von PIN u. PUK, Bedrucken der Karte mit persönl. Identifikationsmerkmalen, Erstellen des sog. PIN-Briefes, Versand der SmartCards) vornehmen. Damit soll auch denjenigen Kom-

munen der Einsatz von fortgeschrittenen Signaturen ermöglicht werden, die zwar eine eigene Registrierungsstelle, aber keine sog. Personalisierungsstation haben.

In diesem Zusammenhang wird nochmals darauf hingewiesen, dass spätestens zu Beginn des Personalisierungsprozesses eine zuverlässige Identifikation des jeweiligen Teilnehmers (Signaturschlüssel-Inhabers) gewährleistet sein muss. Dies gilt vor allem dann, wenn die Registrierungsstelle bei der Antragstellung die von einer anderen Stelle erhobenen Daten nutzt.

2.6 zu Nr. 6 Unterrichtungspflicht

Durch die vorgeschriebene Unterrichtung wird ein Teil der mit der Schriftform bezweckten Warnfunktion auf den elektronischen Bereich übertragen und ein sorgfältiger und sicherer Umgang des Signaturschlüssel-Inhabers mit seiner Signaturkarte, der PIN und den Signaturanwendungskomponenten bezweckt. Gerade bei elektronischen Identitätsnachweisen, die der elektronischen Unterschrift dienen, kommt es wegen der möglichen Rechtsfolgen auf einen gewissenhaften Umgang mit den Speichermedien (SmartCard) und dem persönlichen Passwort (PIN) an. Ein zuverlässiger Schutz vor missbräuchlicher Nutzung ist nur dann gegeben, wenn der Signaturschlüssel-Inhaber seine SmartCard sicher verwahrt und seine PIN geheim hält. Eine Weitergabe der SmartCard und deren PIN an andere Personen käme damit einer „Blanko-Unterschrift“ auf einem herkömmlichen Dokument gleich. Wie bei allen komplexeren und sicherheitskritischen Systemen kommt es daher neben der technischen Konzeption in beträchtlichem Maß auf das Verhalten des Anwenders an. Dieser benötigt zum sachgerechten Umgang mit den zur Verfügung gestellten IT-Einrichtungen eine entsprechende Einweisung und Schulung, die mit dieser Regelung sichergestellt werden soll.

2.7 zu Nr. 7 Inhalt und Gültigkeitsdauer fortgeschrittener Zertifikate

Diese Regelung präzisiert die zwingend notwendigen und die optional möglichen Informationen, die in fortgeschrittenen Zertifikaten der VPKI hinterlegt werden müssen bzw. dürfen. Zugleich wird klargestellt, dass Pseudonyme, auch wenn sie unverwechselbar sind, nicht anstelle des Namens verwendet werden dürfen, da stets die problemlose Identifikation des Signaturschlüssel-Inhabers über das der Signatur zugrundeliegende Zertifikat möglich sein muss.

2.8 zu Nr. 8 Sperrung fortgeschrittener Zertifikate

Eine Sperrung von Zertifikaten soll nicht nur durch den Signaturschlüssel-Inhaber selbst (z.B. bei Verlust der Signaturkarte oder bei Kompromittierung des privaten Signaturschlüssels oder der Signaturerstellungseinheit), sondern auch durch den Dienst-

herrn oder Arbeitgeber oder die zuständige Registrierungsstelle möglich sein, wenn diesen Tatsachen bekannt werden, wonach eine weitere Verwendung des Zertifikats und der damit verbundenen Signaturschlüssel nicht mehr notwendig oder als zu riskant erscheint.

2.9 zu Nr. 9 Verfahren zum langfristigen Erhalt der Beweiskraft signierter Dokumente

Der Beweiswert fortgeschrittener Signaturen nimmt wegen der technischen Fortentwicklung erfahrungsgemäß ab. So kann nicht ausgeschlossen werden, dass heute als sicher erscheinende Hash- oder Verschlüsselungsalgorithmen, insbesondere aber die zugehörigen Parameter (z.B. deren Schlüssellänge), angreifbar oder manipulierbar sind. In Anlehnung an § 17 SigV wird daher in Nr. 9 AFS-HKR gefordert, dass die signierten Daten von Zeit zu Zeit neu signiert werden müssen, um deren Beweiswert zu erhalten. Auf einen qualifizierten Zeitstempel als Alternative zur erneuten fortgeschrittenen Signatur wurde an dieser Stelle bewusst verzichtet, da dieser Dienst in der VPKI grundsätzlich nicht zur Verfügung steht.

Im Interesse der Verwaltungsvereinfachung kann auf die erneute Signatur verzichtet werden, wenn die signierten Daten gemeinsam mit den Signaturdaten in sog. qualifizierten Archivsystemen (vgl. hierzu BKPV Geschäftsbericht 2004) aufbewahrt werden. Die strengen haushaltsrechtlichen Anforderungen an qualifizierte Archivsysteme (vgl. § 71 Abs. 2 KommHV-Kameralistik bzw. § 67 Abs. 2 KommHV-Doppik i. V. m. Nr. 3.2 der Finanzplanungsbekanntmachung 2008) stellen die Unveränderbarkeit der Daten sicher, so dass die Gefahr von Manipulationen ausgeschlossen werden kann, solange die originären Daten/Signaturen darin aufbewahrt werden.

Die mit der Transformation von Daten zusammenhängenden Fragen regelt Nr. 9 Buchst. b AFS-HKR. Hier ist schon aus technischen Gründen eine erneute Signatur der Daten unumgänglich, zumal die Daten nach der Transformation zwangsläufig zu anderen Hashwerten führen.

2.10 zu Nr. 10 Produkte für fortgeschrittene elektronische Signaturen

Durch den Verweis auf § 17 Abs. 1 und 2 SigG in Nr. 10 Buchst. a und b AFS-HKR wird sichergestellt, dass für die Erzeugung von fortgeschrittenen Signaturen nur geprüfte und ausreichend sichere Komponenten verwendet werden. Dies trägt entscheidend zur Vertrauenswürdigkeit von fortgeschrittenen Signaturen bei, da damit wesentliche Elemente der händischen Unterschrift (Warn-, Hinweis-, Perpetuierungsfunktion) sichergestellt sind und die Nicht-Abstreitbarkeit der elektronischen Signaturen gewährleistet ist. Zugleich wird damit klargestellt, dass im Bereich des kommunalen Haus-

halts-, Kassen- und Rechnungswesens keine rein softwarebasierte Lösung als Signaturerstellungseinheit eingesetzt werden kann.

Erleichterungen wurden hinsichtlich der verwendeten Visualisierungskomponenten und Signaturanwendungskomponenten eingeräumt. Hier genügt eine entsprechende Erklärung des Herstellers oder Lieferanten, dass die eingesetzten Visualisierungskomponenten die Anforderungen des § 17 Abs. 2 SigG und die Signaturanwendungskomponenten mindestens die Sicherheitsstufe EAL 4+ der Common Criteria (CC) erfüllen. Eine separate, landesspezifische Prüfung oder Zertifizierung dieser Komponenten ist deshalb nicht erforderlich.

Für sichere Signaturanwendungskomponenten im Sinne von Nr. 10 Buchst. c AFS-HKR gelten § 17 Abs. 2 SigG i. V. m. § 15 Abs. 2 SigV entsprechend. Was die Auslegung und Anwendung dieser Vorschrift betrifft, kann somit ohne weiteres auf die Begründung des Gesetzgebers zu § 15 SigV zurückgegriffen werden. Danach kann auch bei sicheren Signaturanwendungskomponenten die Eingabe der notwendigen Identifikationsdaten (z.B. PIN, biometrisches Merkmal) auf die Arbeitsabläufe der Signierenden hin angepasst werden, so dass der Nutzer (Signaturschlüssel-Inhaber) diese auf seine individuellen Bedürfnisse einstellen kann. Die Begründung zur SigV nennt folgende (optional) möglichen Einstellungen für die Eingabe der Identifikationsdaten:

– vor jeder Signatur

– nach einer zuvor festgelegten Anzahl von Signaturen oder

– nach bestimmtem Zeitablauf bei Nichtbenutzung der Signaturerstellungseinheit

Bei entsprechender Gestaltung der Signaturanwendungskomponenten liegt es daher im pflichtgemäßen Ermessen des Unterschriftsberechtigten, wann und wie oft er vor der Erzeugung von elektronischen Signaturen seine persönlichen Identifikationsdaten eingibt. Unter anderem lässt sich auf diese Weise auch die von Anwenderseite oftmals geforderte Signatur von mehreren, aufeinander folgenden elektronischen Anordnungen realisieren (sog. Stapelsignatur). Damit aber auch bei solchen Verfahrensweisen die Warn- und Hinweisfunktion der Unterschrift erhalten bleibt, muss die Signaturanwendungskomponente gewährleisten, dass dem Signierenden sämtliche zu signierenden Daten vorher angezeigt werden und er deren Kenntnisnahme auch bestätigt. Vorstellbar ist hier eine Verfahrensweise, wie sie häufig bei elektronischen Lizenzverträgen angewandt wird (z.B. vor Installation von Betriebssystemen oder Software), bei denen erst nach dem „Durchblättern“ aller Seiten der Lizenzbestimmungen eine entsprechende Bestätigung und Fortsetzung des Vorgangs möglich ist. Eine vergleichbare Lösung erscheint auch aus Sicht der Verfahrens- und Kassensicherheit notwendig und zweckmäßig, da Stapelsignaturen sonst das gewünschte „Vier-Augen-Prinzip“ und die damit verbundenen Kontrollfunktionen aushebeln könnten.

2.11 zu Nr. 11 Begriffsbestimmungen

Im Rahmen der AFS-HKR wurden grundsätzlich die Begriffsbestimmungen des SigG und die SigV verwendet und darauf verwiesen. Damit wird nicht nur die Lesbarkeit der getroffenen Regelungen erleichtert. Der einheitliche Sprachgebrauch fördert auch das Verständnis der Softwarehersteller und Lieferanten für die jeweiligen Festlegungen und lässt eine einheitliche Umsetzung erwarten. Insgesamt trägt dies auch zur Standardisierung und technischen Kompatibilität der unterschiedlichen Signaturlösungen bei.

Im Hinblick auf die speziellen Strukturen der VPKI und zum besseren Verständnis der in der AFS-HKR getroffenen Regelungen sind darüber hinaus einige technische und organisatorische Begrifflichkeiten definiert, soweit dies notwendig und zweckmäßig erschien.