Begründung zur AFS-HKR

Inhalt

1. Allgemeiner Teil

1.1 Ausgangslage

Mit Inkrafttreten des Gesetzes zur Durchführung der eIDAS-VO (eIDAS-Durchführungsgesetz) ist das bisher geltende nationale Signaturrecht (SigG u. SigV) außer Kraft getreten. Anstelle des nationalen Signaturrechts bildet inzwischen die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung oder kurz eIDAS-VO) einen europäischen Rechtsrahmen, unter den auch die elektronischen Signaturen als Teil der Vertrauensdienste fallen (vgl. Art. 1 Buchst. c i.V. mit Art. 3 Nr. 16 eIDAS-VO).

Als unmittelbar geltendes Unionsrecht bedarf die eIDAS-VO hinsichtlich ihrer materiellen Vorschriften grundsätzlich keiner Umsetzung in nationales Recht. Da die eIDAS-VO gem. Artikel 2 Abs. 2 bei Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht verwendet werden, nicht anwendbar ist, gelten deren materiell-rechtliche Regelungen allerdings nicht automatisch für elektronische Signaturen im Bereich des internen Haushalts-, Kassen- und Rechnungswesens einer Kommune.

Aufgrund der herausragenden Bedeutung, die die im Haushaltsrecht vorgeschriebenen Wissens- und Willenserklärungen für die Ausführung und Kontrolle von finanzwirksamen Vorgängen, insbesondere die ordnungsmäßige Abwicklung von Zahlungsvorgängen und die Ausführung von Kassenanordnungen haben, wird hierfür bei ausschließlich elektronisch abgewickelten Prozessen ein zuverlässiges, sicheres und beweiskräftiges elektronisches Mittel als Unterschriftsersatz benötigt, das der Verwender mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

Aus vorstehenden Gründen verweist die AFS-HKR hinsichtlich der fortgeschrittenen elektronischen Signaturen auf grundlegende Begriffe und Anforderungen der eIDAS-VO. Zudem dient die Referenzierung auf die eIDAS-VO der einheitlichen Verwendung bereits legaldefinierter Begriffe und stellt zugleich sicher, dass an fortgeschrittene elektronische Signaturen gleichartige Anforderungen gestellt werden, unabhängig davon, ob diese von Teilnehmern des Binnenmarkts oder nur im innerdienstlichen Bereich eingesetzt werden. Eine weitergehende Anwendung der eIDAS-VO wird dagegen mit Blick auf Erwägungsgrund 21 der eIDAS-VO ausgeschlossen.

Die dadurch entstehende Regelungslücke, z.B.

- zum Aufbau und Inhalt fortgeschrittener elektronischer Zertifikate,
- zum Schutz der fortgeschrittenen Signaturerstellungsdaten,
- zu den Signaturerstellungseinheiten für fortgeschrittene Signaturen,
- zur Absicherung des Signaturerstellungsprozesses und
- zum Betrieb der Zertifizierungsdienste.

kann durch entsprechende Regelungen in der AFS-HKR und Verweise auf die vom IT-Dienstleistungszentrum des Freistaats Bayern erstellte Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung für die X.509-Zertifizierungshierarchie innerhalb der deutschen Verwaltungs-PKI (Bayerische Verwaltungs-PKI) geschlossen werden.

Mit der Verordnung zur Änderung der Kommunalhaushaltsverordnungen vom 20.07.2018 (GVBl Nr. 15, S. 672) wurde aus den vorstehenden Gründen auf die beiden in der eIDAS-VO enthaltenen Legaldefinitionen für fortgeschrittene und qualifizierte Signaturen verwiesen, da die bisherigen Verweise sonst ins Leere gehen würden. Daneben wurde in der o.g. Änderungsverordnung neben der elektronischen Signatur der Feststellungsbescheinigungen und Kassenanordnungen nun auch die elektronische Signatur der Tagesabschlüsse/Tagesabgleiche zugelassen, um in diesem Bereich ebenfalls eine medienbruchfreie elektronische Abwicklung zu gewährleisten.

Bei Festlegung der haushaltsrechtlichen Anforderungen an fortgeschrittene Signaturen ist zu berücksichtigen, dass automatisierte Verfahren, die dem Haushalts-, Kassen- und Rechnungswesen dienen, in der Regel in besonders abgesicherten lokalen Netzwerken ablaufen und ausschließlich interne Verwaltungsprozesse unterstützen (z.B. die Ermittlung und Prüfung von Ansprüchen oder Zahlungsverpflichtungen, die Buchführung und den Zahlungsverkehr). Zudem werden diese Verfahren von einer geschlossenen Benutzergruppe (Beschäftigte mit entsprechender Zugangsberechtigung) genutzt. Hinzu kommen die beim Einsatz solcher Verfahren zu beachtenden haushaltsrechtlichen Sicherheitsanforderungen (vgl. § 37 KommHV-Kameralistik, § 33 KommHV-Doppik). Insoweit bestehen im Regelfall geringere Risiken als bei einer elektronischen Kommunikation mit Externen. Gleichwohl sind im Hinblick auf die Ordnungsmäßigkeit des Haushalts-, Kassen- und Rechnungswesens, die Kassensicherheit und die Nachvollziehbarkeit der Buchungen anhand von elektronischen Belegen ergänzende Regelungen notwendig, die den Einsatz von fortgeschrittenen elektronischen Signaturen in diesem Bereich einheitlich regeln und revisionssicher gestalten.

1.2 Zielsetzung und Gegenstand

Die neue AFS-HKR enthält in Abstimmung mit den Bayerischen Kommunalen Spitzenverbänden nur noch Mindestanforderungen an den Einsatz von fortgeschrittenen Signaturen im Sinne von § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik. Damit soll neben einer Verwaltungsvereinfachung eine größere Flexibilisierung bei der Umsetzung örtlicher Anforderungen, mehr Raum für die Gestaltung von elektronischen Verwaltungsprozessen und eine leichtere Anpassung an technische Entwicklungen (z.B. Virtual Token- oder Virtual Smartcard-Konzepte oder Fernsignaturlösungen) erreicht werden.

Nach den langjährigen Erfahrungen des Bayerischen Kommunalen Prüfungsverbandes beim Einsatz von automatisierten Verfahren i. S. von § 37 Abs. 1 KommHV-Kameralistik, § 33 Abs. 1 KommHV-Doppik ist nur bei Einsatz von fortgeschrittenen oder qualifizierten elektronischen Signaturen sichergestellt, dass

- die signierten Daten (z.B. Belege) samt den Signaturdaten verkehrsfähig sind,
- der Unterzeichner auch unabhängig vom Verfahren für das Haushalts-, Kassen- und Rechnungswesen (HKR-Verfahren) identifiziert werden kann,
- die Integrität der signierten Daten manuell und auch automatisch mit allgemein zugänglichen, meist kostenfreien Werkzeugen (z.B. PDF-Viewer, Signaturprüfprogrammen) überprüft und eine nachträgliche Veränderung der Daten erkannt werden kann,
- die Verknüpfung der elektronischen Signatur zu den signierten Daten auch bei einem Verfahrenswechsel, bei etwaigen Datenverlusten oder einem Verlust der referentiellen Integrität erhalten bleibt,
- die signierten Daten gemeinsam mit den Signaturen auf einem nachträglich nicht veränderbaren Speichermedium und damit unabhängig vom HKR-Verfahren gespeichert werden können,
- sie internationalen technischen Normen entsprechen.

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 der AFS-HKR in erster Linie von den Vertrauensdiensteanbietern und den Herstellern automatisierter Verfahren zu berücksichtigen.

Mittelbar können sich für die Kommunen zwar Kosten bei der Einführung ergeben (z.B. bei der Umstellung und dem laufenden Betrieb). Es ist aber davon auszugehen, dass die mit den elektronischen Verwaltungsprozessen einhergehenden Nutzenpotentiale

diesen Aufwand deutlich übersteigen und mittel- bis langfristig zur Wirtschaftlichkeit des elektronischen Anordnungswesens führen. In diesem Zusammenhang wird auf die Einspareffekte verwiesen, die allein schon mit dem Empfang und der Verarbeitung strukturierter, maschinell verarbeitbarer elektronischer Rechnungen einhergehen können (vgl. u.a. „eRechnung - Handlungsempfehlungen zur Umsetzung des elektronischen Rechnungsaustauschs mit der öffentlichen Verwaltung, Hrsg.: BMI und Goethe Universität, Frankfurt a.Main). Zudem wird bei medienbruchfreien digitalen Prozessen den Risiken begegnet, die bei Medienbrüchen/Transformationen (z.B. dem Ausdruck von elektronischen Dokumenten) latent vorhanden sind (z.B. Verlust elektronischer Sicherungsmerkmale und Zugriffskontrollen).

2. Besonderer Teil

2.1 Zu Nr. 1 - Präambel

Die Regelung verdeutlicht, dass bereits fortgeschrittene elektronische Signaturen mit bestimmten Qualitätsmerkmalen die haushaltsrechtlich vorgeschriebene Schriftform ersetzen können. Die verwendeten fortgeschrittenen Signaturen müssen eine sichere Identifizierung des Unterzeichners und eine zuverlässige Prüfung der Integrität und Authentizität 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 Unterzeichner mit einem hohem Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Diese Anforderungen sind bei der Freigabe automatisierter Verfahren i.S. von § 37 Abs. 1 Nr. 1 KommHV-Kameralistik, § 33 Abs. 1 Nr. 1 KommHV-Doppik entsprechend zu berücksichtigen.

Die bisherigen (hohen) Anforderungen an die Aufbewahrungsmedien für die Signaturerstellungsdaten und die Signaturerstellungseinheiten werden mit Blick auf die liberaleren Anforderungen der eIDAS-VO, die technische Weiterentwicklung (z.B. Cryptography API Next Generation, Virtual-Smart-Card oder Virtual-Token Konzepte) und ebenso aus Revisionssicht nicht mehr als erforderlich angesehen. So gelten zum einen auch für den sog. elektronischen Anordnungsworkflow die haushaltsrechtlichen Sicherheitsanforderungen (vgl. § 37 Abs. 1 Nrn. 2 bis 10 KommHV-Kameralistik, § 33 Abs. 1 Nrn. 2 bis 10 KommHV-Doppik), so dass beim Einsatz von finanzwirksamen Verfahren in der Praxis ohnehin von einem höheren Sicherheitsniveau ausgegangen werden kann. Zum anderen soll damit den Bemühungen der bayerischen Kommunen Rechnung getragen werden, die mit der Einführung von Managementsystemen für Informationssicherheit (ISMS, z.B. nach den BSI- Standards, ISO/IEC 27001, ISIS12 oder vergleichbaren, anderen Konzepten) sowie den daraus resultierenden Informationssicherheitskonzepten nach Art. 11 Abs. 1 BayEGovG stetige Verbesserungen ihrer informationstechnischen Systeme anstreben.

2.2 Zu Nr. 2 - Zweck und Geltungsbereich

Die Beschränkung auf Mindest-Anforderungen, die ausdrückliche Zulassung von Software-Zertifikaten und weiteren Zertifikatsspeichern soll eine noch leichtere Implementierung und Handhabung der elektronischen Signaturen im Haushalts-, Kassen- und Rechnungswesen erlauben.

Mit Blick auf die in § 371a Abs. 3 Satz 1 ZPO festlegten Beweisregeln sollen die fortgeschrittenen elektronischen Signaturen vor allem die Integrität, Authentizität und Verkehrsfähigkeit der damit signierten elektronischen Dokumente erhöhen. Allerdings unterliegt die Echtheit der fortgeschritten signierten Dokumente im Zweifel der freien richterlichen Beweiswürdigung (vgl. § 286, § 371 Abs. 1 Satz 2 i.V. mit § 371a Abs. 3 Satz 2 ZPO). Die elektronisch signierten Wissens- und Willenserklärungen dürften aber zumindest als beweiswerterhöhend angesehen werden.

2.3 Zu Nr. 3 - Eigenschaften der fortgeschrittenen elektronischen Signatur

Die fortgeschrittenen elektronischen Signaturen müssen die in Art. 26 eIDAS-VO genannten Anforderungen erfüllen und unterscheiden sich insoweit nicht von den ersten beiden Stufen qualifizierter Signaturen nach der eIDAS-VO.

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 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. b 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 (Nr. 3 Buchst. c AFS-HKR). Dies wird zusätzlich durch die Regelung in Nr. 3.1.3 der Zertifizierungsrichtlinie der Bayerischen Verwaltungs-PKI sichergestellt.

2.4 Zu Nr. 4 - Zertifizierungsstellen

Die Regelung verdeutlicht, dass sich der Betrieb der Zertifizierungsstellen an den Sicherheits- und Zertifikatsrichtlinien der V-PKI orientieren muss und hiervon nicht abgewichen werden darf. Damit soll ein sicherer, ordnungsmäßiger und ordnungsgemäßer Betrieb der Zertifizierungsdienste sichergestellt werden, was erheblich zur Vertrauens-

würdigkeit der im Haushalts-, Kassen- und Rechnungswesen verwendeten elektronischen Zertifikate und Signaturschlüssel beiträgt.

Die Erweiterung des Kreises der möglichen Zertifizierungsstellen ist dem Umstand geschuldet, dass ca. 30 bis 40 % der bayerischen Kommunen und zahlreiche kommunale Einrichtungen nicht an das BYBN angeschlossen sind. Zugleich soll diese Öffnung größeren Kommunen ermöglichen, den Zertifizierungsdienst selbst zu betreiben. Voraussetzung hierfür ist allerdings, dass dieser Dienst vergleichbar den Sicherheits- und Zertifikatsrichtlinien der V-PKI, insbesondere den hohen Sicherheitsstandards der Bayerischen Verwaltungs-PKI betrieben wird, das Sicherheitsniveau vergleichbar und auf Policy-Ebene überprüfbar ist und hierüber eine entsprechende Selbsterklärung vorliegt. Eine Zertifizierung durch die Wurzelzertifizierungsinstanz der deutschen Verwaltungs-PKI oder die Mitgliedschaft in der EBCA ist dagegen nicht zwingend erforderlich.

Weitergehende Anforderungen, wie sie in der eIDAS-VO für die Zertifizierungsdienstanbieter gesetzlich geregelt sind, werden für den internen Anwendungsbereich nicht für erforderlich gehalten.

2.5 Zu Nr. 5 - Vergabe fortgeschrittener Zertifikate

Nr. 5 AFS-HKR definiert Mindestanforderungen, die bei der Vergabe von Zertifikaten für fortgeschrittene Signaturen zu beachten sind. Die Regelungen sollen eine sichere, zugleich aber möglichst einfache Identifikation der Unterzeichner (Zertifikatsteilnehmer bzw. Signaturschlüssel-Inhaber) durch die jeweiligen Registrierungsstellen sowie eine nachvollziehbare Verfahrensweise bei der Vergabe, Erzeugung und Speicherung der Zertifikate sicherstellen. Die Registrierungsstellen müssen die Identifizierung der Unterzeichner 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 keine Probleme bei der Identifikation der Unterzeichner oder der eindeutigen Zuordnung von Zertifikat und des Signaturschlüsselpaares 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.

Aus Gründen des Investitionsschutzes und um diese Option nach wie vor anzubieten, können die in Nr. 11 AFS-HKR definierten Produktionsstellen 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 Smartcards übertragen und die damit

zusammenhängenden Prozesse (z.B. Generierung von PIN u. PUK, Bedrucken der Karte mit persönlichen Identifikationsmerkmalen, Erstellen des sog. PIN-Briefes, Versand der Smartcards) vornehmen. Damit soll auch denjenigen Kommunen der Einsatz von fortgeschrittenen Signaturen auf Basis von Smartcards 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 (Unterzeichners bzw. 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 sicherer Umgang des Unterzeichners mit seinen Signaturerstellungsdaten bezweckt. Gerade bei elektronischen Signaturen kommt es wegen der möglichen Rechtsfolgen auf eine sichere Aufbewahrung des privaten Signaturschlüssels und einen gewissenhaften Umgang mit dem persönlichen Passwort (PIN) an, mit dem der jeweilige Signaturvorgang autorisiert wird. Ein zuverlässiger Schutz vor missbräuchlicher Nutzung ist insbesondere bei Software-Token nur dann gegeben, wenn der Unterzeichner seine PIN entsprechend sicher gestaltet (komplexes Passwort mit mind. 10 - 12 Stellen, vgl. IT-Grundschutz-Kompendium, Basis-Anforderung ORP.4.A8 „Regelung des Passwortgebrauchs“) und diese dann auch geheim hält. Wie bei allen 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 Informationen, die in den fortgeschrittenen elektronischen Zertifikaten hinterlegt werden müssen. Zugleich wird klargestellt, dass Pseudonyme, auch wenn sie unverwechselbar sind, nicht anstelle des Namens verwendet werden dürfen, da stets die problemlose Identifikation des Unterzeichners 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 Sig-

naturschlüssels oder der Signaturerstellungseinheit), sondern auch durch den Dienstherrn 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. Schlüssellänge), angreifbar oder manipulierbar sind. In Anlehnung an die vom BSI veröffentlichte technische Richtlinie TR-03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) 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 fortgeschrittenen oder qualifizierten Zeitstempel als Alternative zur erneuten fortgeschrittenen Signatur wurde an dieser Stelle bewusst verzichtet, da dieser Dienst in der V-PKI grundsätzlich nicht zur Verfügung steht.

Im Interesse der Verwaltungsvereinfachung kann allerdings auf die erneute Signatur verzichtet werden, wenn die signierten Daten gemeinsam mit den Signaturdaten in einer Weise gespeichert werden, dass deren Unveränderbarkeit gewährleistet ist. Die strengen haushaltsrechtlichen Anforderungen an die Aufbewahrung elektronischer Belege (vgl. § 71 Abs. 2 KommHV-Kameralistik, § 67 Abs. 2 KommHV-Doppik) stellen dies 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. c 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 - Anforderungen an Produkte für fortgeschrittene elektronische Signaturen

Der vom IT-Dienstleistungszentrum des Freistaats Bayern im Rahmen der Bayerische Verwaltungs-PKI betriebene Zertifizierungsdienst hat sich als sichere und zuverlässige Lösung bewährt. Die Regelung in Nr. 10 Buchst. a AFS-HKR bezweckt, dass die bewährten Standards für die Schlüsselerzeugung, Installation, Aufbewahrung und Ma-

nagement der Schlüssel auch durch eine andere Zertifizierungsstelle (vgl. Nr. 4 AFS-HKR) eingehalten werden müssen.

Die Regelung in Nr. 10 Buchst. b AFS-HKR kommt dem Wunsch der kommunalen Spitzenverbände und vieler Kommunen nach einer leichteren und kostengünstigeren Umsetzbarkeit von elektronischen Signaturen entgegen. Die bisherige Forderung nach einer Zwei-Faktor-Authentisierung und Speicherung der Signaturerstellungsdaten auf einem sicheren Hardware-Token war dem nationalen SigG geschuldet, da dort auch bei fortgeschrittenen Signaturen gefordert war, dass diese mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann (vgl. § 2 Nr. 2 Buchst. c SigG, galt bis 28.07.2017). Hiervon weicht die neue gesetzliche Regelung in Art. 26 Buchst. b eIDAS-VO deutlich ab. Es genügt, wenn der Unterzeichner (vgl. Art. 3 Nr. 9 eIDAS-VO) die elektronischen Signaturerstellungsdaten (vgl. Art. 3 Nr. 13 eIDAS-VO) mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle halten kann. Davon ist grundsätzlich auszugehen, wenn die zuständige Stelle den Beschäftigten ein geeignetes, fachlich geprüftes Programm anbietet und dieses unter Berücksichtigung der in § 37 Abs. 1 Nr. 2 bis 6 KommHV-Kameralistik, § 33 Abs. 1 Nr. 2 bis 6 KommHV-Doppik genannten Sicherheitsanforderungen als automatisiertes Verfahren für den Einsatz im Wirkbetrieb freigibt.

Zugleich dient die Zulassung von Software-Token und von zentralen (Fern-)Signaturlösungen der Verwaltungsmodernisierung, da sich damit noch leichter (medienbruchfreie) elektronische Verwaltungsprozesse und plattformunabhängige Lösungen realisieren lassen. Andererseits sind auf der Basis von Hardware-Token oder multifunktionalen Signaturkarten nach wie vor weitere Anwendungslösungen denkbar, die bei entsprechenden örtlichen Anforderungen über eine reine Signaturlösung hinausgehen (z.B. elektronischer Dienstausweis, Zutritts- und Zugangskontrolle, Zeiterfassung, Single-Sign-On an IT-Systemen und automatisierten Verfahren).

Die Regelungen in Nr. 10 Buchst. c und Buchst. d dienen insb. dem Schutz der Vertraulichkeit der privaten Signaturschlüssel und der sicheren Erstellung der elektronischen Signaturen. Der Unterzeichner muss diesen Schutzmaßnahmen vertrauen können und die alleinige Kontrolle über seinen privaten Signaturschlüssel haben. Dies ist durch geeignete, dem Schutzbedarf angemessene technische und organisatorische Maßnahmen sicherzustellen. Wenn für eine Vielzahl von Benutzern die Signaturerstellungsdaten auf zentralen Komponenten gespeichert sind und die fortgeschrittenen elektronischen Signaturen auch dort erzeugt werden sollen, ergibt sich schon durch die Vielzahl der dort verwalteten Signaturerstellungsdaten ein erhöhter Schutzbedarf, der grundsätzlich den Einsatz eines kryptographischen Moduls erfordert. Insoweit kommt der Sicherheit dieser Komponenten eine erhöhte Bedeutung zu, da sie als vertrauensbildende Maßnahme dient. Die Forderung nach einer geeigneten Sicherheitszertifizierung des kryptographischen Moduls soll dies unterstreichen.

In Anlehnung an die bisherigen Regelungen zur Verwendung fortgeschrittener Signaturen im Haushalts-, Kassen- und Rechnungswesen soll auch die Erzeugung mehrerer fortgeschrittener Signaturen bei einmaliger PIN-Eingabe zugelassen werden. Unter anderem lässt sich auf diese Weise auch die von der 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 gewährleistet sein, dass dem Unterzeichner sämtliche zu signierenden Daten vorher angezeigt werden, er deren Kenntnisnahme bestätigt und sich die im Stapel erstellten Signaturen nur auf die zuvor angezeigten Daten beziehen. Vorstellbar ist eine Verfahrensweise, wie sie häufig bei elektronischen Lizenzverträgen angewandt wird, 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 Kontroll- und Hinweisfunktionen aushebeln könnten.

2.11 Zu Nr. 11 - Begriffsbestimmungen

In der AFS-HKR wurde bei grundlegenden Begriffen die Begriffsbestimmungen der eIDAS-VO verwendet und darauf verwiesen. Damit wird ein einheitlicher Sprachgebrauch bezweckt, der auch das Verständnis der verantwortlichen Stellen, Softwarehersteller und -lieferanten für die jeweiligen Festlegungen fördert und eine einheitliche Umsetzung erwarten lässt. Insgesamt dürfte dies zur Standardisierung und technischen Kompatibilität der unterschiedlichen Signaturlösungen beitragen.