Bayerischer Kommunaler Prüfungsverband

FAQ-Beitrag

Elektronischer Signatur- und Anordnungsworkflow

Prüfungserfahrungen, Praxisfragen und Handlungsempfehlungen

Verfasser: Bernd Schricker, Herbert Gruschka

Stand: 09.08.2023

Dieser Beitrag möchte die Prüfungserfahrungen und Fragestellungen aus der Praxis zum aktuellen Thema „Elektronischer Signatur- und Anordnungsworkflow“ in den Mittelpunkt stellen. Thematisiert werden die zu beachtenden gesetzlichen Rahmenbedingungen, die erforderlichen technischen und organisatorischen Maßnahmen sowie Handlungsempfehlungen zur Umsetzung.

Inhaltsübersicht Seite

1 Vorbemerkung 4

2 Elektronischer Rechnungseingang und elektronischer Anordnungsworkflow 6

2.1 Regelungen für das Haushalts-, Kassen- und Rechnungswesen 8

2.1.1 Was muss ich in meiner Dienstanweisung (DA) für das Finanz- und Kassenwesen ergänzen bzw. neu regeln? 8

2.1.2 Muss ich meine bestehenden Regelungen zur elektronischen Belegarchivierung (DA-Scan) anpassen? 10

2.2 Eingang und Verarbeitung von elektronischen Rechnungen 11

2.2.1 Wer ist zuständig für den Empfang und die Übernahme der Eingangsrechnungen? 11

2.2.2 Dürfen elektronische Rechnungen ausgedruckt werden? 13

2.3 Elektronisches Rechnungseingangsbuch 16

2.3.1 Wie erhöhe ich den Anteil an digitalen Rechnungen, um von einer automatisierten Verarbeitung zu profitieren? 16

2.3.2 Welche flankierenden Maßnahmen bieten sich an, um die ordnungsgemäße Übernahme von elektronischen Rechnungen zu gewährleisten? 17

2.3.3 Wie kann ich die Leitweg-ID im Workflow nutzen? 21

2.4 Elektronischer Anordnungsworkflow 24

2.4.1 Welche Kassenanordnungen sollten über den elektronischen Anordnungsworkflow abgewickelt werden? 24

2.4.2 Ist es zulässig, im Workflowsystem nach dem Prüfschritt „Anordnen“ die Belege automatisiert zu buchen? 25

2.4.3 Wie kann ich die Anforderungen nach § 2b UStG organisatorisch beim Anordnungsworkflow berücksichtigen? 27

2.4.4 Wie binde ich meine nicht an das lokale Netzwerk angeschlossenen Außenstellen/Einrichtungen in den Anordnungsworkflow ein? 29

2.5 Aufbewahrung von Belegen 30

2.5.1 Was bedeutet revisionssichere Aufbewahrung in einem elektronischen Belegarchiv? 31

2.5.2 Was gilt bei der Aufbewahrung der papiergebundenen Originalbelege? 34

2.5.3 Welche Anforderungen sind beim elektronischen Belegarchiv im Outsourcing-Betrieb zu beachten? 36

2.5.4 Welche Anforderungen gelten hinsichtlich der Belegrecherche? 37

3 Elektronische Signaturen im Haushalts-, Kassen- und Rechnungswesen 40

3.1 Vor- und Nachteile verschiedener Signaturlösungen 40

3.1.1 Was ist beim Betrieb einer eigenen Zertifikatsinfrastruktur zu beachten? 43

3.1.2 Unter welchen Voraussetzungen kann ich die Signatur-Zertifikate der Bayern-PKI nutzen? 44

3.1.3 Können Fernsignaturdienste verwendet werden? 48

3.2 Ordnungsgemäßer Einsatz elektronischer Signaturen und deren Nachprüfbarkeit 50

3.2.1 Wie kontrolliere ich, ob die elektronischen Signaturen von Kassenanordnungen gültig sind? 51

3.2.2 Welche Anforderungen gelten beim Einsatz von Software-Token? 53

3.2.3 Welche Regelungen sind beim Einsatz fortgeschrittener Signaturen zu erlassen? 54

3.2.4 Welche Vorgehensweise empfiehlt sich für eine ordnungsgemäße Nutzung von Stapel- bzw. Komfortsignaturen? 56
3.2.5 Ist eine Benutzeranmeldung mit Passwort und Protokollierung der Benutzeraktivitäten als Unterschriftsersatz erlaubt? 58
3.2.6 Müssen Eigenbetriebe, Körperschaften oder Einrichtungen, für die § 10 Abs. 1 Satz 3 EBV gilt, ebenfalls elektronische Signaturen verwenden? 60
3.3 Elektronische Signaturen beim Electronic Banking 62
3.3.1 Erfüllen EBICS-Signaturen die haushaltsrechtlichen Anforderungen? 63
3.3.2 Können beim Electronic Banking anstelle des signaturbasierten EBICS oder FinTS/HBCI auch andere Sicherheitsverfahren und -medien als Ersatz für die Unterschriften der Einreicher eingesetzt werden? 65
4 Anlage 1 - Muster-Dienstanweisung zum Einsatz fortgeschrittener elektronischer Signaturen im Haushalts-, Kassen- und Rechnungswesen 67
1. Allgemeines/Präambel 67
2. Geltungsbereich 67
3. Zertifizierungsstelle 68
4. Registrierungsstelle 68
5. Antragsverfahren 68
6. Rechte und Pflichten der Zertifikatsnehmer 69
7. Anzeige und Prüfung von Signaturdaten 70
8. Widerruf, Sperren und Löschen von Signaturzertifikaten 71
9. Inkrafttreten 72

Hinweis

Der Beitrag gibt die persönliche Meinung der Autoren für die zum Zeitpunkt der Beitragserstellung geltende Rechtslage wieder und greift dabei lediglich einzelne Aspekte aus dem sehr weitreichenden, dynamischen Themenumfeld auf. Dabei konnte auf besondere Umstände einzelner Fallkonstellationen nicht eingegangen werden. Diese können im Einzelfall zu abweichenden Betrachtungsweisen und Ergebnissen führen. Der Beitrag kann daher eine rechtliche oder steuerliche Beratung im Einzelfall nicht ersetzen. Es empfiehlt sich, eine auf die jeweiligen Umstände zugeschnittene Beratung einzuholen, bevor Entscheidungen über die in diesem Beitrag aufgegriffenen Themen getroffen werden. Zudem bleibt die Entscheidungspraxis der Finanz- bzw. der Steuerverwaltung und Gerichte abzuwarten und bei den örtlichen Entscheidungen zu berücksichtigen. Hinsichtlich der verwendeten externen Links verweisen wir auf den Disclaimer unter https://www.bkpv.de/impressum

Änderungshistorie

Übersicht der wesentlichen Inhaltsänderungen/-ergänzungen

Datum	Abschnitt	Anpassung/Ergänzung
03.11.2022		Erstellung des Beitrags
22.02.2023	Nr. 3.2.6	Verweise in Fn. 159
	Nr. 3.1.3	Anforderungen beim Einsatz von Fernsignaturen konkretisiert
19.06.2023	Nr. 2.2.2	Pflicht zur Annahme von digitalen Baurechnungen
	Anlage 1	Muster-Dienstanweisung (DA-Signatur) ins Gesamtdokument integriert
09.08.2023	insgesamt	Ablösung der BayEGovV durch die BayDiV zum 01.08.2023

1 Vorbemerkung

Während sich die elektronische Aufbewahrung von Kassenbelegen aufgrund der seit 01.01.2007 geltenden Kommunalhaushaltsverordnungen schon seit längerem etabliert hat, erhielten viele Projekte zur Umsetzung eines durchgängigen elektronischen Signatur- und Anordnungsworkflows erst mit der Richtlinie 2014/55/EU[1] sowie der gesetzlichen Verpflichtung zum Empfang und zur Verarbeitung von digitalen Rechnungen eine rechtliche Grundlage (Art. 18 Abs. 2 BayDiG[2] und § 8 BayDiV[3]; zur Abgrenzung der Begriffe „elektronische Rechnungen", „digitale Rechnungen" und „E-Rechnungen" vgl. die Ausführungen unter Nr. 2.2) .

Ziel der EU-Richtlinie sowie der nationalen Regelungen war es, den Prozess der Rechnungsstellung bei allen Beteiligten (rechnungsstellende Wirtschaft und öffentliche Auftraggeber) zu vereinfachen und zu beschleunigen. Durch den Einsatz ausschließlich strukturierter Rechnungsdaten, die dem in § 8 Abs. 1 Satz 1 Nr. 2 BayDiV beschriebenen europäischen Datenaustauschstandard EN 16931-1:2017 oder dem darauf aufbauenden nationalen Standard XRechnung[4] entsprechen, wird ein medienbruchfreier und friktionsloser Prozess vom Rechnungsversand bis zur Bezahlung ermöglicht. Im Zusammenspiel mit einer elektronischen Auftragsvergabe soll durch die elektronische Rechnungsstellung die bestehende Lücke in einem durchgängigen und konsistenten Prozess von der Ausschreibung bis zur Bezahlung geschlossen werden.[5]

Wir stießen daher im Rahmen unserer überörtlichen Prüfungstätigkeit verstärkt auf derartige Implementierungsprojekte. Gleichzeitig haben sich in den letzten Jahren die Anforderungen an die Digitalisierung der öffentlichen Verwaltung erheblich verändert. Dies geschah nicht nur durch gesetzliche Regelungen, sondern auch durch eigene Zielsetzungen der Behörden in Bezug auf die Digitalisierung der Verwaltungstätigkeit und die Etablierung verwaltungsökonomischer Prozesse. In diesem Zuge haben sich zudem die technischen, rechtlichen und organisatorischen Rahmenbedingungen an eine ordnungsgemäße, sichere und effiziente Buchführung verändert. Beispiele hierfür sind:

- Empfang und Verarbeitung rechtsverbindlicher elektronischer Kontoauszüge der Kreditinstitute,
- Abruf und automatisierte Buchung von Kontoauszugsinformationen (ELKO),
- neue haushaltsrechtliche Anforderungen an die Aufbewahrung elektronischer Belege,
- neue Anforderungen an den Einsatz elektronischer Signaturen im Haushalts-, Kassen- und Rechnungswesen,[6] die u.a. den Einsatz von Software-Token oder Fernsignaturdiensten für fortgeschrittene elektronische Signaturen ermöglichen,

[1] Richtlinie 2014/55/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen.
[2] Art. 18 Abs. 2 des Gesetzes über die Digitalisierung im Freistaat Bayern (Bayerisches Digitalgesetz – BayDiG) gilt seit 01.08.2022 und ersetzt Art. 5 Abs. 2 BayEGovG, der bis 31.07.2022 galt.
[3] Verordnung über die Digitalisierung im Freistaat Bayern (Bayerische Digitalverordnung – BayDiV) gilt seit 01.08.2023 und ersetzt die BayEGovV, die bis 31.07.2023 galt.
[4] Spezifikation XRechnung 2.3.1 siehe https://xeinkauf.de/app/uploads/2023/02/231-XRechnung-2023-02-03.pdf (gültig ab 01.08.2023) und Spezifikation XRechnung 3.0.0 siehe https://xeinkauf.de/app/uploads/2023/07/XRechnung-v3.0.0.pdf (gültig ab 01.02.2024).
[5] Vgl. Begründung zu § 18 Abs. 2 BayDiG in der LT-Drs.18/19572, S. 62.
[6] Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen-und Rechnungswesen der Bayerischen Kommunen (AFS-HKR); vgl. Anlage 1 zum IMS vom 30.04.2019, Az. B4-1512-4-17; https://www.innenministerium.bayern.de/kub/komfinanzen/haushaltsrecht/index.php

- eine zunehmende Anzahl von elektronischen Rechnungen in unstrukturierten, nicht automatisiert verarbeitbaren elektronischen Formaten, wie z.B. PDF-Rechnungen oder Bild-Dateien,
- die gesetzliche Verpflichtung zum Empfang und zur Verarbeitung elektronischer Rechnungen in strukturierten, automatisiert verarbeitbaren Formaten i.S. von § 8 Abs. 1 Satz 1 Nr. 2 und Satz 2 BayDiV,
- verstärktes E-Payment bei Dienstleistungen nach dem Onlinezugangsgesetz,
- erweiterte Aufzeichnungspflichten beim Einsatz von PC-Kassensystemen nach § 146a AO oder
- Erweiterung der Umsatzbesteuerung der öffentlichen Hand durch die Anwendung des § 2b UStG.

Da es bereits eine Reihe von Veröffentlichungen zum Thema „Empfang und Verarbeitung von elektronischen Rechnungen" gibt (vgl. insb. den Leitfaden des Bayerischen Landkreistags zur Umsetzung der E-Rechnung bei den Landratsämtern[7] oder die Erläuterungen der KoSIT Bremen im Standard XRechnung), möchten wir nachfolgend Antworten zu Fragen geben, die in diesem Zusammenhang in den letzten Jahren immer wieder an uns herangetragen wurden, und zu Sachverhalten, die wir regelmäßig in unseren Prüfungsberichten beanstandet haben. Dabei möchten wir, aufbauend auf den beiden genannten Veröffentlichungen, insbesondere die Prüfungserfahrungen und Fragestellungen aus der Praxis in den Mittelpunkt stellen.

Aus Vereinfachungsgründen und zur besseren Lesbarkeit haben wir in diesem Beitrag auf die für Gemeinden geltenden kommunalrechtlichen Vorschriften abgestellt; gleichlautende Regelungen finden sich auch in den anderen Kommunalgesetzen (LKrO, BezO).

[7] https://www.bay-landkreistag.de/Landkreistag/BayerischerInnovationsring.aspx

2 Elektronischer Rechnungseingang und elektronischer Anordnungsworkflow

Die gesetzliche Verpflichtung zum Empfang und zur Verarbeitung von digitalen Rechnungen i.S. von Art. 18 Abs. 2 BayDiG und § 8 BayDiV gilt für öffentliche Aufträge im sog. Oberschwellenbereich und auch für Aufträge im sog. Unterschwellenbereich, sofern der Auftragswert den Betrag von 1.000 € ohne Umsatzsteuer erreicht oder überschreitet. Von der Annahmeverpflichtung im Unterschwellenbereich waren Bauaufträge befristet bis 18.04.2023 ausgenommen. Zur Umsetzung dieser Anforderungen und mit Blick auf die zunehmende Anzahl von PDF-Rechnungen, die zwischenzeitlich bei den Kommunen eingehen, empfehlen wir grundsätzlich, die Umstellung des Anordnungswesens auf **maschinell verarbeitbare digitale Rechnungen** zügig voranzutreiben.

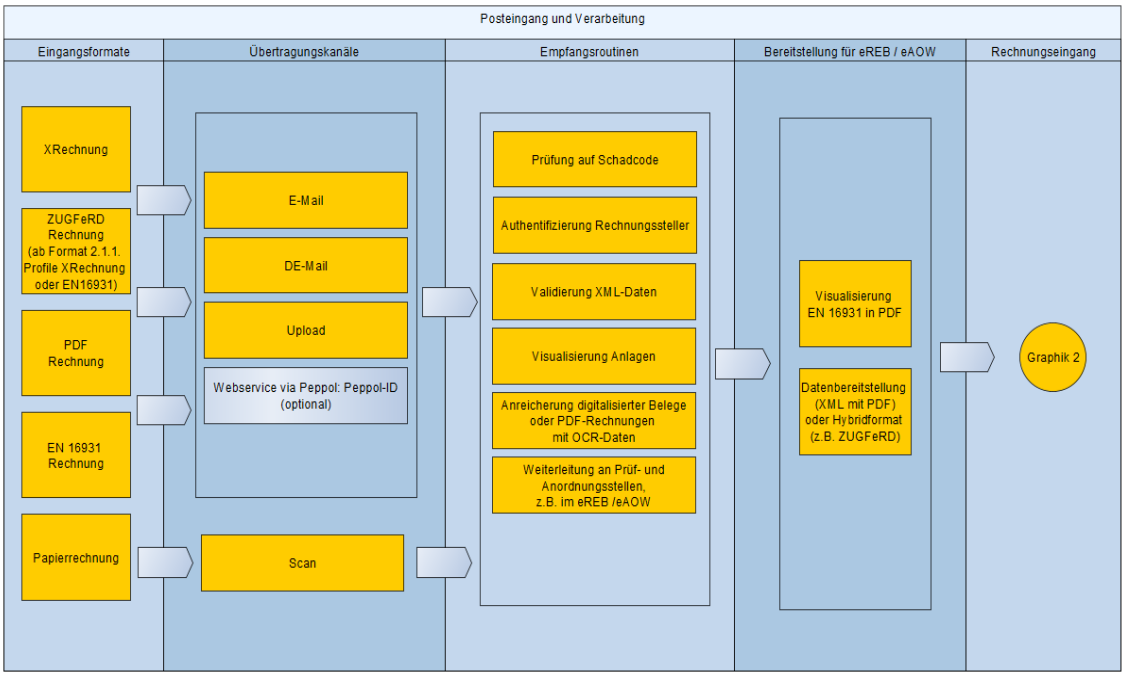
Dies beinhaltet

- den **zentralen Empfang** und die Validierung/Visualisierung strukturierter digitaler Rechnungen, die dem nationalen Datenaustauschstandard XRechnung oder der europäischen Norm EN 16931 entsprechen (z.B. ZUGFeRD 2.1.1 in den Profilen XRechnung oder EN 16931 im XML-Format)[8],
- den **zentralen Empfang** und ggf. die Konvertierung von elektronischen Rechnungen, die in einem nicht automatisiert verarbeitbaren Format empfangen werden (z.B. im Dateiformat PDF),
- die Digitalisierung von eingehenden papiergebundenen Rechnungen in einem **vertrauenswürdigen und qualitätsgesicherten Transformationsprozess** und
- die Anreicherung von Rechnungsdaten mit Daten aus dem Bestellwesen (z.B. AVA-Software[9]) und Finanzwesen (z.B. HÜL oder integrierte Auftragsverwaltung) sowie den Fachverfahren (z.B. Gebäudemanagement).

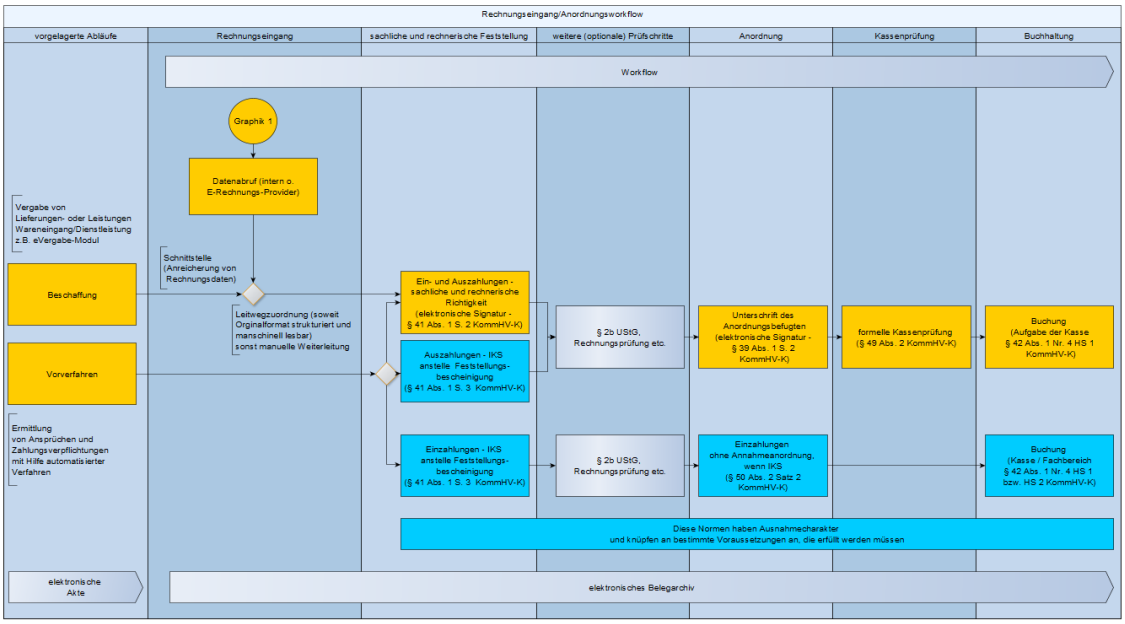
Hinzu kommt, dass das Bayerische Staatsministerium des Innern, für Sport und Integration (StMI) die erstmals mit IMS vom 13.09.2010, Az.: IB4-1512.5-9, festgelegten Anforderungen an den Einsatz von fortgeschrittenen Signaturen im Haushalts-, Kassen und Rechnungswesen zwischenzeitlich grundlegend überarbeitet und im Vorgriff auf noch zu erlassende Verwaltungsvorschriften zur KommHV-Kameralistik und KommHV-Doppik als ergänzende Merkmale gemäß § 87 Nr. 12 KommHV-Kameralistik/§ 98 Nr. 21 KommHV-Doppik mit IMS vom 30.04.2019, Az. B4-1512-4-17, neu festgelegt hat (vgl. auch die Veröffentlichung auf der Homepage des StMI zum Thema „Einsatz elektronischer Signaturen")[10]. Daraus resultieren aus unserer Sicht erhebliche Erleichterungen für die Einführung eines friktionslosen und medienbruchfreien elektronischen Anordnungsworkflows, da nunmehr auch Software-Token für die Erstellung von fortgeschrittenen elektronischen Signaturen verwendet werden können.

Bei der Umstellung des Anordnungswesens sind u.E. folgende idealtypischen Abläufe zu berücksichtigen:

[8] Mit Blick auf die TAX-Compliance muss die Kommune entscheiden, ob sie ggf. auch den Zugang für hybride ZUGFeRD-Formate eröffnen möchte.
[9] Ausschreibung, Vergabe und Abrechnung.
[10] Vgl. https://www.innenministerium.bayern.de/kub/komfinanzen/haushaltsrecht/index.php



(**Zentrale Verarbeitung** aller Rechnungsarten mit dem Ziel einer **ausschließlich digitalen Weiterverarbeitung**)



(**Friktionslose digitale Anordnungsprozesse** unter Berücksichtigung erweiterter steuerlicher Anforderungen)[11]

Im Idealfall sollte der elektronische Workflow bereits mit der Auftragsvergabe bzw. Bestellung beginnen und medienbruchfrei bis zur elektronischen Aufbewahrung der Kassenbelege (einschließlich der begründenden Unterlagen) gestaltet werden. Nur mit medienbruchfreien Prozessen lassen sich unseres Erachtens

[11] Zur einfacheren Lesbarkeit wurden lediglich die Vorschriften der KommHV-Kameralistik in der Graphik vermerkt (dort abgekürzt mit KommHV-K). Die KommHV-Doppik enthält in den zitierten Bereichen die gleichen Regelungsinhalte (vgl. §§ 35 Abs. 1 Satz 2, 37 Abs. 1, 38 Abs. 1 Nr. 4 und § 46 Abs. 2 Satz 2 KommHV-Doppik).

- der Anordnungsprozess insgesamt vereinfachen und vereinheitlichen (Aspekte: Bürokratieabbau, geordneter und sicherer Zugang von Rechnungen, einheitliche Transformation und Datenübernahme),
- eine zuverlässige und schnelle Weiterleitung von Rechnungen an die zuständigen Anordnungsdienststellen sicherstellen (Aspekte: Wegfall von Transportwegen, Einhaltung von Zahlungszielen und Ausschöpfung von Skontovorteilen),
- eine automatische Verbindung zu elektronisch dokumentierten Bestell- bzw. Vergabevorgängen und/oder ein automatischer Abgleich mit noch verfügbaren oder schon in Anspruch genommenen Haushaltsmitteln realisieren (Aspekte: verlässlicher Prüfpfad, Haushaltsüberwachung, frühzeitige Liquiditätsplanung, Vermeidung von Doppelzahlungen),
- eine Optimierung der verwaltungsinternen Prüf- und Anordnungsprozesse erreichen (Aspekte: Wirtschaftlichkeit, Kassensicherheit, automatische Prüfung der Feststellungs- und Anordnungsbefugnis, elektronische Signaturen statt Unterschriften, Möglichkeit von Stapelsignaturen, Transparenz der Bearbeitungsprozesse und -stände, einheitliche Personendatenpflege) und
- formale Prüfpflichten des Anordnungsberechtigten und der Kasse durch den Einsatz der Informationstechnik unterstützen oder ggf. sogar ersetzen (Aspekte: automatische Berechtigungs- und Vollständigkeitsprüfung der Zeichnungsberechtigungen, automatische Prüfung der Integrität und Authentizität von Belegen).

2.1 Regelungen für das Haushalts-, Kassen- und Rechnungswesen

Aufgrund der neuen Vorgehensweise, die sich aus der konsequenten Digitalisierung von eingehenden Papierrechnungen (sog. frühes Scannen), der Verarbeitung von elektronischen – inkl. digitaler – Rechnungen und dem Einsatz eines elektronischen Rechnungseingangsbuchs/Workflowsystems ergibt, bedarf es der Überarbeitung und Anpassung der bestehenden örtlichen Regelungen zum Haushalts-, Kassen- und Rechnungswesen sowie des Erlasses ergänzender bzw. neuer Regelungen.

2.1.1 Was muss ich in meiner Dienstanweisung (DA) für das Finanz- und Kassenwesen ergänzen bzw. neu regeln?

➢ Antwort:

Bei Einsatz eines elektronischen Rechnungseingangsbuchs/Anordnungsworkflows sind die örtlichen Regelungen zum Haushalts-, Kassen- und Rechnungswesen, insbesondere in den Bereichen

- Zuständigkeiten und Befugnisse beim Rechnungseingang und im Anordnungsworkflow,
- Umfang wahrzunehmender Kontrollen mit ergänzenden technischen und organisatorischen Maßnahmen,
- qualitätsgesicherter Transformationsprozess bei ersetzendem Scannen von Papierbelegen,
- Aufbewahrung der Kassenbelege und
- Einsatz elektronischer Signaturen,

anzupassen, zu ergänzen oder neu zu erlassen.

➢ Im Detail:

Nach § 37 Abs. 2 KommHV-Kameralistik/§ 33 Abs. 2 KommHV-Doppik ist das Nähere über den Einsatz automatisierter Verfahren sowie deren Sicherung und Kontrolle durch Dienstanweisung zu regeln. Zudem ist die Feststellungs- und Anordnungsbefugnis ebenfalls durch Dienstanweisung zu regeln; Form und Umfang der Befugnis sind dabei mitzubestimmen. Das Schriftformerfordernis ergibt sich aus § 86 KommHV-Kameralistik/§ 97 KommHV-Doppik.

Bei Einführung bzw. Verwendung eines elektronischen Anordnungsworkflows zur Abwicklung des Anordnungswesens sehen wir insbesondere folgende Bereiche als anpassungs- bzw. neu regelungsbedürftig an:

- die Befugnis für die sachliche und rechnerische Feststellung, inkl. deren Form und Umfang[12],
- die Befugnis Kassenanordnungen zu erteilen, inkl. deren Form und Umfang[13],
- die Verpflichtung zur Verwendung des elektronischen Anordnungsworkflows (ggf. inkl. elektronischen Rechnungseingangsbuchs) zur Abwicklung des Anordnungswesens,
- die Zuständigkeiten für den Empfang und die Übernahme von Eingangsrechnungen in das elektronische Rechnungseingangsbuch/Workflowsystem,
- die technischen und organisatorischen Maßnahmen, um die Integrität, Authentizität und Lesbarkeit[14] der empfangenen elektronischen Rechnungen[15] sicherzustellen,
- die Anreicherung von Rechnungsdaten mit bereits vorhandenen Daten aus dem Bestell-, Auftrags- und/oder Finanzwesen sowie den vorgelagerten Fachverfahren,
- der Einsatz elektronischer Signaturen und die Sicherstellung der Anforderungen, die sich aus den Kommunalhaushaltsverordnungen und den AFS-HKR ergeben, soweit dies nicht in einer gesonderten Dienstanweisung (z.B. DA-Signatur) geregelt wird,
- die Digitalisierung von eingehenden papiergebundenen Rechnungen in einem vertrauenswürdigen und qualitätsgesicherten Transformationsprozess, sofern dies nicht in einer gesonderten Dienstanweisung geregelt wird (z.B. DA-Scan),
- die Aufbewahrung der gescannten papiergebundenen Belege und die Bildung, Führung und Aufbewahrung elektronischer Belege i.S. von § 71 KommHV-Kameralistik/§ 67 KommHV-Doppik, sofern dies nicht in einer gesonderten Dienstanweisung geregelt wird,
- die Zuständigkeiten hinsichtlich Vergabe, Strukturierung und Verwendung der Leitweg-Identifikationsnummer (Leitweg-ID) zur Adressierung digitaler Rechnungen i.S. des Art. 18 Abs. 2 BayDiG und § 8 BayDiV, sofern dies nicht in einer gesonderten Dienstanweisung geregelt wird (z.B. DA-Leitweg).

U.E. wäre es einfacher und zweckmäßiger, in der Dienstanweisung für das Finanz- und Kassenwesen alle allgemeinen Aspekte zu regeln und in separaten Dienstanweisungen die speziellen

[12] Vgl. § 41 Abs. 3 i.V. mit § 86 KommHV-Kameralistik/§ 37 Abs. 3 i.V. mit § 97 KommHV-Doppik.
[13] Vgl. § 38 Abs. 2 Satz 1 i.V. mit § 86 KommHV-Kameralistik/§ 34 Abs. 2 Satz 1 i.V. mit § 97 KommHV-Doppik.
[14] § 61 KommHV-Kameralistik/§ 57 Abs. 3 und 4 KommHV-Doppik, § 14 Abs. 1 Sätze 2 und 3 UStG.
[15] Zur Abgrenzung der Begriffe vgl. hierzu auch Ausführungen unter Nr. 2.2.

Aspekte (z.B. Dienstanweisungen für die Bereiche elektronischer Anordnungsprozess, Anwendung und Prüfung elektronischer Signaturen, Aufbewahrung der Belege, Handhabung der Leitweg-ID). Dies würden u.E. die Lesbarkeit und das Verständnis für die einzelnen Regelungsbereiche erhöhen und die Fortschreibung der örtlichen Regelungen erleichtern. Zur DA-Scan vgl. auch die Ausführungen unter Nr. 2.1.2 und zur DA-Signatur die Nr. 3.2.3.

2.1.2 Muss ich meine bestehenden Regelungen zur elektronischen Belegarchivierung (DA-Scan) anpassen?

➢ Antwort:

Bestehende Dienstanweisungen für die Bildung, Führung und Aufbewahrung elektronischer Belege i.S. des § 71 Abs. 1 KommHV-Kameralistik/§ 67 Abs. 1 KommHV-Doppik (DA-Scan), die auf das sog. späte Scannen, also das nach Abwicklung des Anordnungswesens in der Kasse vorgenommene Scannen, ausgerichtet sind, sollten entsprechend der geänderten Vorgehensweise, wie sie sich aus dem elektronischen Anordnungsworkflow ergibt, angepasst werden. Dabei wären u.U. steuerliche Buchführungs- und Aufzeichnungspflichten zu berücksichtigen.

➢ Im Detail:

Die örtlichen Regelungen sollten Ausführungen zur Umwandlung von in Papierform vorliegenden Dokumenten in elektronische Dokumente (Transformation) und die Qualitätssicherung dieses Transformationsprozesses sowie die Pflichten zur Aufbewahrung des gescannten Papierguts aus anderen Gründen (Rechtsstreitigkeiten, Verwendungsnachweise, Beweisführung, Eigentumsvorbehalte Dritter etc.) enthalten. Soweit sich für die einsetzende Stelle steuerliche Buchführungs- und Aufzeichnungspflichten ergeben (vgl. z.B. §§ 14b, 22 UStG, §§ 4, 41 EStG oder §§ 90, 141 bis 144 AO), sollten bei der elektronischen Belegarchivierung die mit BMF-Schreiben vom 28.11.2019, Az. IV A 4-S 0316/19/10003 :001, BStBl. I S. 1269, veröffentlichten „Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) ebenfalls beachtet werden (vgl. insbesondere die Abschnitte 9.2 und 9.3 der GoBD).

Die in der Muster-Dienstanweisung im BKPV-Geschäftsbericht 2006[16] aufgegriffenen Regelungen zur ordnungsgemäßen, qualitätsgesicherten Transformation können u.E. auch als Grundlage für die örtlichen Regelungen zum sog. frühen Scannen (z.B. über das elektronische Rechnungseingangsbuch/Workflowsystem oder für die elektronische Aktenführung in den Fachbereichen) verwendet werden.

Darüber hinaus verweisen wir auf die von der Bundessteuerberaterkammer und dem Deutschen Steuerberater-Verband e.V. am 29.11.2019 auf Basis der "BSI Technische Richtlinie 03138 Ersetzendes Scannen (TR RESISCAN)"[17] veröffentlichte Muster-Verfahrensdokumentation zum ersetzenden Scannen von Belegen/Geschäftsbriefen,[18] wenn für diese Unterlagen steuerrechtliche Buchführungs- oder Aufzeichnungspflichten bestehen. U.E. ergänzen sich beide Muster gut hinsichtlich des Regelungsumfangs zu haushalts- und steuerrechtlichen Anforderungen.

[16] Geschäftsbericht 2006, Elektronische Archivierung von Buchungsbelegen in Kommunalkassen (Scan-Dienstanweisung und weitere Fragestellungen), S. 78 ff.
[17] https://www.bsi.bund.de, Stichwort: TR03138
[18] https://www.bstbk.de/de/themen/brennpunktthemen/digitalisierung

2.2 Eingang und Verarbeitung von elektronischen Rechnungen

Unter dem Begriff der elektronischen Rechnung verstehen wir jede Rechnung, die in einem elektronischen Format ausgestellt und empfangen wird, also

- nicht automatisiert verarbeitbare elektronische Rechnungen in einem unstrukturierten Dokumentenformat (wie z.B. Rechnungen im PDF-Format) oder
- maschinell lesbare Rechnungen in einem zwischen dem Rechnungssteller und Rechnungsempfänger vereinbarten Datenaustauschformat (z.B. im EDIFACT-Format) oder
- automatisiert verarbeitbare digitale Rechnungen, die in einem strukturierten digitalen Format ausgestellt, übermittelt und empfangen werden.[19]

Eine digitale Rechnung[20] erlaubt einen medienbruchfreien und gesetzlich normierten Rechnungsaustausch innerhalb des europäischen Wirtschaftsraums. Dafür müssen zwei Voraussetzungen vorliegen:

- Die Rechnung wird in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen und
- das digitale Format ermöglicht eine automatische und elektronische Verarbeitung der Rechnung.[21]

Eine lediglich auf elektronischem Weg übermittelte oder zum Herunterladen bereitgestellte Rechnung, wie z.B. eine Rechnung, die als PDF-Dokument an eine E-Mail angehängt ist oder über ein Online-Portal des Rechnungsstellers zum Herunterladen angeboten wird und im Wesentlichen unstrukturierte Daten enthält, wird nicht als digitale Rechnung verstanden.

Der Rechnungsempfänger kann empfangene Rechnungen mit unstrukturierten Inhalten nur mit weiteren Bearbeitungsschritten (u.a. automatische Texterkennung über OCR - Optical Character Recognition) in sein elektronisches Rechnungseingangsbuch/Workflowsystem übernehmen und verarbeiten.

2.2.1 Wer ist zuständig für den Empfang und die Übernahme der Eingangsrechnungen?

➢ Antwort:

Organisatorisch und rechtlich bietet sich wegen der fachlichen Verknüpfung zum Haushalts- und Rechnungswesen eine Zuordnung dieser Aufgaben zu einer zentralen Stelle an, welche in der Finanzverwaltung – Kämmerei angesiedelt ist. Mit einer zentralen Zuständigkeit für die Übernahme und Anreicherung der Eingangsrechnungen kann insbesondere den haushalts- und steuerrechtlichen Bestimmungen verstärkt Rechnung getragen werden.

[19] Vgl. die neue Legaldefinition in Art. 18 Abs. 2 Satz 2 BayDiG und die Begründung in der LT-Drs. 18/19572, S. 62 und 96.
[20] Digitale Rechnungen werden häufig auch als sog. E-Rechnungen bezeichnet; vgl. Leitfaden E-Rechnung (Fn.7).
[21] Also elektronische Rechnungen, bei denen im Gegensatz zu elektronischen Rechnungen i.S. von § 14 Abs. 1 Satz 8 UStG sowohl das semantische Datenmodell, die Geschäftsregeln, die Integritäts- und Plausibilitätsprüfungen als auch die möglichen technischen Syntaxen gesetzlich definiert sind.

➢ Im Detail:

Im Rahmen unserer Prüfungen haben wir regelmäßig dezentrale und verteilte Zuständigkeiten für den Empfang und die Übernahme von Eingangsrechnungen in die örtlich eingesetzten Workflowsysteme vorgefunden. Diese führten zu Doppel- und Mehrfacharbeiten, Medienbrüchen und Abweichungen von den rechtlichen Anforderungen.

Aufgrund der rechtlichen Anforderungen und unserer Erfahrungen bei Prüfungen und Organisationsberatungen empfehlen wir daher, eine zentrale Zuständigkeit für den Empfang und die Übernahme der Eingangsrechnungen in das örtlich eingesetzte elektronische Rechnungseingangsbuch bzw. Workflowsystem zu schaffen und als zentrale Stelle im Bereich Finanzverwaltung – Kämmerei anzusiedeln. Dort startet die elektronische Sachbearbeitung der über die Poststelle eingegangenen oder auf elektronischem Weg übermittelten Rechnungen mit den weiteren haushalts- oder buchungsrelevanten Unterlagen. Ergänzend kann dies mit der Neuanlage oder Änderung von Personendaten (z.B. Finanzadressen) verbunden werden. Die sachliche und rechnerische Prüfung und die Anordnung erfolgen dann durch die für die Mittelbewirtschaftung zuständigen Dienststellen. Die Dienststellen werden insoweit im Anordnungsverfahren unterstützt und deren Ressourcenverantwortung nicht eingeschränkt.

Die Übernahme von Eingangsrechnungen kann mit einer zentralen Zuständigkeit am wirtschaftlichsten durchgeführt und sowohl fachlich als auch technisch (automatisiertes Einlesen) optimal gesteuert werden. Wir weisen darauf hin, dass hierbei eine Reihe verschiedener Anforderungen zu beachten sind, die u.E. nur über einen zentralen Ansatz entsprechend den rechtlichen Vorgaben realisiert werden können. Insbesondere sind dies:

- Nach den haushalts- und steuerrechtlichen Bestimmungen sind bei empfangenen elektronischen Rechnungen die Authentizität, Integrität und Lesbarkeit des Dokuments sicherzustellen. Elektronische Rechnungen sollten daher ausschließlich an ein zentral eingerichtetes E-Mail-Postfach[22] gehen, um Doppelzahlungen zu vermeiden, die Integrität der elektronischen Rechnungen nicht zu gefährden und die zeitnahe zentrale und qualitätsgesicherte Übernahme in ein Dokumentenmanagement-/Archivsystem oder elektronisches Rechnungseingangsbuch sicherzustellen. Beim Download von Rechnungen aus Online-Rechnungsportalen (z.B. Bundesdruckerei) empfehlen wir sicherzustellen, dass durch technische und organisatorische Maßnahmen eine zeitnahe und sichere Weiterleitung an das zentrale E-Mail-Postfach oder das elektronische Rechnungseingangsbuch bzw. Workflowsystem gewährleistet ist.
- Eingehende Papierrechnungen sind nach dem Stand der Technik und den haushalts- und steuerrechtlichen Anforderungen zu digitalisieren. Sie sollten daher unter einer zentralen Zuständigkeit sowie unter einheitlichen, qualitätsgesicherten Kontrollen digitalisiert werden. Dabei wären eine zeitnahe Übernahme der digitalisierten Rechnungen in ein Dokumentenmanagement-/Archivsystem und die revisionssichere Speicherung sicherzustellen (§ 71 Abs. 2 Satz 1 KommHV-Kameralistik/§ 67 Abs. 2 Satz 1 KommHV-Doppik; vgl. auch Ausführungen unter Nr. 2.5.1) und technisch abzusichern.
- Die papiergebundenen Originale sollen bis zum Abschluss der örtlichen Rechnungsprüfung aufbewahrt werden (§ 71 Abs. 2 Satz 2 KommHV-Kameralistik/§ 67 Abs. 2 Satz 2 KommHV-Doppik). Die Sammlung der papiergebundenen Originale lässt sich mit einer zentralen Zuständigkeit für den Rechnungseingang einfach realisieren.

[22] Soweit noch kein zentrales E-Rechnungs-Portal oder der Versand über das Peppol-Netzwerk (vgl. FAQs zu Peppol unter https://xeinkauf.de/peppol/) realisiert ist oder andere Zugangskanäle etabliert sind.

Wir verweisen hierzu auf die unter Nr. 2 dargestellte Graphik zur Abbildung eines optimierten friktionslosen elektronischen Anordnungsworkflows.

Denkbar ist zudem, den rein technischen Prozess der Transformation von originär papiergebundenen Rechnungen einer zentralen Rechnungseingangsstelle (z.B. Poststelle) zuzuordnen oder durch externe Dienstleister abwickeln zu lassen. Gerade bei größeren Kommunen mit einem hohen Aufkommen an Eingangsrechnungen bietet sich eine Prüfung an, ob der Rechnungseingang durch externe Dienstleister wirtschaftlicher als durch eigenes Personal wahrgenommen werden kann, zumal es am Markt hierfür hochspezialisierte externe Dienstleister gibt (sog. E-Invoicing-Provider). Wir verweisen hierzu auf die Nr. 5.3 des Leitfadens E-Rechnung (vgl. Fn. 7) und hinsichtlich der mit der Verlagerung dieser Hilfstätigkeiten einhergehenden datenschutzrechtlichen Fragen auf den Leitfaden zum Outsourcing kommunaler IT[23].

Ergänzend weisen wir darauf hin, dass vom Freistaat Bayern aktuell kein zentrales E-Rechnungs-Portal für den Empfang von elektronischen (inkl. digitaler) Rechnungen betrieben wird, weswegen auf der örtlichen Ebene auch eigene Planungen zu Übertragungs-/Empfangswegen erforderlich sind. Nach unseren Erfahrungen wird der Empfang in der Praxis bisher im Wesentlichen über ein zentrales E-Mail-Postfach, einen eigens betriebenen Online-Dateispeicher oder die Bereitstellung durch den Rechnungssteller per Download realisiert.

2.2.2 Dürfen elektronische Rechnungen ausgedruckt werden?

➢ Antwort:

Aufzubewahren ist das empfangene elektronische Dokument und nicht etwa ein vom elektronischen Dokument erstellter Papierausdruck (Hilfsbeleg) oder der nach Abschluss des Anordnungswesens und der Buchführung digitalisierte, manuell bearbeitete Hilfsbeleg. Zudem gehen mit dem Ausdruck auch elektronische Identifizierungs- und Integritätsmerkmale (z.B. elektronische Signaturen oder Zeitstempel) verloren.

Wenn eine elektronische Rechnung aus verwaltungsinternen Gründen ausnahmsweise ausgedruckt und der so erstellte Eigen-/Hilfsbeleg als Grundlage für die weiteren Bearbeitungsschritte verwendet wird (z.B. Prüfvermerke, Feststellungsbescheinigung, Anordnung, Buchung), sind verschiedene technische und organisatorische Maßnahmen zu ergreifen.

➢ Im Detail:

a) Allgemeines

Eingegangene elektronische Rechnungen müssen stets in dem Format aufbewahrt werden, in dem sie empfangen wurden (vgl. BKPV-Geschäftsbericht 2016, S. 61; GoBD, Rz. 131, 135 [siehe Nr. 2.1.2]). Ein das elektronische Original ersetzender Ausdruck[24] ist weder in den haushalts- noch in den steuerrechtlichen Bestimmungen vorgesehen. Der Ausdruck einer elektronischen

[23] Leitfaden zum Outsourcing kommunaler IT, abrufbar unter https://www.datenschutz-bayern.de (Rubrik „Datenschutzreform 2018 – Orientierungs-und Praxishilfen – Auftragsverarbeitung" als PDF-Datei); vgl. auch IMS vom 30.03.2021, Az. A7-1081-1-72.

[24] Er genießt auch nicht das Privileg des „ersetzenden Scannens", das u.a. in Art. 33 Abs. 3 BayDiG und § 71 Abs. 2 und 4 KommHV-Kameralistik/§ 67 Abs. 2 und 4 KommHV-Doppik gesetzlich geregelt ist.

Rechnung und dessen weitere Verwendung im herkömmlichen papiergebundenen Anordnungswesen ist insbesondere auch mit Blick auf die mit der Einführung von digitalen Rechnungen verfolgten Digitalisierungsziele als kontraproduktiv anzusehen.

Die vom Freistaat angebotene Software für die Visualisierung von digitalen Rechnungen soll daher nur die Einführung der digitalen Rechnung erleichtern. Sie steht auch kommunalen Stellen kostenfrei zur Verfügung.[25] Damit ist aus Sicht des Verordnungsgebers sichergestellt, dass jede Behörde – unabhängig vom Umsetzungsstand der elektronischen Verarbeitungsprozesse – in der Lage ist, die bei ihr eingehenden digitalen Rechnungen zu lesen und weiterzuverarbeiten.

Trotz der vorstehend geäußerten Bedenken gegen den Ausdruck von elektronischen Rechnungen und der von uns favorisierten friktionslosen (elektronischen) Verarbeitung (z.B. mittels elektronischem Rechnungseingangsbuch/Anordnungsworkflow und elektronischem Belegarchiv) werden im Rahmen der überörtlichen Rechnungsprüfung der Ausdruck und die nachfolgenden manuellen Bearbeitungsprozesse akzeptiert, wenn sichergestellt ist, dass

- die Transformation der elektronischen Rechnungen verlustfrei erfolgt,
- der Zeitpunkt der Transformation und dessen Übereinstimmung mit dem elektronischen Original in geeigneter Weise, z.B. auf dem erzeugten Papierdokument, dokumentiert wird,
- bei elektronischen Rechnungen vor und bei der Transformation keine inhaltlichen Veränderungen der Daten vorgenommen werden können und dies technisch und organisatorisch abgesichert ist,
- die transformierte Version als Duplikat der elektronischen Rechnung gekennzeichnet wird,
- der Ausdruck nach Abschluss der papiergebundenen Bearbeitungsprozesse (z.B. Kontierungsvermerke, Feststellungsbescheinigungen, Zahlungsanordnung) digitalisiert und in derselben digitalen Belegmappe wie die ursprünglich eingegangene elektronische Rechnung verwaltet wird,
- stets ein Abgleich des Ausdrucks mit der empfangenen Originalrechnung möglich ist und
- die maschinelle Auswertbarkeit der elektronischen Rechnungsoriginale durch die papiergebundene Verarbeitung weder eingeschränkt noch erschwert wird.

Bei Einsatz eines Dokumentenmanagementsystems oder elektronischen Belegarchivs sollten die vorgenannten Unterlagen daher immer in einer digitalen Belegmappe verwaltet und aufbewahrt werden.

b) Besonderheit bei Baurechnungen

Im Rahmen von Prüfungen und Anfragen wurde regelmäßig die Frage an uns herangetragen, wie mit Baurechnungen zu verfahren sei. Nach unseren Erfahrungen werden Baurechnungen – sofern sie elektronisch eingehen – regelmäßig ausgedruckt, während papiergebundene Rechnungen oft gar nicht ins elektronische Rechnungseingangsbuch/Workflowsystem übernommen werden.

Seit 18.04.2023 besteht nunmehr auch die Pflicht zur Entgegennahme und Verarbeitung von digitaler Baurechnungen im Unterschwellenbereich (vgl. die bis 31.07.2023 geltenden Regelungen in §§ 6, 6a und 7 BayEGovV sowie die Begründung der BayEGovV in der Fassung vom

[25] https://www.e-rechnung.bayern.de/app/#/upload

11.02.2020). Unabhängig von dieser Verpflichtung bleiben weiterhin einige Fragestellungen hinsichtlich der Verarbeitung digitaler Baurechnungen (z.B. im Format XRechnung) unbeantwortet. Dies hängt vor allem mit der hohen Komplexität von Rechnungen im Baugewerbe zusammen. Rechnungsbegründende Unterlagen (Baupläne, Fotos, Aufmaße, Wiegescheine, Lieferscheine etc.), die z.T. auch in unterschiedlichen Formaten eingehen können (wie z.B. GAEB[26], DGM[27], DGH[28], DWG[29]), können dem Rechnungsdatensatz aktuell nicht adäquat beigefügt werden.

Zudem zeigt sich in der Praxis, dass Baurechnungen, insbesondere Schlussrechnungen, einen erheblichen Umfang annehmen können. Auch stellen sie häufig eine Bearbeitungsgrundlage für Anpassungen, Korrekturen und Kontrollen mit einer Vielzahl von Beteiligten dar. Das "Arbeiten" mit dem haptischen papiergebundenen Format ist dabei noch in vielen Verwaltungen und bei externen Beteiligten verankert. Zwar gibt es eine Reihe von Softwarelösungen, die z.B. PDF-Dokumente mit entsprechenden Bearbeitungsvermerken, Notizen und Unterschriften versehen können, allerdings werden diese nach unseren Erfahrungen in der Praxis aufgrund des Mehraufwands kaum akzeptiert. Zudem liegen häufig nicht allen Beteiligten (z.B. Architekten, Ingenieurbüros) entsprechende (gleiche) Softwarelösungen vor. Viele Kommunen stellten externen Beteiligten sämtliche Bauinformationen ohnehin auch im GAEB DA XML-Format zur Verfügung, anhand dessen dann entsprechende Kontrollen und Korrekturen vorgenommen wurden.[30]

Losgelöst davon, in welchem Format eine Baurechnung elektronisch eingeht (digitale Rechnung, PDF-Rechnung), akzeptieren wir als Vorgehensweise, wenn Korrekturen[31] ausschließlich an den intern erstellten Eigen-/Hilfsbelegen (z.B. Ausdruck, digitale Kopie) vorgenommen und dabei die unter Buchst. a dargestellten Anforderungen beachtet werden. Insbesondere ist sicherzustellen, dass die intern erstellten Hilfsbelege, über die sich die Anpassung des Rechnungsbetrags ergibt, nach Abschluss der Bearbeitungsprozesse ebenfalls beim Original aufbewahrt und in derselben digitalen Belegmappe mit demselben Index wie die ursprünglich eingegangene Rechnung verwaltet werden.

Dies gilt auch für alle weiteren die Rechnung begründenden Unterlagen und Dateien, wenn sich Korrekturen z.B. nur über die GAEB-Datei erschließen. Wir weisen darauf hin, dass mit der Version GAEB DA XML 3.3 Anpassungen vorgenommen wurden, um die Verbindung zur elektronischen Rechnungsstellung (beispielsweise via XRechnung) hinsichtlich Einbettung der GAEB-Datei als rechnungsbegründende Unterlage zu erleichtern.

Begründende Unterlagen, die – z.B. aufgrund ihres Umfangs – nicht mit der Kassenanordnung zusammengefasst werden, sollen so geordnet werden, dass sie anhand der Kassenanordnungen ohne Schwierigkeiten zur Einsicht und zur Prüfung bereitgestellt werden können (vgl. VV Nr. 3

[26] GAEB DA XML 3.3 Ausgabe 2021-05, GAEB Gemeinsamer Ausschuss Elektronik im Bauwesen; https://www.gaeb.de/de/service/downloads/gaeb-datenaustausch/
[27] Digitales Geländemodell (z.B. zur Berechnung von Baugruben)
[28] Schnittstellenbeschreibung des Deutschen Großhandelsverband Haustechnik (DGH).
[29] DWG ist ein Dateityp, der zum Speichern von CAD-Zeichnungen verwendet wird.
[30] GAEB DA XML soll dazu dienen, einen einheitlichen Standard für den Austausch von Bauinformationen zu vereinbaren und damit alle Anforderungen an elektronische Prozesse zur Ausschreibung, Vergabe und Abrechnung bei der Durchführung von Baumaßnahmen zu unterstützen.
GAEB Gemeinsamer Ausschuss Elektronik im Bauwesen; https://www.gaeb.de/de/produkte/gaeb-datenaustausch/
[31] Hinsichtlich der Abgrenzung der Themen "Berichtigung von Rechnungen" und "Berichtigung der Bemessungsgrundlage" vgl. BMF-Schreiben vom 08.12.2004, Az. IV A 5 - S 7286a - 3/04 und Verfügung der OFD Nürnberg vom 03.05.2005, Az. S 7286a - 1/St 43 (https://bayernrecht.beck.de/Bcid/Y-100-G-BMF_IV_A5_S7286a_3_04) sowie BFH, Urteil vom 27.09.1979 - V R 78/73.

zu § 71 KommHV a.F.[32] i. V. mit VV Nr. 3 zu § 38 KommHV a.F., Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht in Bayern – Praktikerhandbuch, Stand: Januar 2023, Erl. 4 zu § 39 KommHV-Kameralistik/Erl. 4 zu § 35 KommHV-Doppik). Bei elektronischer Aufbewahrung der Belege wäre dies über gegenseitige Verweise oder Verknüpfungen sicherzustellen. Die näheren Einzelheiten diesbezüglich sollten ebenfalls in einer Dienstanweisung geregelt werden.

Ergänzend verweisen wir auf den Beitrag im BKPV-Geschäftsbericht 2021 „Elektronische Bauabrechnung mit digitalen Geländemodellen - Erfahrungen aus der Prüfungstätigkeit und Empfehlungen", S. 72 ff.

2.3 Elektronisches Rechnungseingangsbuch

Weder Art. 18 Abs. 2 BayDiG noch § 8 BayDiV enthalten eine gesetzliche Verpflichtung, empfangene digitale Rechnungen nach der erfolgreichen Validierung und Visualisierung der Rechnungsinhalte ausschließlich elektronisch zu verarbeiten.

Allerdings empfehlen wir nicht zuletzt aus Gründen der Sparsamkeit und Wirtschaftlichkeit, solche elektronischen Prozesse (flächendeckend) zu etablieren, um die Vorteile des sicheren und automatisierten Imports von strukturierten Rechnungsdaten zu nutzen, einen möglichst effizienten und sicheren elektronischen Anordnungsprozess zu unterstützen und die Nachteile und Risiken von Medienbrüchen zu vermeiden. Die Nutzenpotenziale der elektronischen Form, insbesondere mit Blick auf vollständig maschinell verarbeitbare digitale Rechnungen (z.B. nach dem nationalen XRechnung-Standard[33] oder der CEN 16931), liegen auch ohne eine entsprechende gesetzliche Verpflichtung auf der Hand.[34]

2.3.1 Wie erhöhe ich den Anteil an digitalen Rechnungen, um von einer automatisierten Verarbeitung zu profitieren?

➢ Antwort:

Die Kommunen, die bereits den Rechnungseingang und ihr Anordnungswesen auf den Empfang und die Verarbeitung von digitalen Rechnungen angepasst haben, sollten aktiv an die Rechnungssteller herantreten, um die Anzahl an digitalen Rechnungen zu erhöhen und von den Vorteilen einer automatisierten Verarbeitung in zunehmendem Maße zu profitieren.[35]

Die von der KGSt und VITAKO[36] veröffentlichte „Leitlinie zum ersetzenden Scannen in Kommunen nach der TR RESISCAN" führt hierzu auf S. 4 aus: *„Scannen ist gut, es ist aber immer nur die zweitbeste Lösung. Die beste Lösung ist, erst gar nicht scannen zu müssen. Neben der weitgehenden Digitalisierung der Papieroriginale sollte also mindestens genau so viel Energie in die Vermeidung des Papieraufkommens gelegt werden. Die KGSt empfiehlt, dies prioritär in Angriff zu nehmen."*

[32] VVKommHV; zur Anwendbarkeit vgl. Finanzplanung 2006 bis 2010, IMBek vom 06.02.2007, Az. IB4-1512.5-9 (AllMBl. 2007/3, S. 190, Nr. 5).
[33] Der nicht nur die Konformität einer digitalen Rechnung mit der CEN 16931, sondern auch die Einhaltung nationaler Geschäftsregeln und Merkmale gewährleistet.
[34] Vgl. u.a. Erwägungsgrund Nr. 7 der EU-Richtlinie 2014/55/EU vom 16.04.2014.
[35] Vgl. Nr. 5.2. "Effizienzpotenziale von E-Rechnungen" im Leitfaden E-Rechnung (Fn. 7).
[36] Vgl. https://www.kommune21.de/meldung_26356_on.html

➢ Im Detail:

Im Rahmen unserer Prüfungen werden wir regelmäßig darauf hingewiesen, dass von den Rechnungsstellern bislang nur unstrukturierte elektronische Rechnungen (z.B. PDF-Rechnungen) und kaum digitale Rechnungen übermittelt werden.

Dabei erscheint es mit Blick auf die Vielzahl der zu verarbeitenden Rechnungen aus verwaltungsökonomischen Gesichtspunkten wirtschaftlich und zweckmäßig, die Umstellung des Anordnungswesens bereits jetzt konsequent auf digitale Rechnungen auszurichten und zur Erhöhung des Anteils aktiv beizutragen.

Um diesen Ansatz zu unterstützen, sollte die jeweils einsetzende Stelle durch Anpassung der Vertrags- bzw. der Ausschreibungsunterlagen um die Vorlage digitaler Rechnungen bitten, um Papier- und unstrukturierte elektronische Rechnungen weitgehend zu vermeiden. Darüber hinaus empfehlen wir, aktiv an die Rechnungssteller heranzutreten und die Umstellung auf digitale Rechnungen anzuregen und den Empfang von digitalen Rechnungen über ein zentrales E-Mail-Postfach sicherzustellen.

Für die Rechnungssteller bieten sowohl (teils kostenlose) Fakturierungsprogramme und XRechnungs-Generatoren als auch E-Billing-Provider und die professionellen ERP-Lösungen bzw. Buchhaltungsprogramme inzwischen die Möglichkeit, digitale Rechnungen für einen großen Anwenderbereich zu erstellen.

Mit dem zunehmenden Umfang an digitalen Rechnungen sollte ein Konzept zur Strukturierung der Leitweg-ID ausgearbeitet werden, um die Adressierung der digitalen Rechnung für die nachgelagerten workflowgestützten Prozesse effektiv nutzen zu können.[37]

2.3.2 Welche flankierenden Maßnahmen bieten sich an, um die ordnungsgemäße Übernahme von elektronischen Rechnungen zu gewährleisten?

➢ Antwort:

Nach unseren Erfahrungen handhaben die bayerischen Kommunen Zuständigkeiten, Verfahrenseinsatz und Systemumgebung sehr unterschiedlich. Gleiches gilt für den Empfang und die Aufbewahrung von elektronischen Rechnungen sowie die Abwicklung des Anordnungsworkflows. Dies bedingt neben den bereits dargestellten Maßnahmen (vgl. z.B. Nr. 2.2.1 zur Organisation des Rechnungseingangs) individuelle und auf die jeweiligen Einsatzbedingungen angepasste technische und organisatorische Maßnahmen. Dabei sollen Maßnahmen, die der Sicherung und Kontrolle der eingesetzten finanzwirksamen Verfahren dienen, durch Dienstanweisung geregelt und bei der haushaltsrechtlichen Freigabe berücksichtigt werden. Technischen Kontrollen und Sicherungsmaßnahmen ist der Vorzug zu geben.

➢ Im Detail:

Hinsichtlich der unterschiedlichen Formate, in denen Rechnungen eingehen, und hinsichtlich der Frage, wie diese ins elektronische Rechnungseingangsbuch bzw. Workflowsystem zu übernehmen sind, verweisen wir erneut auf den ausführlichen Leitfaden zur E-Rechnung (siehe Fn. 7). An

[37] Vgl. auch Ausführungen unter Nr. 2.3.3 "Wie kann ich die Leitweg-ID im Workflow nutzen".

dieser Stelle möchten wir lediglich auf Sachverhalte aus der Praxis eingehen, die zu Medienbrüchen, unnötigem Mehraufwand und Doppelzahlungen führten oder die Informationssicherheit gefährdeten.

Hauptzugangskanäle für elektronische Rechnungen waren dabei E-Mail und der Download (Online-Datenspeicher, Lieferantenportal)[38]. Dabei stellten wir im Rahmen unserer Prüfungen beispielsweise folgende Sachverhalte fest:

- Elektronische Rechnungen gingen in den E-Mail-Postfächern der einzelnen Sachbearbeiter ein, wurden von diesen ausgedruckt und (teils mit zeitlichem Verzug) papiergebunden dem Anordnungsgeschäftsgang zugeleitet. Gleichzeitig wurden die elektronischen Rechnungen ans zentrale E-Mail-Postfach weitergeleitet und hierüber ins elektronische Rechnungseingangsbuch bzw. Workflowsystem übernommen. Diese Vorgehensweise führte in mehreren geprüften Fällen zu Doppelzahlungen. Die Ausdrucke enthielten zum Teil keine ausreichenden Sichtvermerke, dass es sich um Kopien handelte.
- Die empfangenen elektronischen Rechnungen wurden vor der Übernahme ins elektronische Rechnungseingangsbuch bzw. Workflowsystem im Dateiverzeichnis zwischengespeichert. Auf das Dateiverzeichnis hatten alle an der Domäne des lokalen Netzwerks angemeldeten Beschäftigten mindestens Schreib- und Leserechte und damit auch die Möglichkeit, Änderungen an den elektronischen Rechnungen vorzunehmen, bevor sie ins Workflowsystem übernommen wurden.
- E-Mails enthielten im Anhang neben den elektronischen Rechnungen auch Schadsoftware. Ausreichende technische (z.B. ausreichender Virenschutz am Mail-Gateway und/oder E-Mail-Server, Filterung von sicherheitsgefährdenden Inhalten und Adressen am Mail-Gateway) und organisatorische Maßnahmen (z.B. Prüfungen zur Echtheit der Herkunft, Sensibilisierung der Beschäftigten) waren nicht getroffen worden.
- Elektronische Rechnungen gingen bei den Sachbearbeitern in den Fachbereichen ein, die die Rechnungsinhalte und die Bankverbindung manipulierten, bevor sie die elektronische Rechnung an das zentrale E-Mail-Postfach zur Übernahme ins elektronische Rechnungseingangsbuch bzw. Workflowsystem weiterleiteten.

Nach den haushalts- und steuerrechtlichen Bestimmungen sind bei empfangenen elektronischen Rechnungen die Authentizität, Integrität und Lesbarkeit des Dokuments sicherzustellen. Zudem sind beim Einsatz finanzwirksamer Verfahren, wie z.B. des elektronischen Rechnungseingangsbuchs/Workflowsystems, Sicherheits- und Kontrollmaßnahmen durch Dienstanweisung zu regeln (vgl. auch Ausführungen unter Nr. 2.1) und bei der haushaltsrechtlichen Freigabe nach § 37 Abs. 1 Nr. 1 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 1 KommHV-Doppik zu berücksichtigen. Hierbei ist technischen Maßnahmen, die der Sicherung und Kontrolle finanzwirksamer Verfahren dienen, stets der Vorzug zu geben, da sie – im Gegensatz zu den organisatorischen Kontrollen – automatisch ablaufen, stets greifen und keine Medienbrüche oder Folgekosten verursachen (VV Nr. 2 zu § 41 KommHV a.F., Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht, Stand: Januar 2023, Erl. 7 zu § 37 KommHV-Kameralistik/Erl. zu § 33 KommHV-Doppik).

Um die Integrität und die Authentizität zu gewährleisten und den Sicherungs- und Kontrollzweck zu erfüllen, bedarf es daher technischer und organisatorischer Maßnahmen, die auf die jeweilige

[38] Da bislang kein zentrales E-Rechnungs-Portal in Bayern betrieben oder der Versand über das Peppol-Netzwerk bislang nicht genutzt wird; hinsichtlich weiterer Zugangskanäle vgl. Nr. 2.4 des Leitfadens E-Rechnung (Fn. 7)

Situation vor Ort angepasst sind. Einige dieser möglichen Maßnahmen möchten wir beispielhaft darstellen:[39]

- Der Empfang und die Übernahme von Eingangsrechnungen sollte zentral organisiert (vgl. Ausführungen unter Nr. 2.2.1) und auf den Ausdruck von elektronischen Rechnungen möglichst verzichtet werden. Sofern der Ausdruck notwendig ist, sollten die unter Nr. 2.2.2 Buchst. a genannten Anforderungen berücksichtigt werden.

- Es bietet sich an, einen ausreichenden technischen oder organisatorischen Kontrollprozess zu etablieren, über den zuverlässig geprüft wird, ob der fakturierte Betrag bereits angeordnet/ausgezahlt wurde. Einige der in der Praxis verwendeten Finanzverfahren, elektronischen Rechnungseingangsbücher oder Workflowsysteme unterstützten eine automatisierte Verprobung, ob eine Eingangsrechnung bereits erfasst wurde.

  Damit automatisierte oder manuell nachgelagerte Verprobungen effektiv genutzt werden können, bedarf es einer hohen Buchungsqualität, bei der Rechnungsdaten korrekt und einheitlich erfasst werden. Auch sollten Angaben und Mindestinhalte zum Buchungstext, Verwendungszweck und Anordnungsgrund einheitlich vorgegeben werden und nicht der Arbeitsweise des jeweiligen Fachamtes oder des einzelnen Beschäftigten überlassen bleiben. Des Weiteren sollten Maßnahmen ergriffen werden, um die Mehrfachanlage von Personendaten (wie z.B. Finanzadressen[40]) zu vermeiden.

  Die Doppelerfassung von originär papiergebundenen Rechnungen könnte ggf. auch mithilfe von einem sog. Imprinting (automatischer Aufdruck von Scan-Informationen) beim frühen Scannen von Belegen oder anderen technischen und organisatorischen Maßnahmen (z.B. Scan-Stempel, Schneideecke) vermieden werden. Bei originär elektronischen Rechnungen bieten sich dafür entsprechende elektronische Merkmale (z.B. elektronische Zeitstempel, Siegel oder Signaturen) an.

  Wir empfehlen, die sich bietenden technischen und organisatorischen Möglichkeiten zu nutzen bzw. diese beim jeweiligen Verfahrensanbieter bei der Fortentwicklung der Lösung einzufordern.

- Jeder Auftrag und jede Bestellung sollte unverzüglich in einem zentralen Auftragsverwaltungssystem mit zwingenden Mindestinhalten erfasst werden.[41] Bei Rechnungseingang sollte dann bei einer vorhandenen Verknüpfung des elektronischen Rechnungseingangsbuchs/Workflowsystems mit dem Auftragsverwaltungssystem der Abgleich automatisiert und spätestens im Rahmen der fachtechnischen Prüfung vorgenommen werden (vgl. auch Anforderungen an den verlässlichen Prüfpfad zwischen Rechnung und Leistung i.S. des § 14 Abs. 1 UStG).[42] Wir verweisen hierzu auch auf unsere Ausführungen unter Nr. 2.3.3 Buchst. b zur Nutzung der Leitweg-ID.

  Sind Besteller und Feststellungsbefugter dieselbe Person, sollte durch organisatorische Kontrollen sichergestellt werden, dass beide Prozesse ordnungsgemäß abgewickelt werden.

---

[39] Vgl. auch Nr. 5.1.3. „Prüfungserfahrungen mit friktionsbehafteten papiergebundenen Anordnungsprozessen" im Leitfaden E-Rechnung (Fn. 7).

[40] Dieser Begriff wird ggf. in den Finanzverfahren uneinheitlich gebraucht.

[41] Z.B. Auftragsbezeichnung, Auftragsnummer, Leitweg-ID, Auftragsdatum, Auftragssumme, Zahlungsbedingungen, Fälligkeit, Finanzadresse, Bankverbindung, Rechnungs- und Lieferanschrift, Haushaltsstellen bzw. Konten Ergebnisrechnung und Finanzrechnung, Produkt / Leistung, Kostenstelle / Kostenträger.

[42] Ein verlässlicher Prüfpfad ist Bestandteil eines internen Kontrollverfahrens zur Gewährleistung der Echtheit der Herkunft einer Rechnung, der Unversehrtheit ihres Inhalts und ihrer Lesbarkeit. Anhand eines verlässlichen Prüfpfads ist ein Zusammenhang zwischen der Rechnung und der zugrundeliegenden Leistung herzustellen.

- In der Praxis kann es bereits unmittelbar beim Empfang von elektronischen Rechnungen per E-Mail sinnvoll sein, technische Kontrollen zu etablieren, um die Authentizität des Rechnungsstellers und die Zulässigkeit der Rechnungsstellung sicherzustellen. Solange kein zentrales E-Rechnungs-Portal in Bayern angeboten wird oder andere Zugangskanäle etabliert sind (z.B. Peppol-Netzwerk), ist man hier zunächst auf eigene Lösungen oder die der Verfahrensanbieter angewiesen.

  Bayerische Kommunen verfahren daher z.B. dergestalt, dass sich der Rechnungssteller im Vorfeld (z.B. im Rahmen der Auftragsvergabe) bei der Kommune mit seiner E-Mail-Adresse registrieren muss,[43] über die der spätere Rechnungsversand erfolgt. Mit Eingang der Rechnung wird die E-Mail-Adresse bereits am Mail-Gateway abgeglichen und entweder ans zentrale E-Mail-Postfach für den Rechnungseingang weitergeleitet oder (zur Kontrolle) herausgefiltert.

  Weitere Lösungen, die in die gleiche Richtung zielen, wären z.B. die E-Mail-Adresse des Rechnungsstellers bzw. -senders bereits beim Auftrag oder bei den Personendaten (z.B. Finanzadresse) zu hinterlegen und einen etwaigen Abgleich bei den elektronischen Rechnungseingangsbüchern/Workflowsystemen zu implementieren.

- Hinsichtlich der Nutzung des Zugangskanals E-Mail empfehlen wir, den Zugang von elektronischen Rechnungen grundsätzlich zu zentralisieren und einen definierten Zugangspunkt in der Form eines Funktionspostfachs anzubieten (z.B. erechnung@musterhausen.de). Dies bietet den Vorteil, dass dieses zentrale Postfach in definierten Zeitintervallen automatisiert ausgelesen, eingegangene digitale Rechnungen automatisiert geprüft und visualisiert sowie anschließend zusammen mit den Prüfprotokollen an nachgelagerte Verfahren (z.B. elektronisches Rechnungseingangsbuch/Workflowsystem, Finanzverfahren) weitergeleitet werden können. Eine manuelle Übernahme kann insoweit reduziert werden. Entsprechende Verfahrensfunktionen sollten genutzt werden.

- Sollte eine automatisierte Übernahme der elektronischen Rechnungen aus dem zentralen E-Mail-Postfach durch das elektronische Rechnungseingangsbuch/Workflowsystem (noch) nicht angeboten werden, empfehlen wir, bei einer Zwischenspeicherung auf Dateiverzeichnisebene auf einen ausreichenden Zugriffsschutz zu achten. Die Zugriffsrechte sollten daher auf den zwingend notwendigen Umfang reduziert[44] und die Überwachungsrichtlinie[45] vom System auf das Dateiverzeichnis angewendet werden, um die Zugriffe zu protokollieren. Gegebenenfalls können die Netzwerkverzeichnisse als sog. versteckte Freigabe eingerichtet werden, damit diese nicht über die Netzwerkumgebung sichtbar sind und nur aus dem Dialogfenster des Workflowsystems die elektronischen Rechnungen übernommen werden können.

- Am Mail-Server wären ausreichende Maßnahmen zum Virenschutz zu ergreifen. Neben einer Erhöhung der Sicherheit des Mail-Servers selbst (sog. Härtung)[46] bedingt dies auch den Einsatz einer Virenschutzlösung. Darüber hinaus sollten weitere Maßnahmen am Mail-Gateway

[43] Z.B. die Internetseite der Gemeinde.

[44] Vgl. § 37 Abs. 1 Nrn. 2, 4 und 5 und § 61 Abs. 1 und 2 KommHV-Kameralistik bzw. § 33 Abs. 1 Nrn. 2, 4 und 5 und § 57 Abs. 3 und 4 KommHV-Doppik, Art. 43 Abs. 1 BayDiG sowie die Basis-Anforderungen ORP.4.A2 „Einrichtung, Änderung und Entzug von Berechtigungen" und ORP.4.A7 „Vergabe von Zugriffsrechten" des IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik, Edition 2023 (www.bsi.de).

[45] Mit einer Überwachungsrichtlinie kann man am System (PC oder Server) nach Kategorien festlegen, welche sicherheitsrelevanten Ereignisse in die Systemprotokollierung aufgenommen werden, um diese später auswerten zu können (z.B. Aufzeichnen von unberechtigten Dateiverzeichniszugriffen).

[46] Ein Prozess, der dazu dient, eine Angriffsmöglichkeit zu eliminieren, indem Schwachstellen gepatcht und nicht benötigte Dienste abgeschaltet werden.

ergriffen (Filterung, Virenschutz) und die Beschäftigten für das Thema Virenschutz sensibilisiert werden. Das Thema wäre bei der Erstellung und Fortschreibung der eigenen Informationssicherheitskonzepte nach Art. 43 Abs. 1 BayDiG zu berücksichtigen. Je nach ermitteltem Schutzbedarf des Informationsverbundes verweisen wir auf die relevanten Anforderungen des BSI-Kompendiums[47] und insbesondere auf den Prozessbaustein ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit", die Systembausteine OPS.1.1.4 „Schutz vor Schadprogrammen" und APP.5.3 „Allgemeiner E-Mail-Client und -Server" sowie die hierzu veröffentlichten Umsetzungshinweise.

Weitere Ausführungen hierzu enthält die Nr. 2.5.2.1. „Prüfung der XML-Daten und rechnungsbegründenden Unterlagen auf Schadcode (Virenprüfung)" im Leitfaden E-Rechnung (siehe Fn. 7).

– Beim Herunterladen von elektronischen Rechnungen über Lieferantenportale oder eigene Online-Datenspeicher empfehlen wir darauf zu achten, dass diese unverzüglich an das zentrale E-Mail-Postfach weitergeleitet bzw. ins elektronische Rechnungseingangsbuch/Workflowsystem übernommen werden; die Rahmenbedingungen und die zu etablierenden Kontrollen empfehlen wir per Dienstanweisung zu regeln. Hinsichtlich der dezentral in den persönlichen E-Mail-Postfächern der einzelnen Sachbearbeiter eingehenden elektronischen Rechnungen sollen die Rechnungssteller konsequent auf das zentrale Funktionspostfach verwiesen werden.

2.3.3 Wie kann ich die Leitweg-ID im Workflow nutzen?

➢ Antwort:

Die Leitweg-Identifikationsnummer (Leitweg-ID)[48] dient der Adressierung und Weiterleitung von digitalen Rechnungen an den Rechnungsempfänger und kann eine automatisierte Zuordnung zum zuständigen Bewirtschafter in den Workflowsystemen unterstützen. Die Feinadressierung kann als Bestandteil der Leitweg-ID frei von der einsetzenden Stelle vergeben werden und somit beispielsweise eine Verknüpfung zum Auftragsverwaltungssystem herstellen oder direkt Informationen zum Auftrag/zur Bestellung, zur Organisation oder zur Buchung enthalten. Wir empfehlen, die Leitweg-ID als Identifikationskennzeichen zu verwenden.

➢ Im Detail:

a) Die Leitweg-ID

In § 8 Abs. 1 Satz 1 Nr. 3 Buchst. a bis d BayDiV sind folgende **Pflichtangaben** definiert, die eine digitale Rechnung enthalten muss:

– ein eindeutiges Identifikationskennzeichen (z.B. Auftragsnummer, ein Aktenzeichen, Leitweg-ID),
– Zahlungsbedingungen, Bankverbindungsdaten und die E-Mail-Adresse des Zahlungsempfängers

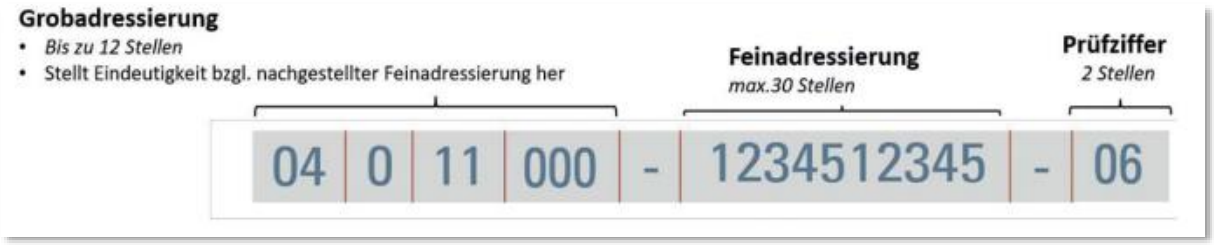
[47] IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik, Edition 2023 (www.bsi.de)
[48] Koordinierungsstelle für IT-Standards (KoSIT) - aktuelle Spezifikation der Leitweg-ID; https://xeinkauf.de/app/uploads/2022/11/Leitweg-ID-Formatspezifikation-v2-0-2-1.pdf

Die Leitweg-ID ist, sofern sie als Identifikationskennzeichen gewählt wird, Pflichtbestandteil einer digitalen Rechnung, um eine automatisierte Zuordnung zu ermöglichen. Die Leitweg-ID dient daher insbesondere der Adressierung und Weiterleitung der eingegangenen digitalen Rechnung an die Rechnungsbearbeitungssysteme der öffentlichen Auftraggeber und die zuständigen Bewirtschafter. Dabei handelt es sich um eine Zahlenkombination, die sich eindeutig einer bestimmten Behörde zuordnen lässt. Die Leitweg-ID dient als Adresse der digitalen Rechnung. Sie ist damit vergleichbar mit der Anschrift des Rechnungsempfängers bei der klassischen Papierrechnung.

Die Adressierung der digitalen Rechnung ist Teil des strukturierten Datensatzes der digitalen Rechnung und kann als Identifikationskennzeichen zur Angabe bei der Rechnungsstellung dem Auftragnehmer/Lieferanten mitgeteilt werden (z.B. im konkreten Auftrag oder auf der Internetseite). Für die Vergabe der Leitweg-ID ist die jeweilige einsetzende Stelle selbst zuständig.[49]

Aufbau der Leitweg-ID[50]: Die Leitweg-ID setzt sich aus drei Bestandteilen zusammen: Grobadressierung, Feinadressierung und Prüfziffer.

Die Grobadressierung und Prüfziffer sind Pflichtbestandteile, die Feinadressierung ist ein optionaler Bestandteil:



Quelle: Koordinierungsstelle für IT-Standards, Leitweg-IT, Format-Spezifikation Version 2.0.2, Fassung vom 28.07.2021

Der Aufbau der Leitweg-ID untergliedert sich wie folgt:

- Die Grobadressierung ist fest vorgegeben und beträgt zwischen zwei und zwölf Stellen (siehe Spezifikation). Die Elemente 1 bis 4 der Grobadressierung sind Teil-Merkmale des Regionalschlüssels[51]: 1. Bundesland / Bund (2 Stellen), 2. Regierungsbezirk (1 Stelle), 3. Landkreis (2 Stellen), 4. Gemeindeverband / Gemeindekennzahl (3, 4 oder 7 Stellen). Im kommunalen Bereich entspricht die Grobadressierung dem Amtlichen Gemeindeschlüssel (AGS).
- Die Feinadressierung kann frei vergeben werden und beträgt bis zu 30 Stellen. Sie kann aus alphanumerischen Zeichen bestehen, d.h. aus Buchstaben des lateinischen Alphabets (A-Z, nicht case-sensitiv) und den Ziffern 0-9.

[49] FAQ des Bayerischen Staatsministeriums für Digitales - https://e-rechnung.bayern.de/app/#/faq
[50] Forum elektronische Rechnung Deutschland – Datenblatt Leitweg-ID; https://www.ferd-net.de/ressourcen/veroeffentlichungen/kurzpapier-zur-leitweg-identifikationsnummer.html
[51] Informationen zum Regionalschlüssel - https://www.destatis.de/DE/Themen/Laender-Regionen/Regionales/Gemeindeverzeichnis/_inhalt.html

- Zudem muss die zweistellige Prüfziffer aus der Grob- und Feinadressierung berechnet werden. Die Generierung der Prüfziffer erfolgt gemäß ISO/IEC 7064:2003 per Modulo 97-10 Verfahren, welches u.a. auch bei IBAN eingesetzt wird.
- Hierzu kann das Tool zur Berechnung der Leitweg-ID Prüfziffer[52] genutzt werden.

Kommunalunternehmen, Eigenbetriebe, Stiftungen usw. (im Nachfolgenden Einrichtungen genannt) erhalten die gleiche Grobadressierung wie der öffentliche Träger. Dieser ist daher verantwortlich, ggf. eine Unterscheidung über die Feinadressierung zu treffen.

b) Leitweg-ID im Workflow nutzen

Nachdem die Feinadressierung von der einsetzenden Stelle frei vergeben werden kann, lassen sich hier insbesondere Informationen hinterlegen, die der einsetzenden Stelle helfen, eine rasche Zuordnung und Verarbeitung zu ermöglichen.

Dabei sollen der strukturierte Datensatz der digitalen Rechnung und das Identifikationskennzeichen, also z.B. die Leitweg-ID,

- eine zuverlässige und schnelle Weiterleitung von Rechnungen an die zuständigen Anordnungsdienststellen sicherstellen (Aspekte: Wegfall von Transportwegen, Einhaltung von Zahlungszielen und Ausschöpfung von Skontovorteilen),
- eine automatische Verbindung zu elektronisch dokumentierten Bestell- bzw. Vergabevorgängen und/oder
- einen automatischen Abgleich mit noch verfügbaren oder schon in Anspruch genommenen Haushaltsmitteln gewährleisten (Aspekte: verlässlicher Prüfpfad, Haushaltsüberwachung, frühzeitige Liquiditätsplanung, Vermeidung von Doppelzahlungen).

Im Idealfall sollte der elektronische Workflow bereits mit der Auftragsvergabe bzw. Bestellung beginnen und friktionslos bis zur elektronischen Aufbewahrung der Kassenbelege einschließlich der begründenden Unterlagen gestaltet werden. Dies bedeutet, dass bereits im Auftragsverwaltungssystem alle wesentlichen Inhalte mit angelegt werden (z.B. eindeutiges Kennzeichen für die Feinadressierung der Leitweg-ID, ggf. Buchungsinformationen, Personendaten, Zuleitungsinformationen), um beim Rechnungseingang eine automatisierte Verarbeitung zu ermöglichen. Dies bedingt daher sowohl den Einsatz entsprechender Fachanwendungen zur Auftragsvergabe/Auftragsmanagement bzw. eine ordnungsgemäße HÜL-Buchführung als auch eine Verknüpfung zu diesen Verfahren oder Verfahrensmodulen. Wir verweisen hierzu auf § 26 Abs. 2 KommHV-Kameralistik/§ 26 Abs. 5 KommHV-Doppik.

Ergänzend merken wir auch an, dass ein Großteil der in der Praxis vorgefundenen Lösungen bislang weder manuelle Zuordnungstabellen anbietet noch Informationen in der Feinadressierung der Leitweg-ID mit Workflow-Routinen verknüpfen kann (z.B. Anreicherung mit Buchungsinformationen oder Zuleitungsinformationen). Entsprechende Möglichkeiten sollten bei den Anbietern der Workflowsysteme, Finanzverfahren bzw. ERP-Systemen angeregt bzw. eingefordert werden.

[52] Bayerisches Staatsministerium für Digitales – Leitweg-ID Prüfziffer; https://e-rechnung.bayern.de/app/#/leitweg-id

2.4 Elektronischer Anordnungsworkflow

Im Rahmen unserer Prüfungstätigkeit bei unseren Mitgliedern haben wir verschiedene Umsetzungen des elektronischen Signatur- und Anordnungsworkflows vorgefunden. Trotz der Unterschiede in der technischen Umsetzung und den organisatorischen Rahmenbedingungen wurden häufig gleichgelagerte Fragen an uns herangetragen. Diese betrafen insbesondere den Nutzungsumfang, die Zuständigkeiten, den Funktionsumfang der eingesetzten Lösung oder die Frage, wie neu hinzugekommene gesetzliche Anforderungen bei der bisherigen Abwicklung berücksichtigt werden können. Einige dieser Fragestellungen möchten wir nachfolgend aufgreifen.

2.4.1 Welche Kassenanordnungen sollten über den elektronischen Anordnungsworkflow abgewickelt werden?

➢ Antwort:

Im digitalen Wandel der öffentlichen Verwaltung gilt es, nicht nur die rechtlichen Vorschriften rechtskonform umzusetzen, sondern auch die sich bietenden Nutzenpotenziale zu realisieren. Der elektronische Rechnungseingang und daran anschließend der elektronische Anordnungsworkflow sollten daher als ein Baustein zur Digitalisierung der Verwaltungsprozesse effektiv genutzt werden. Aus verwaltungsökonomischen Gesichtspunkten sollte das Ziel sein, möglichst alle Kassenanordnungen (§ 38 KommHV-Kameralistik/§34 KommHV-Doppik) über den elektronischen Anordnungsworkflow abzuwickeln, um Medienbrüche, Doppel- und Mehrfacherfassungen sowie vermeidbare Mehrarbeiten durch parallele Prozesse und Ablage- bzw. Aufbewahrungsstrukturen zu verhindern.[53]

➢ Im Detail:

Bei unseren Prüfungen stellten wir häufig fest, dass nicht alle Kassenanordnungen über den Anordnungsworkflow geführt wurden. So wurden regelmäßig zwar die Eingangsrechnungen und die zugehörigen Zahlungsanordnungen über den Anordnungsworkflow abgewickelt, alle weiteren Kassenanordnungen wurden aber weiterhin papiergebunden im Rahmen des vorbereitenden Anordnungswesens bearbeitet und entweder in der Kasse ins elektronische Belegarchiv übernommen (spätes Scannen) oder sogar noch ausschließlich papiergebunden abgelegt und aufbewahrt. Für Integrationsbuchungen aus Vorverfahren oder einer im Finanzverfahren integrierten Personenkontenführung wurden regelmäßig keine förmlichen Zahlungsanordnungen erstellt oder es fehlten die begründenden Unterlagen.

Mit Einsatz eines elektronischen Anordnungsworkflows bietet es sich daher nicht nur an, sämtliche Eingangsrechnungen konsequent auf digitale Rechnungen auszurichten, sondern auch sämtliche Kassenanordnungen über den Anordnungsworkflow abzuwickeln. Hierdurch wird erst die Basis geschaffen, um eine einheitliche elektronische Abwicklung des Anordnungswesens und der elektronischen Aufbewahrung zu etablieren. Gerade im Hinblick auf die mit der Einführung von Workflowsystemen verbundenen Investitionen, die finanziellen jährlichen Aufwendungen und die weiteren eigenen personellen Ressourcen ist darauf zu achten, dass entsprechende Nutzenpotentiale auch ausgeschöpft werden. Die Umsetzung eines solchen Implementierungsprojektes sollte auch dazu genutzt werden, bestehende Prozesse zu hinterfragen und diese ggf. anzupassen.

[53] Vgl. Nr. 5.2 "Effizienzpotenziale von E-Rechnungen" des Leitfadens E-Rechnung (Fn. 7).

Die meisten in der Praxis vorgefundenen Workflowsysteme unterstützen beispielsweise auch die Abwicklung von (Sammel-)Annahme- und Auszahlungsanordnungen[54], allgemeinen Anordnungen und die unterjährig zu erstellenden Feststellungsbescheinigungen oder Anordnungen für Erlass, Stundungen und Niederschlagungen.

Zudem weisen wir darauf hin, dass alle Ansprüche und Zahlungsverpflichtungen zu belegen sind. Die in § 61 KommHV-Kameralistik/§ 57 KommHV-Doppik enthaltenen Grundsätze ordnungsgemäßer Buchführung machen es unter anderem erforderlich, dass jede einzelne Buchung nachvollziehbar ist, d.h. belegt sein muss (sog. Belegzwang, vgl. § 71 Abs. 1 KommHV-Kameralistik/§ 67 Abs. 1 KommHV-Doppik). Die Buchungen müssen durch Kassenanordnungen und Auszahlungsnachweise sowie durch Unterlagen belegt sein, aus denen sich der Zahlungsgrund ergibt (begründende Unterlagen).

Hinsichtlich der begründenden Unterlagen gilt Folgendes:

- Soweit dies zum Verständnis der Kassenanordnungen notwendig ist, sind Unterlagen, aus denen sich der Zahlungsgrund ergibt, grundsätzlich den Kassenanordnungen beizufügen.
- Können Unterlagen nicht beigefügt werden, weil sie z.B. besonders umfangreich sind, so ist durch gegenseitige Hinweise zu gewährleisten, dass Doppelzahlungen vermieden und die Schriftstücke und die Zahlungsanordnung für Zwecke der Rechnungsprüfung zusammengeführt werden können (VV Nr. 3 zu § 38 KommHV a.F.).
- Begründende Unterlagen, die nicht mit der Kassenanordnung zusammengefasst werden, sollen so geordnet werden, dass sie anhand der Kassenanordnungen ohne Schwierigkeiten zur Einsicht und zur Prüfung bereitgestellt werden können (VV Nr. 3 zu § 71 KommHV a.F.).

2.4.2 Ist es zulässig, im Workflowsystem nach dem Prüfschritt „Anordnen“ die Belege automatisiert zu buchen?

➢ Antwort:

Grundsätzlich ist die Buchführung Aufgabe der Kasse, die die Buchung im Sachbuch bzw. im sachlichen Nachweis erst nach der ihr obliegenden formalen Prüfung der Kassenanordnung vornimmt. Für die Wahrnehmung dieser formalen Prüfpflichten sollte daher im Anordnungsworkflow ein eigener Prüfschritt vorhanden sein. Eine automatisierte Buchung durch den Anordnungsberechtigten mit Abschluss des Prüfschritts „Anordnung“ verstößt i.d.R. gegen eine Reihe von haushaltsrechtlichen Grundsätzen.

➢ Im Detail:

Nach § 42 Abs. 1 Nr. 4 KommHV-Kameralistik/§ 38 Abs. 1 Nr. 4 KommHV-Doppik ist die Buchführung originäre Aufgabe der Kasse, falls diese Aufgabe nicht an eine andere Stelle innerhalb der Verwaltung übertragen wurde. Zudem darf die Soll-Buchung im Sachbuch bzw. im sachlichen Nachweis grundsätzlich erst nach der formalen Prüfung der Kassenanordnung durch die

[54] Losgelöst davon, ob die Anordnungsdaten über Schnittstelle ins Finanzverfahren übernommen werden (Integration) oder diese manuell erfasst werden.

Kasse (vgl. § 49 Abs. 2 KommHV-Kameralistik/§ 45 Abs. 2 KommHV-Doppik) vorgenommen werden.

Eine automatisierte Buchung im Sachbuch/sachlichen Nachweis durch den Anordnungsberechtigten beim Workflow-Prüfschritt „Anordnen" verstößt daher gegen den Grundsatz der Trennung von Anordnung und Vollzug (Art. 100 Abs. 2 Satz 3 GO i.V. mit § 38 Abs. 3 KommHV-Kameralistik/§ 34 Abs. 3 KommHV-Doppik) und, sofern sachbearbeitende Tätigkeiten und die Buchführung zusammenfallen, auch gegen den Grundsatz der Funktionstrennung (§ 37 Abs. 1 Nr. 10 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 10 KommHV-Doppik). Die Einhaltung dieser Anforderungen sollte technisch, z.B. durch zusätzliche Prüfschritte im Workflowsystem und ein differenziertes und restriktives Berechtigungskonzept, abgesichert werden (§ 61 i.V. mit § 37 Abs. 1 Nrn. 3 und 5 KommHV-Kameralistik i.V. mit VV Nr. 2 zu § 41 KommHV a.F. sowie Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht, Stand: Januar 2023, Erl. 7 zu § 37 KommHV-Kameralistik).[55]

Der Kasse sollte daher im Workflowsystem ein eigener Prüfschritt zugeordnet werden, über den sie den ihr obliegenden formellen Prüfpflichten nachkommen kann. Mit Abschluss dieses Prüfschrittes durch die Kasse kann dann (automatisiert) die Soll-Buchung vorgenommen werden. Zu den formellen Prüfpflichten gehört zumindest stichprobenweise auch die Kontrolle, ob die auf den Kassenanordnungen angebrachten elektronischen Signaturen gültig sind (vgl. Ausführungen unter Nr. 3.2.1). Eine Ausnahme hiervon kann sich ggf. nach § 38 Abs. 3 i.V. mit § 42 Abs. 2 KommHV-Kameralistik/§ 34 Abs. 3 i.V. mit 38 Abs. 2 KommHV-Doppik ergeben.

Daneben besteht aus technischer Sicht auch die Möglichkeit, die Prüfung der formellen Anforderungen zu automatisieren, um einen möglichst effizienten und friktionslosen elektronischen Anordnungsprozess zu gewährleisten. Neben einer Plausibilisierung der Mindestinhalte einer Zahlungsanordnung nach § 39 Abs. 1 Satz 1 Nrn. 1 bis 9 KommHV-Kameralistik/§ 35 Abs. 1 Satz 1 Nrn. 1 bis 9 KommHV-Doppik bietet es sich insbesondere auch an, die Gültigkeitsprüfung von elektronischen Signaturen im elektronischen Anordnungsworkflow künftig zu automatisieren und das Ergebnis dem Benutzer mit einem entsprechenden Hinweis (z.B. mittels farblicher Kennzeichnung, Flag auf der Signaturkachel) anzuzeigen. Sofern die Workflowsysteme dies nicht bereits implementiert haben, empfehlen wir, entsprechende Verfahrensanpassungen beim Anbieter anzuregen. Mittelfristig ließe sich dies bei großen Verwaltungen mit entsprechender technischer Ausstattung bis hin zu einem einfachen PTP-Prozess[56] i.S. von Abschn. 5.2 der CEN 16931-1:2017[57] weiterentwickeln.

Da die Form und (Mindest-)Inhalte der Feststellungsbescheinigung und Zahlungsanordnungen haushaltsrechtlich vorgegeben sind und der Umfang der Feststellungs-/Anordnungsbefugnisse meist nicht nur in der Dienstanweisung geregelt, sondern beides auch in vielen Finanzverfahren konfigurierbar ist, lassen sich neben der Gültigkeit der elektronischen Signatur auch diese Aspekte automatisiert prüfen (z.B. mit entsprechenden Plausibilitäts- und Berechtigungsprüfungen).

---

[55] Bzw. die gleichlautenden doppischen Vorschriften § 57 i.V. mit § 33 Abs. 1 Nrn. 2 und 5 KommHV-Doppik sowie Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht, Stand Juli 2022, Erl. zu § 33 KommHV-Doppik i.V. mit VV Nr. 2 zu § 41 KommHV a.F. und Schreml/Bauer/Westner, a.a.O., Erl. 7 zu § 37 KommHV-Kameralistik.

[56] Purchase to Pay oder auch Procure to Pay-Prozess (auf Deutsch: Einkauf bis Bezahlung-Prozess); eine Reihenfolge von Vorgängen, die von der Beschaffung bis zum Bezahlen einer Rechnung abgewickelt werden.

[57] Elektronische Rechnungsstellung - Teil 1: Semantisches Datenmodell der Kernelemente einer elektronischen Rechnung; Deutsche Fassung EN 16931-1:2017 (https://www.beuth.de/de/norm/din-en-16931-1/274990963).

Ergänzend weisen wir darauf hin, dass zwar die Buchführung (einschließlich der Sammlung) der Belege einer anderen Stelle innerhalb der Gemeindeverwaltung übertragen werden kann (§ 42 Abs. 1 Nr. 4 KommHV-Kameralistik/§ 38 Abs. 1 Nr. 4 KommHV-Doppik). Dabei gelten für diese Stelle die einschlägigen Vorschriften der KommHV-Kameralistik/KommHV-Doppik dann allerdings in gleicher Weise. Dies bedeutet, dass die Führung von Büchern oder Konten etc. in vollem Umfang Kassengeschäfte bleiben, auch wenn sie durch eine andere Stelle der Gemeinde als die grundsätzlich zuständige Kasse erledigt werden, mit der Maßgabe, dass Anordnungsberechtigte dieser Stelle nicht zugleich mit der Buch- bzw. Kontenführung betraut werden können.

Die Abtrennung von Buchhaltungsgeschäften, also originären Kassenaufgaben, und ihre Übertragung auf eine andere Stelle der Gemeindeverwaltung sollte nur aus zwingenden organisatorischen Gründen in Betracht gezogen werden. Grundsätzlich ist schon aus Gründen der Kassensicherheit dem einheitlichen Vollzug aller Kassengeschäfte in der Einheitskasse (Art. 100 GO) und ihren Zahlstellen der Vorzug zu geben. Eine Übertragung wäre per Dienstanweisung zu regeln.

2.4.3 Wie kann ich die Anforderungen nach § 2b UStG organisatorisch beim Anordnungsworkflow berücksichtigen?

➢ Antwort:

Mit der Erweiterung der Umsatzbesteuerung der öffentlichen Hand durch die Anwendung des § 2b UStG[58] und der damit einhergehenden Zunahme steuerrelevanter Geschäftsvorfälle sowie unter Würdigung der Forderungen im BMF-Schreiben vom 23.05.2016 zum Anwendungserlass zu § 153 AO[59] ist auch ein auf steuerliche Fragestellungen abgestelltes internes Kontrollsystem (IKS) vorzuhalten.[60] Neben der Bündelung entsprechender Kompetenzen an zentraler Stelle (z.B. Steuerstelle) bietet sich es sich u.U. auch an, im elektronischen Anordnungsworkflow einen eigenen Bearbeitungsschritt hierfür vorzusehen (vgl. Graphik, abgebildet unter Nr. 2). Mit zunehmender Verbreitung und Etablierung der digitalen Rechnung können dabei ggf. notwendige steuerliche Vorprüfungs- und Zuleitungsaufgaben bei der Rechnungseingangsstelle durch technische Kontrollen und Workflow-gestützte Zuleitungen unterstützt bzw. ersetzt werden.

➢ Im Detail:

Wir gehen grundsätzlich von einer zentralen Wahrnehmung dieser Aufgaben aus, also sowohl hinsichtlich Rechnungseingangsstelle (vgl. Ausführungen unter Nr. 2.2.1) als auch hinsichtlich der Bündelung von Kompetenzen bei steuerrechtlichen Themen (z.B. Steuerstelle). Als zentrale Unterstützungs-, Steuerungs- und Querschnittsaufgaben mit Finanzbezug bietet es sich daher an, beide Aufgaben im Organisationsbereich Finanzwesen anzusiedeln, um insbesondere eng verbundene Kommunikations- und Abstimmungsprozesse und einheitliche Vorgaben hinsichtlich der Abbildung von steuerrelevanten Geschäftsvorfällen beim elektronischen Anordnungsworkflow zu etablieren.

[58] Die ursprüngliche Übergangsfrist zur Fortführung des alten Rechts, die am 31.12.2020 endete (bei Abgabe einer Optionserklärung), wurde nochmals mit der Beschlussfassung zum Jahressteuergesetz 2022 am 2.12.2022 bis zum 31.12.2024 verlängert (vgl. BT-Drs. 20/4729, Artikel 16, § 27 Abs. 22a UStG).
[59] BMF-Schreiben vom 23.05.2016 zum Anwendungserlass zu § 153 AO; https://www.bundesfinanzministerium.de/
[60] BKPV-Geschäftsbericht 2017, Beitrag „Tax Compliance Management Systeme bei Kommunen und kommunalen Unternehmen", S. 151 ff., https://www.bkpv.de/veröffentlichungen

Dabei sollte eine steuerrechtliche Relevanz bereits beim Auftragsmanagement berücksichtigt werden. Dies bedeutet, dass die für steuerrechtliche Fragen zuständige Stelle nicht erst beim Rechnungsempfang bzw. im Rahmen des Anordnungsworkflows eingebunden werden sollte, sondern z.B. bereits bei der Vergabe von Aufträgen. Dies gilt insbesondere auch beim Abschluss von Verträgen oder Beschaffungen, die eine grundsätzliche steuerrechtliche Bedeutung haben.

Auch hier bietet es sich mit dem zunehmenden Umfang von digitalen Rechnungen an, die Informationen für eine nach Rechnungseingang notwendige steuerrechtliche Bearbeitung im Rahmen des Anordnungsworkflows bereits beim Auftragsmanagement zu berücksichtigen. Dies können insbesondere Buchungs- und Aufteilungsinformationen, notwendige Anpassungen bei Personendaten oder Zuleitungsinformationen sein. Mit einer strukturierten Ausarbeitung der Feinadressierung bei der Leitweg-ID können dann für eine steuerrechtliche Berücksichtigung relevante digitale Rechnungen beim Empfang automatisiert angereichert (sofern eine Verknüpfung zu einem Auftragsmanagement oder den Fachanwendungen besteht) und als Prüfschritt zur steuerrechtlichen Beurteilung im Anordnungsworkflow berücksichtigt werden. Wir verweisen hierzu auf unsere Ausführungen zur Leitweg-ID unter Nr. 2.3.3 Buchst. b als Identifikationskennzeichen.

Die uns in der Praxis bekannt gewordenen Workflowsysteme bieten zudem die Funktionalität, zu den üblichen Prüfschritten (wie z.B. Feststellungsbescheinigung, Anordnung, Kasse) auch weitere Prüfschritte im Workflow zu berücksichtigen. Hiervon haben eine Reihe von Kommunen bereits Gebrauch gemacht und zusätzliche Prüfschritte berücksichtigt, wie beispielsweise Rechnungsprüfung, Steuerstelle, Anlagenbuchhaltung, Kosten- und Leistungsrechnung, oder eine mehrgliedrige Aufteilung der Feststellungsbescheinigung vorgenommen. Mit der zentralen Bündelung der Kompetenzen zu steuerrechtlich relevanten Themen und der zu erwartenden Zunahme an hierbei zu berücksichtigenden Eingangsrechnungen bietet es sich daher an, dies als weiteren optionalen Prüfungsschritt im Workflow vorzusehen (vgl. Graphik, abgebildet unter Nr. 2). Sollte sich der Bedarf für einen zusätzlichen Prüfschritt ergeben, empfehlen wir, diesen im Workflow erst nach Rücklauf der elektronischen Rechnung von den Fachdienststellen zu berücksichtigen, um die Beurteilung der steuerrechtlichen Anforderungen (z.B. Aufteilung der Haushaltsstellen oder Produktkonten, Ergänzungen bei den Personendaten, zu berücksichtigende Rechnungspositionen) auf Basis der sachlich und rechnerisch geprüften Rechnungen vorzunehmen zu können. Gerade die Korrektur von Rechnungspositionen, die Authentizität des Rechnungsstellers bzw. die Zulässigkeit der Rechnung insgesamt, die Aufteilung von Rechnungspositionen auf Einrichtungen u.v.m. kann häufig nur vom Fachamt beurteilt werden.

Je nach Größe der Verwaltung und der Anzahl an steuerrechtlich zu berücksichtigenden Geschäftsvorfällen wird u.U. für die Aufgaben der Steuerstelle kein weiterer zentraler Prüfschritt im Anordnungsworkflow erforderlich sein, da diese Aufgaben z.B. bereits durch eine zentrale Anordnungsstelle in der Kämmerei (ggf. i.V. mit einer externen Beratung) wahrgenommen werden. Bei großen Kommunen kann hingegen der Bedarf bestehen, dass der Prüfschritt im Anordnungsworkflow nicht nur einer zentralen Steuerstelle zuordenbar ist, sondern ggf. auch dezentralen Bündelstellen in einzelnen Fachbereichen, die mit der Bearbeitung steuerrelevanter Fälle für ihre Organisationseinheit betraut sind.

Wir weisen zudem darauf hin, dass über die Validierungsprüfung einer digitalen Rechnung (diese Aufgabe übernimmt i.d.R. das elektronische Rechnungseingangsbuch/Workflowsystem) bereits

automatisiert zahlreiche Kontrollen und Plausibilitäten zu den Rechnungsinhalten vorgenommen werden.[61] Dies betrifft z.B. auch den Ausweis der Umsatzsteuer und die Umsatzsteueraufschlüsselung. Die Plausibilitäten verproben i.d.R. die Einzelpositionen mit den im Rechnungskopf und -fuß dargestellten Daten. Es bietet sich daher an, dies beim Umfang der eigenen (Vor-)Überprüfungen der eingehenden digitalen Rechnung zu berücksichtigen.

2.4.4 Wie binde ich meine nicht an das lokale Netzwerk angeschlossenen Außenstellen/Einrichtungen in den Anordnungsworkflow ein?

➢ Antwort:

Wir empfehlen, die Außenstellen/Einrichtungen möglichst an das lokale Netzwerk und das zentrale Workflowsystem anzubinden, um die Funktionalitäten der Workflowsysteme umfänglich nutzen zu können. Sollte dies nicht möglich sein, können die elektronischen Signaturen der Feststellungsbefugten und des Anordnungsberechtigten auch außerhalb der Workflowsysteme geleistet werden, sofern die haushaltsrechtlichen Anforderungen beachtet werden. Davon abzugrenzen sind Bestätigungen und Sichtvermerke, bei denen es sich lediglich um Informationen zur Sachverhaltsaufklärung handelt und die nicht formgebunden sind.

➢ Im Detail:

Während an das lokale Netzwerk angebundene Außenstellen/Einrichtungen i.d.R. problemlos in den Anordnungsworkflow eingebunden werden können, kann eine rein elektronische Abwicklung des Anordnungswesens bei nicht angebundenen Außenstellen/Einrichtungen oder bei der Beteiligung von externen Dritten (z.B. Ingenieure, Architekten, Schulen) häufig zu Medienbrüchen führen. In der Praxis stellten wir bei dieser Fallkonstellation daher häufig parallele papiergebundene Prozesse mit vermeidbarem Mehraufwand durch Medienbrüche fest (Ausdruck, manuelle Unterschriften, erneutes Digitalisieren). So bestanden z.B. Unsicherheiten, wie die (Teil-)Feststellungsbescheinigungen von Feststellern oder fachtechnische Bescheinigungen von Externen oder nicht angebundenen Außenstellen/Einrichtungen in einem rein elektronischen Anordnungswesen medienbruchfrei realisiert werden können. Auch bei kaufmännisch buchenden Einrichtungen, für die bestimmte Regelungen der Kommunalhaushaltsverordnungen zur Anwendung kamen (vgl. § 10 Abs. 1 Satz 3 EBV), wurden elektronische Signaturen zum Teil nicht über das Workflowsystem unterstützt.

Bei der Anordnung (§ 39 Abs. 1 Satz 2 KommHV-Kameralistik/§ 35 Abs. 1 Satz 2 KommHV-Doppik) sowie bei eigenverantwortlichen (Teil-)Feststellungsbescheinigungen (§ 41 Abs. 1 Satz 2 KommHV-Kameralistik/§ 37 Abs. 1 Satz 2 KommHV-Doppik) oder fachtechnischen Bescheinigungen i.S. von Anlage 1 der VV Nr. 1 zu § 40 KommHV a.F. kann die gesetzlich vorgeschriebene Schriftform nur durch eine mindestens fortgeschrittene elektronische Signatur (§ 87 Nr. 12 KommHV-Kameralistik/§ 98 Nr. 21 KommHV-Doppik) ersetzt werden.

Nicht an das lokale Netzwerk angebundene Außenstellen/Einrichtungen sollten daher möglichst technisch an die zentrale IT-Infrastruktur angebunden werden, um die Funktionalitäten der Workflowsysteme umfänglich nutzen zu können. Dabei bieten z.B. Remote Desktop Services (u.a.

[61] Im Datenmodell der E-Rechnung wurden auch europaweit geltende Geschäftsregeln und Integritätsbedingungen berücksichtigt. Zum Kontroll- und Plausibilisierungsumfang vgl. DIN EN 16931-1:2017 - Semantisches Datenmodell, Nr. 6.4. Geschäftsbedingungen.

Terminalserverlösungen) performante Möglichkeiten, auch Außenstellen/Einrichtungen anzubinden, die nur über eine geringe Bandbreite beim Zugang zu den Online-Diensten verfügen. Die Anbindung an eine zentrale IT-Infrastruktur bietet darüber hinaus zahlreiche weitere technische und organisatorische Vorteile.

Sofern dies nicht möglich ist oder sich die notwendigen Bescheinigungen und die Unterschrift des Anordnungsberechtigten (noch) nicht im Rahmen des Anordnungsworkflows abbilden lassen, muss u.E. nicht zwangsläufig auf die Schriftform mit manuellen Unterschriften ausgewichen werden. In den meisten Fällen ist ebenfalls eine medienbruchfreie elektronische Abwicklung möglich, wenn die formgebundene Bescheinigung oder die Anordnung mit einer elektronisch signierten E-Mail oder PDF-Datei übermittelt werden kann. Die zugelassenen elektronischen Signaturen können somit grundsätzlich auch außerhalb der Workflowsysteme mit anderen Lösungen erstellt werden (z.B. Governikus-Signer[62] oder Banken-Signatur), wenn diese die in § 87 Nr. 12 KommHV-Kameralistik/§ 98 Nr. 21 KommHV-Doppik und in den AFS-HKR festgelegten Anforderungen erfüllen.

Soweit es sich bei den Außenstellen/Einrichtungen oder externen Dritten hinsichtlich der Bestätigungen und Sichtvermerke lediglich um Informationen zur Sachverhaltsaufklärung und nicht um eigenverantwortliche (Teil-)Feststellungsbescheinigungen oder fachtechnische Bescheinigungen handelt, können die Bestätigungen in diesen Fällen auch nicht formgebunden (und damit auch ohne fortgeschrittene Signatur) per einfacher E-Mail oder in Textform eingeholt werden. Liegen alle entscheidungsrelevanten Informationen vor, könnte der zuständige Feststellungsbefugte mit seiner sachlichen und rechnerischen Feststellung letztlich die Gesamtverantwortung für die Richtigkeit der Zahlungsverpflichtung (mit einer Rechnung fakturierte Lieferungen oder Leistungen) oder des Anspruchs (z.B. bei Gewährung von Gutschriften) übernehmen und dies mittels fortgeschrittener Signatur über den Anordnungsworkflow bescheinigen.

Sollten entsprechende Bescheinigungen auf selbst erstellten Eigen-/Hilfsbelegen (z.B. digitale Kopien) oder weiteren Unterlagen (wie z.B. Lieferscheinen) geleistet werden, ist sicherzustellen, dass diese Unterlagen als rechnungsbegründende Unterlage mit zum Rechnungsoriginal und zur Anordnung gegeben werden und in einer gemeinsamen digitalen Belegmappe elektronisch aufbewahrt werden (vgl. auch Nr. 2.2.2 Buchstabe a).

2.5 Aufbewahrung von Belegen

Zur elektronischen Aufbewahrung von Kassenbelegen haben wir bereits in unseren Geschäftsberichten 2004[63], 2006[64] und 2011[65] Beiträge veröffentlicht. Wir möchten daher nachfolgend im Wesentlichen auf Fragestellungen zur (elektronischen) Belegaufbewahrung eingehen, die sich aus der geänderten Vorgehensweise durch den elektronischen Anordnungsworkflow (Verlagerung vom sog. späten Scannen in der Kasse hin zum sog. frühen Scannen in der Rechnungseingangsstelle und Übernahme von elektronischen Rechnungen in ein elektronisches Rechnungs-

[62] https://www.governikus.de/loesungen/produkte/data-boreum/
[63] Geschäftsbericht 2004, Elektronische Archivierung von Buchungsbelegen in Kommunalkassen, S. 28 ff.
[64] Geschäftsbericht 2006, Elektronische Archivierung von Buchungsbelegen in Kommunalkassen (Scan-Dienstanweisung und weitere Fragestellungen), S. 78 ff.
[65] Geschäftsbericht 2011, Elektronische Archivierung von Belegen in Kommunalkassen – Prüfungserfahrungen, Praxisfragen sowie weitere Hinweise –, S. 53 ff.

eingangsbuch bzw. Workflowsystem) oder aus den geänderten rechtlichen Rahmenbedingungen ergeben. Ansonsten verweisen wir auf die angeführten Geschäftsberichte, die in ihren grundlegenden Ausführungen weitgehend auf die aktuellen Verhältnisse übertragbar sind.

2.5.1 Was bedeutet revisionssichere Aufbewahrung in einem elektronischen Belegarchiv?

➢ Antwort:

Nach den seit 01.09.2018 geltenden haushaltsrechtlichen Vorschriften müssen Belege und begründende Unterlagen in einer Weise gespeichert werden, die ihre Unveränderbarkeit gewährleistet. Sinn und Zweck dieser technikneutralen Bestimmung ist, die Integrität (Unversehrtheit des Inhalts), Authentizität (Echtheit der Herkunft) und Verfügbarkeit sowie die Revisionsfähigkeit der elektronisch gespeicherten Belege für die Dauer der Aufbewahrungsfristen sicherzustellen (§ 71 Abs. 2 Satz 1, § 82 Abs. 2 und 4 KommHV-Kameralistik/§ 67 Abs. 2 Satz 1, § 69 Abs. 2 und 4 KommHV-Doppik). Die Anforderungen sind mit technischen und organisatorischen Maßnahmen sicherzustellen.

➢ Im Detail:

a) Begriff der Unveränderbarkeit

Mit der Verordnung zur Änderung der Kommunalhaushaltsverordnungen vom 20.07.2018, GVBl. S. 674, die am 01.09.2018 in Kraft trat, wurden die Anforderungen in § 71 Abs. 2 KommHV-Kameralistik/§ 69 Abs. 2 KommHV-Doppik an das Speichermedium technikneutraler gestaltet, um Optimierungs- und Rationalisierungspotentiale für die Kommunen zu ermöglichen.[66] Seit 01.09.2018 ist daher der Einsatz eines speziellen, nicht veränderbaren elektronischen Speichermediums (WORM-Mediums) nicht mehr zwingend erforderlich. Die grundlegende Anforderung, dass die elektronisch aufbewahrten Belege in einer Weise gespeichert werden müssen, die deren Unveränderbarkeit gewährleistet, blieb allerdings weiterhin erhalten. Die neue Regelung ist lediglich offener für andere technische und organisatorische Maßnahmen, die diese Anforderung ebenfalls sicherstellen können.[67] Vor Aufnahme des Wirkbetriebs ist daher von der einsetzenden Stelle zu prüfen, ob diese gesetzliche Anforderung tatsächlich erfüllt wird. Dies ist in der haushaltsrechtlichen Freigabe des für die Belegarchivierung verwendeten Verfahrens nach § 37 Abs. 1 Nr. 1 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 1 KommHV-Doppik nachvollziehbar zu dokumentieren.

Der unbestimmte Rechtsbegriff der „Unveränderbarkeit" ist weder in den aktuell geltenden Kommunalhaushaltsverordnungen noch in der Begründung der Änderungsverordnung vom 20.07.2018 näher definiert. Er ist deshalb mit Blick auf die allgemeinen haushaltsrechtlichen Grundsätze für die Buchführung (§ 61 KommHV-Kameralistik/§ 57 KommHV-Doppik) und die ergänzend herangezogenen steuerrechtlichen Bestimmungen[68] (§ 146 Abs. 4 und 5 und § 147

[66] Vgl. IMS vom 05.09.2018, Az: B4-1512-3-3/B4-1512-7-2, Abschn. 2.5., https://www.stmi.bayern.de/kub/komfinanzen/haushaltsrecht/index.php
[67] Die zur Sicherung und Kontrolle ergriffenen technischen und organisatorischen Maßnahmen sind in einer Dienstanweisung zu regeln (vgl. § 37 Abs. 2 KommHV-Kameralistik/§ 33 Abs. 2 KommHV-Doppik).
[68] Vgl. vom AWV im Internet veröffentlichten GoBD-Praxisleitfaden für Unternehmen, Version 1.0 (Stand 28.03.2018, S. 113-115) und die dort genannte weitere Quelle (S. 115 unten); https://www.awv-net.de.

Abs. 2 und 5 AO, Rzn. 58 und 107 ff. GoBD) auszulegen. Die neuen haushaltsrechtlichen Vorschriften vom 01.09.2018 zielten darauf ab, keine neuen oder zusätzlichen Anforderungen an die Aufbewahrung von Belegen zu schaffen und eine einheitliche Handhabung sicherzustellen. Der Verweis in § 69 Abs. 2 Satz 3 KommHV-Doppik auf § 147 Abs. 3 AO deutet bereits eine gemeinsame Zielrichtung an.

Die Unveränderbarkeit im Sinne von § 71 Abs. 2 Satz 1 KommHV-Kameralistik und § 67 Abs. 2 Satz 1 KommHV-Doppik ist aus unserer Sicht gewährleistet, wenn folgende Anforderungen erfüllt werden:

- Ein bereits gebuchter, elektronisch aufbewahrter Beleg i.S. des § 71 Abs. 1 KommHV-Kameralistik/§ 67 Abs. 1 KommHV-Doppik darf nicht in einer Weise verändert, gelöscht oder ausgetauscht werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Dies setzt eine entsprechende Protokollierung der Änderungs- oder Löschvorgänge in einem Dokumentenmanagement- oder Archivsystem voraus.[69]
- Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später erfolgten. Es muss also stets ersichtlich sein, wann der Beleg im Belegarchiv gespeichert, geändert oder gelöscht wurde.[70]
- Das für die Aufbewahrung von Belegen eingesetzte automatisierte Verfahren muss gewährleisten, dass gespeicherte Belege nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert, verfälscht oder ersetzt werden können.[71]
- Die Integrität, Authentizität und Verfügbarkeit der Daten und Datensätze (Metadaten) und elektronisch aufbewahrten Belegdokumente[72] ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Die Ablage von Daten und elektronischen Dokumenten in einem Dateisystem erfüllt diese Anforderungen regelmäßig nicht, soweit nicht geeignete zusätzliche Maßnahmen ergriffen werden, die dies nachvollziehbar gewährleisten.[73]
- Spätere Änderungen sind ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar bleiben.[74]
- Wenn Buchungsvermerke, elektronischen Signaturen, Siegel, Indexierungen, Barcodes, farblichen Markierungen oder sonstige Hinzufügungen angebracht werden, darf dies keinen Einfluss auf die Lesbarmachung des Originalzustands haben.[75]

Mit diesen Anforderungen ist es daher nicht vereinbar, wenn die elektronisch aufbewahrten Belege im Dateisystem auf normalen Server-Festplatten, Netzwerkspeichersystemen (NAS; Network-Attached Storage) oder Speichernetzwerken (SAN; Storage Area Network) ohne zusätzliche Schutzmaßnahmen, die eine Unveränderbarkeit im o.g. Sinne gewährleisten, gespeichert werden.

---

[69] Vgl. § 146 Abs. 4 Satz 1 AO i.V. mit Rzn. 58, 59 und 107 GoBD 2019, BStBl. I S. 1269.
[70] Vgl. § 146 Abs. 4 Satz 2 AO i.V. mit Rz. 107 GoBD 2019, a.a.O.
[71] Vgl. § 146 Abs. 5 AO i.V. mit Rz. 108 GoBD 2019, a.a.O.
[72] Kassenanordnungen oder begründende Unterlagen in PDF- oder Bildformaten, die entweder durch das Scannen von Papieroriginalen in einem qualitätsgesicherten Scanprozess digitalisiert wurden oder bereits in originär elektronischer Form bei der Kommune eingegangen sind bzw. selbst erstellt werden.
[73] Vgl. 146 Abs. 5 Satz 4 AO i.V. mit Rz. 110 GoBD 2019, a.a.O.
[74] Vgl. 146 Abs. 5 Satz 4 AO i.V. mit Rz. 111 GoBD 2019, a.a.O.
[75] Vgl. 146 Abs. 5 Satz 4 und § 147 Abs. 2 AO i.V. mit Rz. 123 GoBD 2019, a.a.O.

Die o.g. Verpflichtung kann nach dem Stand der Technik u.E. besonders gut mit Festplatten-Speichermedien, die WORM-Eigenschaften besitzen, realisiert werden. Diese Medien können mittels spezieller Soft- und/oder Hardware so konfiguriert werden, dass die dort gespeicherten Dateien für einen vom Administrator oder vom automatisierten Verfahren vorgegebenen Zeitraum (sog. retention time) nicht mehr veränderbar oder löschbar sind. Zudem ermöglichen Festplattensysteme einen sehr schnellen und effizienten Zugriff auf die dort abgelegten Belegdokumente.

Nach den neuen haushaltsrechtlichen Bestimmungen kommen aber auch andere technische und organisatorische Maßnahmen in Betracht, die eine Unveränderbarkeit der gespeicherten Belegdokumente sicherstellen. Neben der obligatorischen, vom Benutzer oder Administrator nicht beeinflussbaren automatischen Versionierung (z.B. bei einer Änderung oder einem Austausch von Belegdokumenten) setzt dies u.a. eine restriktive Rechtevergabe im Dokumentenmanagement- oder Archivsystem voraus (z.B. kein Recht zum Löschen von Belegdokumenten oder Belegmappen).

Im Übrigen wird auf Nr. 3.2 der Finanzplanungsbekanntmachung 2007 bis 2011[76] und die Beiträge zur „Elektronischen Archivierung von Buchungsbelegen in Kommunalkassen" in den BKPV-Geschäftsberichten 2004, 2006 und 2011 verwiesen.

b) Elektronische Kontoauszüge

Nachweise zu Gutschriften und Lastschriften der Kreditinstitute sind wie Belege aufzubewahren (vgl. § 82 Abs. 2 Satz 5 KommHV-Kameralistik/§ 69 Abs. 2 Satz 6 KommHV-Doppik). Bei Kontoauszügen (z.B. als Einzahlungsnachweise für Einnahmebuchungen bzw. für die Buchung von Erträgen) handelt es sich demnach um Belege, deren Ordnung durch Dienstanweisung bestimmt wird (vgl. Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht, Stand: Januar 2023, Erl. 4 zu § 71 KommHV-Kameralistik/Erl. 4 zu § 67 KommHV-Doppik). Dabei gelten die Vorschriften des § 71 Abs. 2 KommHV-Kameralistik/§ 67 Abs. 2 KommHV-Doppik sowohl für Auszahlungsnachweise als auch für Einzahlungsnachweise, sofern Belege beim Einsatz automatisierter Verfahren elektronisch aufbewahrt werden.

Wir verweisen hierzu insgesamt auf unseren BKPV-Geschäftsbericht 2016 mit dem Thema „Empfang und Aufbewahrung elektronischer Kontoauszüge", S. 59 ff.[77] Unsere Ausführungen unter Nr. 3.2.2 Buchst. c dieses BKPV-Geschäftsberichtsbeitrags gelten unter Berücksichtigung der Änderung der Kommunalhaushaltsverordnungen vom 20.07.2018 mit der Maßgabe, dass elektronische Kontoauszüge nunmehr in einer Weise zu speichern sind, die deren Unveränderbarkeit sicherstellen. Ein dediziertes WORM-Speichermedium ist daher nicht mehr obligatorisch (vgl. Ausführungen unter Buchst. a).

c) Elektronischer Tagesabschluss/Tagesabgleich

Sofern Tagesabschlüsse (Kameralistik) bzw. Tagesabgleiche (Doppik) elektronisch signiert werden, muss die Unveränderbarkeit auch für die elektronisch aufbewahrten Tagesabschlüsse/Tagesabgleiche sichergestellt werden (§ 72 Abs. 1 Sätze 2 und 4 KommHV-Kameralistik/§ 68 Abs. 1 Sätze 3 und 5 KommHV-Doppik i.V. mit Schreml/Bauer/Westner, a.a.O., Erl. 4 zu § 72 KommHV-Kameralistik/Erl. 3 zu § 68 KommHV-Doppik). Dies gilt auch für die manuell unterschriebenen

[76] IMBek. vom 06.02.2008, Az.: IB4-1512.5-9, AllMBl Nr. 3/2008, S. 152
[77] Vgl. https://www.bkpv.de/veroeffentlichungen, Rubrik „Unsere regelmäßigen Veröffentlichungen"

Tagesabschlüsse/Tagesabgleiche, wenn diese elektronisch aufbewahrt werden und die papiergebundenen Originale dabei ersetzend gescannt wurden. Zum Begriff der Unveränderbarkeit vgl. Ausführungen unter Buchst. a).

2.5.2 Was gilt bei der Aufbewahrung der papiergebundenen Originalbelege?

➢ Antwort:

Nach den geltenden hausrechtlichen Bestimmungen sollen die gescannten Originalrechnungen nicht vor Abschluss der örtlichen Prüfung der Jahresrechnung vernichtet werden,[78] soweit keine entgegenstehenden Pflichten zur Rückgabe oder Aufbewahrung bestehen. Von der Soll-Vorschrift kann nur in begründeten Ausnahmefällen und nur nach entsprechender Risikoabwägung in Abstimmung mit der Kasse und der örtlichen Rechnungsprüfung abgewichen werden. Eine Aufbewahrung der gescannten Papieroriginale in Stapelform genügt. Die Belegarchivierung steht unter der Gesamtverantwortung der Kasse.

➢ Im Detail:

Mit dem sog. späten Scannen, also mit der Digitalisierung der papiergebundenen Belege nach Abwicklung des Anordnungswesens und der Buchführung in der Kasse, wurden i.d.R. auch die Sammlung und Aufbewahrung der Papierbelege in der Kasse vorgenommen. Mit der Einführung von elektronischen Rechnungseingangsbüchern/Workflowsystemen hat sich die Digitalisierung der Belege auf die Rechnungseingangsstelle oder in Einzelfällen auf die Fachämter vorverlagert (sog. frühes Scannen). Im Rahmen unserer Prüfungen haben wir daher regelmäßig eine uneinheitliche Handhabung im Umgang mit den papiergebundenen Originalen vorgefunden. Beispielsweise wurden die Papierbelege bereits zeitnah nach dem Digitalisieren vernichtet oder Art und Umfang der Aufbewahrung und der Aussonderung oblag einer uneinheitlichen Arbeitsweise der einzelnen Beschäftigten, ohne dass hier entsprechende Regelungen erlassen worden wären.

a) Zuständigkeit

Nach § 42 Abs. 1 Nr. 4 KommHV-Kameralistik/§ 38 Abs. 1 Nr. 4 KommHV-Doppik ist die Kasse für die Sammlung der Belege zuständig, soweit nicht eine andere Stelle damit beauftragt wurde. Auch mit der Beauftragung einer anderen Stelle bleibt dies Kassengeschäft, bei dem alle haushaltsrechtlichen Anforderungen zu berücksichtigen sind (vgl. Buchst. b).

Sofern die digitalisierten begründenden Unterlagen mit zur Anordnung gegeben und im elektronischen Belegarchiv aufbewahrt[79] und nicht aus organisatorischen oder rechtlichen Gründen in den Fachbereichen eingehen und aufbewahrt werden sowie Teil der dortigen fachbereichsspezifischen Aktenführung sind (z.B. Soziales, Jugendhilfe, Beihilfe; VV Nr. 3 zu 38 KommHV a.F., Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht in Bayern – Praktikerhandbuch, Stand Januar 2023, Erl. 4 zu § 39 KommHV-Kameralistik/Erl. 4 zu § 35 KommHV-Doppik), sollte ebenfalls eine zentrale Sammlung der papiergebundenen Originale etabliert werden,

[78] Sog. ersetzendes Scannen mit verzögerter Vernichtung der papiergebundenen Originale, vgl. hierzu die ausführliche Darstellung in der Begründung der Verordnung zur Änderung kommunalwirtschaftlicher Vorschriften vom 05.10.2007, S. 44 ff.
[79] Vgl. auch Ausführungen unter Nr. 2.4.1 unten.

die von der Kasse organisiert wird. Die Gesamtverantwortung für die Aufbewahrung und Aussonderung verbleibt in der Kasse. Das Nähere ist per Dienstanweisung zu regeln (vgl. Nr. 2.1.2).

b) Aufbewahrung und Aussonderung

Digitalisierte Papierrechnungen (Digitalisat) können aus haushaltsrechtlicher Sicht grundsätzlich anstelle der papiergebundenen Originale verwendet und aufbewahrt werden, soweit keine entgegenstehenden Pflichten zur Rückgabe oder Aufbewahrung bestehen (vgl. Art. 33 Abs. 3 Satz 2 BayDiG[80] i.V. mit § 71 Abs. 2 u. 4 KommHV-Kameralistik/§ 67 Abs. 2 u. 4 KommHV-Doppik).

Nach den haushaltsrechtlichen Bestimmungen sollen die nicht mehr benötigten Unterlagen jedoch nicht vor Abschluss der örtlichen Prüfung der Jahresrechnungen vernichtet werden (gesetzlich bestimmter Aufbewahrungszeitraum gescannter Papieroriginale; vgl. § 71 Abs. 2 Satz 2 KommHV-Kameralistik/§ 67 Abs. 2 Satz 2 KommHV-Doppik). Der Zeitpunkt für die Vernichtung ist in Abstimmung mit der Kasse und dem örtlichen Rechnungsprüfungsorgan festzulegen. Von der gesetzlich vorgegebenen Standard-Aufbewahrungsfrist (Soll-Vorschrift) darf nur in begründeten Ausnahmefällen abgewichen werden. Insoweit wird den Kommunen nur ein begrenzter Ermessensspielraum eingeräumt, der auch eine entsprechende Risikoabwägung[81] erfordert.

Eine spezielle Ordnung der gescannten papiergebundenen Belege ist nicht vorgegeben, es genügt somit auch deren Ablage in Stapelform. § 71 Abs. 3 KommHV-Kameralistik/§ 67 Abs. 3 KommHV-Doppik gelten nur für das führende (elektronische) Belegarchiv.

Dem ersetzenden Scannen von Papierrechnungen können aber Pflichten zur Rückgabe oder Aufbewahrung i. S. von Art. 33 Abs. 3 Satz 2 BayDiG entgegenstehen. Solche Verpflichtungen können sich u.a. aus steuerrechtlichen Bestimmungen (z.B. Zollpapiere – vgl. § 147 Abs. 1 Nr. 4a AO), aus außersteuerlichen Vorschriften (z.B. Aufbewahrungsfristen nach § 71 Abs. 2 Sätze 2 und 3 KommHV-Kameralistik/§ 67 Abs. 2 Sätze 2 und 3 KommHV-Doppik), Nebenbestimmungen in Förderbescheiden oder ggf. aus beweisrechtlichen Gründen (z.B. während eines laufenden Gerichtsverfahrens)[82] ergeben.

Da bei Erlass der haushaltsrechtlichen Vorschriften das Modell des „frühen ersetzenden Scannens" noch nicht berücksichtigt wurde, weisen wir darauf hin, dass bei der anzustellenden Risikoabwägung zu beachten ist, dass alle weiteren Entscheidungs- und Kontrollprozesse nur noch auf der digitalen Kopie (Digitalisat) beruhen und auf dieser eine hohe Informations- und Beweislast liegt.

[80] Art. 33 BayDiG gilt seit 01.08.2022 und ersetzt Art. 7 BayEGovG, der bis 31.07.2022 galt.
[81] Vgl. Begründung der Verordnung zur Änderung kommunalwirtschaftlicher Vorschriften, zu § 71 KommHV-Kameralistik bzw. § 67 KommHV-Doppik.
[82] Vgl. Finanzgericht Münster, Beschluss vom 24.11.2015, Az: 14 K 1542/15 AO PKH.

2.5.3 Welche Anforderungen sind beim elektronischen Belegarchiv im Outsourcing-Betrieb zu beachten?

➢ Antwort:

Der Betrieb des elektronischen Belegarchivs bei einem externen Dritten stellt aus kommunalrechtlicher Sicht eine Übertragung von Kassen- und Rechnungsgeschäften dar. Gemäß Art. 101 GO ist dies nur dann zulässig, wenn die ordnungsgemäße und sichere Erledigung und die Prüfung nach den für die outsourcende Stelle geltenden Vorschriften gewährleistet sind. Darüber hinaus sind datenschutzrechtliche Anforderungen zu berücksichtigen und die Einhaltung der informationstechnischen Schutzziele sicherzustellen.

➢ Im Detail:

Wir verweisen hierzu insgesamt auf die Ausführungen im Leitfaden zum Outsourcing kommunaler IT[83]. Bei einer derartigen Verlagerung auf externe Dritte ist insbesondere Folgendes zu beachten:

- Mit einer Wirtschaftlichkeitsbetrachtung wäre zu bestimmen, ob das Outsourcing auch unter den in Art. 61 GO genannten allgemeinen Haushaltsgrundsätzen die zweckmäßigste und wirtschaftlichste Lösung darstellt. Auch andere Regelungen greifen den Aspekt der wirtschaftlichen Aufgabenerfüllung auf.[84]
- Bei einem Outsourcing finanzwirksamer Verfahren, elektronischer Bücher und Belege muss sichergestellt sein, dass eine ordnungsgemäße und sichere Erledigung nach den für die Kommune geltenden Vorschriften gewährleistet ist. Insbesondere wäre von der Kommune darauf zu achten, dass vom Outsourcing-Dienstleister die in den § 37 Abs. 1 Nrn. 3 bis 9, § 43 Abs. 1 Nr. 3, § 61, § 62 Abs. 1 Satz 3, § 71 Abs. 2 Satz 1 und Abs. 4 und § 82 Abs. 4 KommHV-Kameralistik/§ 33 Abs. 1 Nrn. 3 bis 9, § 39 Abs. 1 Nr. 3, § 58 Abs. 1 Satz 3, § 67 Abs. 2 Satz 1 und Abs. 4 und § 69 Abs. 4 KommHV-Doppik genannten haushaltsrechtlichen Verpflichtungen durch geeignete technische und organisatorische Maßnahmen eingehalten werden.
- Ebenso müssen sich die für die örtliche Prüfung im Sinne des Art. 103 GO und die überörtliche Prüfung im Sinne des Art. 105 GO zuständigen Prüfungsorgane von der ordnungsgemäßen Erledigung der übertragenen Geschäfte insbesondere nach Maßgabe von Art. 106 sowie Art. 120 Abs. 1 GO in Verbindung mit der Kommunalwirtschaftlichen Prüfungsverordnung (KommPrV) vergewissern können (Art. 101 GO, Nr. 2.1.6 des Leitfadens zum Outsourcing kommunaler IT). Dies wäre über eine entsprechende vertragliche Vereinbarung mit dem Outsourcing-Dienstleister sicherzustellen. Auf § 6 KommPrV sowie die dazu ergangenen Verwaltungsvorschriften wird hingewiesen.
- Die datenschutzrechtlichen Anforderungen müssen beachtet werden, welche im Leitfaden zum Outsourcing kommunaler IT näher konkretisiert sind.
- Die informationstechnischen Schutzziele wären zu gewährleisten (Art. 43 Abs. 1 BayDiG[85]). Die Sicherheitskonzepte des jeweiligen Outsourcing-Dienstleisters und deren Umsetzung

[83] Vgl. IMS vom 30.03.2021, Az.: A7-1081-1-72 (https://www.stmi.bayern.de/assets/stmi/sus/datensicherheit/2021-03-18_b1_a7-1081-1-72_ims_leitfaden_outsourcing__reinschrift_.pdf), und den Leitfaden zum Outsourcing kommunaler IT unter https://www.datenschutz-bayern.de/technik/orient/outsourcing.pdf
[84] Regelungen in § 80 Abs. 3 Satz 1 Nr. 2 SGB X und Art. 108 Abs. 3 Satz 1 BayBG.
[85] Art. 43 Abs. 1 BayDiG gilt seit 01.08.2022 und ersetzt Art. 11 Abs. 1 BayEGovG, der bis 31.07.2022 galt.

wären bei den eigenen Sicherheitskonzepten zu berücksichtigen und die eigenen technischen und organisatorischen Maßnahmen darauf abzustimmen.

- Losgelöst davon, ob das elektronische Belegarchiv im Outsourcing oder selbst betrieben wird, bleibt die einsetzende Stelle für die haushaltsrechtliche Freigabe der finanzwirksamen Verfahren zuständig (§ 37 Abs. 1 Nr. 1 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 1 KommHV-Doppik). Die einsetzende Stelle hat sich zumindest stichprobenweise von der ordnungsgemäßen Abwicklung zu überzeugen (VV Nr. 3 zu § 42 KommHV a. F., Nr. 2.2.4 i.V. mit Nr. 2.4.4.4 A.12. des Leitfadens zum Outsourcing kommunaler IT). Zudem dürfte es zweckmäßig sein zu vereinbaren, dass der Outsourcing-Dienstleister der einsetzenden Stelle gegenüber jeweils bescheinigt, dass das elektronische Belegarchiv ordnungsgemäß betrieben wird (z.B. Gewährleistung der Unveränderbarkeit, Zugriffschutz, Maßnahmen, die die Vollständigkeit und Verfügbarkeit über die Aufbewahrungsfristen gewährleisten).[86] Diese Bescheinigung sollte dann bei der Verfahrensfreigabe nach § 37 Abs. 1 Nr. 1 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 1 KommHV-Doppik vorliegen.

2.5.4 Welche Anforderungen gelten hinsichtlich der Belegrecherche?

➢ Antwort:

Die Belegaufbewahrung steht unter der Gesamtverantwortung der Kasse. Diese kann ihrer Verantwortung zur ordnungsgemäßen Führung und zur Vollständigkeitskontrolle des elektronischen Belegarchivs u.E. nur nachkommen, wenn ihr entsprechend flexible Möglichkeiten zur Recherche der digitalisierten Belege zugänglich sind. Auch den örtlichen und überörtlichen Rechnungsprüfungsorganen sollten geeignete Auswertungsmöglichkeiten zur Verfügung stehen.

➢ Im Detail:

In der Praxis stellen wir regelmäßig fest, dass der Kasse oder den Rechnungsprüfungsorganen trotz elektronischer Belegarchivierung keine ausreichend flexible Recherche auf das elektronische Belegarchiv möglich ist. Exemplarisch listen wir hier einige Konstellationen auf:

- Die Recherche von Belegen bedurfte jeweils mehrstufiger Bearbeitungsschritte.
- Die Belege waren übermäßig in einzelne Dokumente aufgeteilt, die sich nur modal öffnen ließen und somit eine Verprobung sehr aufwendig gestalteten.
- Die Buchungsdaten waren nicht mit dem Beleg per Schnittstelle verbunden.
- Die Auswahl- und Suchfelder des Clients zur Archivrecherche entsprachen nicht den Mindestanforderungen an den Inhalt von Zahlungsanordnungen.[87]
- Die mittels der proprietären Viewer angezeigten Belege ließen keine Prüfung der elektronisch angebrachten Signaturen zu.
- Nach der Migration des elektronischen Belegarchivs auf eine neue Software waren nicht mehr alle Belegmappen recherchierbar.

[86] Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht in Bayern – Praktikerhandbuch, Stand: Januar 2023., Erl. zu 3.4 zu § 42 KommHV-Kameralistik/Erl. zu 3.4 zu § 38 KommHV-Doppik.
[87] § 39 Abs. 1 KommHV-Kameralistik, vgl. Nr. 3.5.3 „Maschinelle Auswertbarkeit" des BKPV-Geschäftsberichts 2004.

Nach den in den Kommunalhaushaltsverordnungen enthaltenen Bestimmungen für die Prüfung von Ansprüchen und Zahlungsverpflichtungen (§ 41 Abs. 1 KommHV-Kameralistik/§ 37 Abs. 1 KommHV-Doppik)[88] und den Grundsätzen für die kommunale Buchführung (§ 61 KommHV-Kameralistik/§ 57 KommHV-Doppik) müssen sich die Geschäftsvorfälle vollumfänglich in ihrer Entstehung und Verarbeitung verfolgen lassen (§ 61 Abs. 2 KommHV-Kameralistik/§ 57 Abs. 2 KommHV-Doppik), also sowohl vom Beleg zum Buchungssatz (progressiv) als auch vom Buchungssatz zum Beleg (retrograd) prüfbar sein. Insoweit sind die haushaltsrechtlichen Anforderungen an die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit von Rechnungen nahezu identisch mit den steuerrechtlichen Bestimmungen.[89]

Um einen zeitnahen Zugriff auf Belege zu gewährleisten, muss daher eine geeignete technische Ausstattung zur Verfügung stehen, die eine wahlfreie und effiziente Recherche der gespeicherten Belege zulässt und nicht nur auf sachbearbeitende Funktionen beschränkt ist (vgl. § 71 Abs. 3 und 4 KommHV-Kameralistik/§ 67 Abs. 3 und 4 KommHV-Doppik). Beim Einsatz proprietärer Viewer und Archivrecherche-Clients muss zudem sichergestellt sein, dass bei elektronisch aufbewahrten Belegen erkennbar ist, ob die verwendeten Signaturen korrekt verwendet wurden und zum Zeitpunkt der Signatur gültig waren.

Auch den örtlichen und überörtlichen Rechnungsprüfungsorganen sollten hierfür geeignete Auswertungsmöglichkeiten zur Verfügung stehen und darauf geachtet werden, dass die Revisionsfähigkeit des elektronischen Belegarchivs nicht eingeschränkt ist (Art. 106 Abs. 6 Satz 3 GO i. V. mit § 1 Abs. 3 KommPrV).[90]

Bei einer elektronischen Aufbewahrung von Belegen und begründenden Unterlagen i.S. von § 71 KommHV-Kameralistik oder § 67 KommHV-Doppik muss darüber hinaus sichergestellt sein, dass

- die Belege und zahlungsbegründenden Unterlagen unabhängig von der Ablagesystematik nach der zeitlichen und sachlichen Buchung ausgewertet und angezeigt werden können (z.B. durch entsprechende Filterung und Sortierung),
- die gespeicherten Akten, Vorgänge oder Dokumente sowohl anhand der beschreibenden Daten (Metadaten) als auch nach den in den Dokumenten enthaltenen Textinformationen (Volltext) gesucht, ausgewertet und angezeigt werden können und beide Suchmöglichkeiten kombinierbar sind,
- die Belege und zahlungsbegründenden Unterlagen unter einem eindeutigen Index verwaltet werden, der eine zeitnahe Zusammenführung aller für die Prüfung relevanten Informationen ermöglicht, unabhängig davon, ob die elektronisch aufbewahrten Unterlagen in zentralen Finanzverfahren, finanzwirksamen Fachverfahren, elektronischen Belegarchiven oder Dokumentenmanagementsystemen abgelegt sind oder ggf. noch in Papierform (hybride Aktenführung) aufbewahrt werden,

[88] Diese gesetzlichen Bestimmungen i.V. mit den örtlichen Dienstanweisungen stellen u.E. ein innerbetriebliches Kontrollverfahren i.S. von § 14 Abs. 1 Satz 6 UStG dar (sog. verlässlicher Prüfpfad – vgl. BKPV-Geschäftsbericht 2011, S. 66 ff.).
[89] Vgl. dazu ausführlich die Gesetzesbegründung zu § 14 Abs. 1 und 3 UStG in der BT-Drs. 17/5125 vom 21.03.2011 und im BMF-Schreiben vom 02.07.2012, Az: IV D 2 - S 7287-a/09/10004 :003 (https://www.bundesfinanzministerium.de, Rubrik BMF-Schreiben).
[90] Vgl. auch Ausführungen unter Nr. 2.2.8 „Anforderungen an die Ausstattung des Prüfer-Arbeitsplatzes" unseres Beitrags „Elektronische Archivierung von Belegen in Kommunalkassen - Prüfungserfahrungen, Praxisfragen sowie weitere Hinweise" in unserem Geschäftsbericht 2011.

- immer auch das empfangene elektronische Dokument und nicht nur der vom elektronischen Dokument erstellte Papierausdruck aufbewahrt wird,
- sowohl eine retrograde (von der Buchung zum Beleg) als auch eine progressive (vom Beleg zur Buchung) Prüfung aller gebuchten Geschäftsvorfälle möglich ist und
- die Grundsätze ordnungsgemäßer Aktenführung[91] beachtet und umgesetzt werden.

Allgemein gilt hinsichtlich der Anforderungen an die Ausstattung des Prüfer-Arbeitsplatzes beim unmittelbaren Datenzugriff[92], dass

- für einen effizienten unmittelbaren Datenzugriff den beauftragten Prüfern von der geprüften Stelle eine für diesen Zweck geeignete Hard- und Softwareausstattung samt der erforderlichen Benutzerdokumentation zur Verfügung gestellt wird, die dem Stand der Technik entspricht.
- spätestens zu Beginn der Prüfung die für den Zugang zu den IT-Systemen und automatisierten Verfahren erforderlichen Benutzerkonten eingerichtet werden, die den Prüfern einen lesenden Zugriff auf alle für die Prüfung benötigten Daten ermöglichen. Werden elektronische Akten, Register oder Belegarchive geführt, gilt dies auch für den Zugriff auf die dort gespeicherten Akten, Vorgänge und Dokumente.
- eine Beschränkung des Zugriffs auf rein sachbearbeitende Funktionen, vorgefilterte Bereiche oder Kopien des Original-Datenbestandes nicht zulässig ist.
- im Rahmen der Mitwirkungspflicht die geprüfte Stelle ggf. die beauftragten Prüfer nach deren Anforderung in die Bedienung und Anwendung der zur Verfügung gestellten IT-Systeme und automatisierten Verfahren einweist und die für die Bedienung notwendigen Unterlagen überlässt.

[91] Vgl. zum Anwendungsbereich des BayDiG die Ausführungen in der LT-Drs. 18/19572 S. 38 ff.
[92] Unmittelbarer Zugriff auf automatisierte Verfahren mit nur-Lesezugriffs inkl. Nutzung der von der geprüften Stelle oder von einem beauftragten Dritten eingesetzte Hard- und Software zur Prüfung der gespeicherten Daten. Dies schließt eine Fernabfrage (z.B. Online Zugriff mit einer geeigneten Remote-Desktop- oder Remote-Access-Lösung) mit ein.

3 Elektronische Signaturen im Haushalts-, Kassen- und Rechnungswesen

Bei den bayerischen Kommunen wurden in den letzten Jahren auch im Bereich des Haushalts-, Kassen- und Rechnungswesens vermehrt papiergebundene Arbeitsprozesse durch medienbruchfreie elektronische Workflows ersetzt. Als Ersatz für die bei digitalen Feststellungsbescheinigungen, Zahlungsanordnungen, Zahlungsverkehrstransaktionen und Tagesabschlüssen/Tagesabgleichen vorgeschriebenen Unterschriften sind seit 01.01.2007 sowohl qualifizierte elektronische Signaturen (QES) als auch fortgeschrittene elektronische Signaturen (FES) zugelassen, die seit einigen Jahren bei zahlreichen Kommunen erfolgreich eingesetzt werden und medienbruchfreie digitale Prozesse ermöglichen.

Während im Zeitraum 2010 bis 2019 hierfür nahezu ausschließlich chipkartenbasierte Signaturerstellungseinheiten (Hardware-Token) zum Einsatz kamen, hat sich dies mit der vom StMI im April 2019 veröffentlichten neuen AFS-HKR grundlegend verändert.[93] Die neue AFS-HKR ermöglicht neben Hardware-Token nun auch Software-Token sowie Fernsignaturlösungen für die Erstellung von FES. Dadurch ist nicht nur eine erheblich leichtere und kostengünstigere Implementierung von Signaturlösungen möglich, sondern es werden auch die von den Verwaltungen seit 2010 eingeforderten weiteren Varianten zur Erstellung fortgeschrittener Signaturen ermöglicht, die sowohl von den Bayerischen Kommunalen Spitzenverbänden als auch vielen bayerischen Kommunen und kommunalen Softwareanbietern ausdrücklich begrüßt wurden. Nach Veröffentlichung der neuen AFS-HKR sind schnell neue Signaturanwendungslösungen entstanden, die den jeweiligen örtlichen Verhältnissen und damit auch den unterschiedlichen Anforderungen an eine rechtskonforme, aber auch zweckmäßige Gestaltung der elektronischen Verarbeitungsprozesse, z.B. eines friktionslosen Anordnungswesens in all seinen Ausprägungen, besser gerecht werden.

Gleichzeitig hat dies bei den Kommunen aber auch einige technische und organisatorische Fragen aufgeworfen, z.B. welche Signaturlösung letztendlich zum Einsatz kommen soll und welche Variante mit Blick auf die örtlichen Verhältnisse die zweckmäßigste ist.

Nachfolgend möchten wir auf einige Fragen aus der kommunalen Praxis eingehen, die in diesem Zusammenhang an uns gerichtet wurden:

3.1 Vor- und Nachteile verschiedener Signaturlösungen

Als schriftformersetzende Signaturlösungen im Haushalts-, Kassen- und Rechnungswesen sind nach den geltenden haushaltsrechtlichen Bestimmungen (§ 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik)

- qualifizierte elektronische Signaturen i.S. von Art. 3 Nr. 12 der Verordnung (EU) Nr. 910/2014 und
- fortgeschrittene Signaturen i.S. von Art. 3 Nr. 11 der Verordnung (EU) Nr. 910/2014, deren ergänzende Merkmale zuletzt mit dem o.g. IMS vom 30.04.2019, a.a.O., allgemein in der neuen AFS-HKR festgelegt worden sind,

[93] Vgl. IMS vom 30.04.2019 (Fn. 6), Anlage 1.

zugelassen.

Die mit der neuen AFS-HKR geschaffenen Erleichterungen und flexiblen Gestaltungsmöglichkeiten beim Einsatz von FES wollen wir nachfolgend kurz darstellen:

- Neben den fortgeschrittenen Zertifikaten, die vom IT-DLZ des Freistaats Bayern nach der Zertifizierungsrichtlinie der Bayern-PKI[94] ausgestellt werden, sind auch fortgeschrittene Zertifikate anderer Zertifizierungsstellen zugelassen, die einen vergleichbar sicheren Betrieb des Vertrauensdienstes gewährleisten (vgl. Nr. 4 Buchst. a i.V. mit Nr. 10 Buchst. a AFS-HKR).
- Für die Speicherung von Signaturerstellungsdaten und die Erzeugung fortgeschrittener elektronischer Signaturen dürfen neben den bereits bewährten Chipkarten (Smartcards) auch Software-Token (z.B. PKCS#12-Dateien[95]) oder auch andere Hardware-Token (z.B. Trusted Platform Module[96], USB-Token) verwendet werden (vgl. Nr. 10 Buchst. b AFS-HKR).
- Des Weiteren ist auch der Einsatz von Fernsignaturlösungen[97] möglich (vgl. Nr. 10 Buchst. d AFS-HKR), was u.a. den Einsatz von elektronischen Signaturen im Homeoffice oder bei Dienstreisen mit mobilen Endgeräten oder ggf. die Einbindung externer Stellen (Schulen, Einrichtungen, Ingenieur- oder Architekturbüros) deutlich erleichtert.
- Die Anforderungen an die Stapelsignatur von mehreren Kassenanordnungen wurde an den Stand der Technik angepasst (vgl. Begründung in den AFS-HKR, S. 11).
- Abhängig vom Anwendungsszenario sind auch Mischformen denkbar (z.B. Software-Token für Beschäftigte der Verwaltung; Fernsignatur für externe Stellen oder bei Einsatz von mobilen Endgeräten).

Eine tabellarische Übersicht der seit 30.04.2019 möglichen Lösungsvarianten zur Erzeugung fortgeschrittener Signaturen im kommunalen Haushalts-, Kassen- und Rechnungswesen finden Sie in dem vom Bayerischen Landkreistag veröffentlichten „Leitfaden zur Umsetzung der E-Rechnung bei den Landratsämtern“ a.a.O.

[94] In der AFS-HKR vom 30.04.2019 (Fn. 6) wird zwar noch die Zertifizierungsrichtlinie der Bayerischen Verwaltungs-PKI referenziert, die mit Ablauf des 10.07.2019 in die nahezu unveränderte Policy und Technik der Bayern-PKI überführt wurde (https://www.pki.bayern.de/mam/pki/vpki/policy_bayern-pki.pdf). Wegen der nur geringfügigen Unterschiede, die sich daraus für die kommunale Verwaltungspraxis ergeben, kann u.E. auf eine Anpassung der o.g. AFS-HKR verzichtet werden, zumal diese nach dem IMS vom 30.04.2019 ohnehin nur im Vorgriff auf noch zu erlassende Verwaltungsvorschriften zu KommHV-Kameralistik und KommHV-Doppik als ergänzende Merkmale gem. § 87 Nr. 12 KommHV-Kameralistik und § 98 Nr. 21 KommHV-Doppik festgelegt wurden.

[95] Vgl. Elster- oder Authega-Zertifikate, die einer sicheren Benutzerauthentifizierung dienen.

[96] Vgl. https://docs.microsoft.com/de-de/windows/security/information-protection/tpm/trusted-platform-module-top-node

[97] Fernsignaturdienste werden seit Inkrafttreten der eIDAS-VO zwischenzeitlich von mehreren Zertifizierungsstellen für die Erstellung von fortgeschrittenen und insbesondere qualifizierten Signaturen angeboten.

Vor- und Nachteile der wichtigsten Lösungsvarianten:

Sicherheitsmedium	**Vorteile**	**Nachteile**	**Vertrauens-niveau**[98]
Chip-/Smartcard	ermöglicht einen multi-funktionalen Einsatz als Signaturkarte, Dienstaus-weis, Zutritts- und Zu-gangs-Token, kann vom Signaturschlüsselinhaber leicht und sicher verwahrt werden	neben der Chipkarte wird ein Lesegerät der Klasse 3 sowie die Sig-natursoftware benötigt; höherer administrativer Aufwand	hoch
TPM-Modul	ist fest mit dem Motherboard verbunden; ermöglicht eine virtuelle Smartcard	steht nur auf entspre-chend ausgestatteten Desktop-Systemen zur Verfügung; stellt er-höhte Anforderungen an die Implementierung und Administration der Systeme	substantiell/ hoch
PKCS#12-Datei	keine Hardware; lässt sich leicht vom Signatur-schlüsselinhaber verwal-ten	muss durch zusätzliche technische und organi-satorische Maßnahmen vor unbefugten Zugrif-fen geschützt werden	substantiell[99]
OS-Zertifikatsspei-cher	keine Hardware; lässt sich leicht mittels Software-Assistent vom Signatur-schlüsselinhaber impor-tieren	muss durch zusätzliche technische und organi-satorische Maßnahmen vor unbefugten Zugrif-fen geschützt werden	substantiell
Fernsignatur	hardwareunabhängig, steht auf einer Vielzahl von Systemen zur Verfü-gung	benötigt nur eine ent-sprechende Signaturan-wendungskomponente; kein administrativer Aufwand; erfordert eine sichere Authentisierung am Fernsignaturdienst	substantiell[100]

[98] Die Einschätzung erfolgte auf Grundlage der BSI TR 03107-1 (https://www.bsi.bund.de/SharedDocs/Down-loads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf).
[99] Dies hängt von den technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz der Zertifikatsdateien vor unbefugten Zugriffen ab.
[100] Da das Vertrauensniveau bei Fernsignaturlösungen in besonderem Maße von einer sicheren Authentifizierung des Unterzeichners am Fernsignaturdienst abhängt, gehen wir bei einer reinen PIN-Lösung nur von einem substantiellen Vertrauensniveau aus.

3.1.1 Was ist beim Betrieb einer eigenen Zertifikatsinfrastruktur zu beachten?

Immer wieder stellen uns vor allem größere Kommunen die Frage, ob der Betrieb eines eigenen Signaturdienstes, z.B. in der lokalen Windows-Domäne auf Basis der Active Directory-Zertifikatsdienste, möglich ist.

➢ Antwort:

Der Betrieb einer eigenen Zertifizierungsstelle ist zwar nach der seit 30.04.2019 geltenden AFS-HKR (vgl. Fn. 6) unter den dort genannten technischen und organisatorischen Rahmenbedingungen grundsätzlich möglich, dürfte aber wegen der dafür notwendigen Investitions- und Betriebskosten in eine vertrauenswürdige, sichere und hoch verfügbare PKI-Infrastruktur[101] nur dann zweckmäßig und wirtschaftlich sein, wenn eine große Zahl von Teilnehmern diesen Vertrauensdienst nutzen. Daher steht dem Aufbau einer solchen PKI-Infrastruktur in aller Regel das kommunalrechtliche Gebot der Sparsamkeit und Wirtschaftlichkeit entgegen, da einerseits die vom Freistaat Bayern betriebene Bayern-PKI den Beschäftigten der öffentlichen Verwaltung kostenfrei zur Verfügung steht und andererseits bereits Alternativangebote am Markt verfügbar sind, die neue technische Implementierungsmöglichkeiten bieten (Fernsignaturen) und sowohl die Verwaltung als auch die Nutzung der digitalen Identitäten nochmals erleichtern.

➢ Im Detail:

In Nr. 4 Buchst. a zweiter Spiegelstrich AFS-HKR sind neben Zertifizierungsstellen der deutschen Verwaltungs-PKI auch andere Zertifizierungsstellen zugelassen, die

- einen vergleichbar sicheren Betrieb des Vertrauensdienstes gewährleisten,
- dies mit einer Zertifizierungsrichtlinie nach der RFC 3647 dokumentieren und
- in einer entsprechenden Selbsterklärung bestätigen.

Des Weiteren führt die Begründung zu den AFS-HKR dazu aus, dass eine Zertifizierung durch die Wurzelzertifizierungsinstanz der deutschen Verwaltungs-PKI oder die Mitgliedschaft in der EBCA[102] nicht zwingend erforderlich ist. Für den internen Anwendungsbereich der fortgeschrittenen Zertifikate werden weitergehende Anforderungen, wie sie in der eIDAS-VO[103] für die Zertifizierungsdienstanbieter gesetzlich geregelt sind, ebenfalls nicht für erforderlich gehalten.

Aber wie so oft, steckt auch hier der Teufel im Detail. Mit einem Blick auf die „Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung für die X.509-Zertifizierungshierarchie Bayern PKI" (kurz: Zertifizierungsrichtlinie Bayern-PKI)[104] und die in Nr. 10 Buchst. a, b, d, e AFS-HKR genannten Anforderungen wird schnell deutlich, dass ein vergleichbar vertrauenswürdiger Dienst ohne einen großen Aufwand weder umsetzbar ist noch zuverlässig für die

[101] Public Key Infrastruktur (PKI, Infrastruktur für öffentliche Schlüssel)
[102] TeleTrustT European Bridge CA, vgl. www.ebca.de
[103] 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 - Elektronische-Transaktionen-VO
[104] Mit Ablauf des 10.07.2019 wurde die Bayerische Verwaltungs-PKI in die Bayern-PKI überführt. Da deren Zertifikate teilweise Gültigkeiten über diesen Zeitpunkt hinaus haben, stellt die Bayern-PKI die hier zugrundeliegende Zertifizierungsrichtlinie weiterhin zur Verfügung (vgl. https://www.pki.bayern.de/vpki/allg/policy/index.html).

Dauer der gesetzlichen Aufbewahrungsfristen von Belegen[105] betrieben werden kann. Aufgrund der in Nr. 10 Buchst. a, b, d und e AFS-HKR genannten Anforderungen wären für die Schlüsselerzeugung, Installation, Aufbewahrung und das Management des Schlüsselmaterials durch die Zertifizierungsstelle umfangreiche technische und organisatorische Maßnahmen sowie erhebliche Investitionen in vertrauenswürdige (zertifizierte) und ausfallsichere (redundante) Hardware-Komponenten (z.B. Hardware-Sicherheits-Module)[106] erforderlich, die nicht unerhebliche Investitions- und Betriebskosten verursachen. Hinzu kommt, dass der ordnungsgemäße Betrieb einer solchen Zertifizierungsstelle auch entsprechend qualifiziertes und spezialisiertes Personal erfordert, das sich nach unseren Erfahrungen derzeit und wohl auch in absehbarer Zukunft nicht so einfach gewinnen lässt.

Angesichts dieser Rahmenbedingungen und insbesondere der Tatsache, dass aufgrund des bestehenden E-Government-Pakts des Freistaats mit den Bayerischen Kommunalen Spitzenverbänden[107] die vom IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) erstellten fortgeschrittenen Zertifikate samt Signaturschlüssel kostenfrei genutzt werden können, erscheint der Betrieb einer eigenen Zertifizierungsstelle, auch bei größeren Städten, aus unserer Sicht weder zweckmäßig noch wirtschaftlich. Zumindest ist uns bislang noch keine belastbare Wirtschaftlichkeitsbetrachtung[108] bekannt, die Gegenteiliges belegen würde.

3.1.2 Unter welchen Voraussetzungen kann ich die Signatur-Zertifikate der Bayern-PKI nutzen?

➢ Antwort:

Der vom IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) betriebene Dienst Bayern-PKI[109] steht in Form des Zertifikatsverwaltungssystems PRIME grundsätzlich allen Beschäftigten der öffentlichen Verwaltung Bayerns zur Verfügung. Da der Dienst aber nur über das Bayerische Behördennetz (BYBN) erreichbar ist, setzt dies grundsätzlich einen Anschluss der Behörde oder des Teilnehmers an das BYBN voraus, wenn die Behörde und der Teilnehmer das Zertifikatsverwaltungssystem PRIME (Java-Anwendung) für die Beantragung und Verwaltung von Zertifikaten nutzen möchten.

Die von der Bayern-PKI ausgestellten Zertifikate können aber auch von Kommunen und deren Einrichtungen genutzt werden, die über keinen Anschluss an das BYBN verfügen, wenn ein vertrauenswürdiger Dritter (z.B. Landkreis, vom IT-DLZ zugelassene IT-Dienstleister) die Aufgaben der Registrierungsstelle übernimmt (z.B. Identifikation der Teilnehmer, Antragstellung beim IT-DLZ, Sperrung von korrumpierten Zertifikaten).

---

[105] Diese gilt gem. § 37 Abs. 1 Nr. 9 KommHV-Kameralistik und § 33 Abs. 1 Nr. 9 KommHV-Doppik auch für elektronische Signaturen, da diese während der Dauer der Aufbewahrungsfristen (i. d. Regel 10 Jahre) nachprüfbar sein müssen.
[106] Hardware-Sicherheitsmodul oder englisch Hardware Security Module *(sog.* HSM*)*
[107] Vgl. https://www.stmd.bayern.de/themen/digitale-verwaltung/digitale-verwaltung-in-bayern-rahmenbedingungen/
[108] Vgl. BKPV-Geschäftsbericht 2008, S. 65 ff.
[109] Das IT-Dienstleistungszentrum (IT-DLZ) betreibt mit der Bayern-PKI eine Infrastruktur, welche für alle Behörden in Bayern eine gemeinsame Wurzel-CA und damit eine übergreifende Vertrauensstruktur zur Verfügung stellt.

➢ Im Detail:

Die Bayern-PKI stellt elektronische Zertifikate für natürliche Personen, juristische Personen, Personengruppen und Funktionen aus. Den Teilnehmern wird die Bayern-PKI angeboten, um die Vertraulichkeit, Integrität und Verbindlichkeit von Daten oder Nachrichten zu gewährleisten. Teilnehmer sind dabei Beschäftigte der staatlichen und kommunalen Verwaltungen in Bayern sowie in Ausnahmefällen vertrauenswürdige Dritte. Die Zertifikate, die im Rahmen der Bayern-PKI ausgestellt werden, sind kostenlos.

Die von der Bayern-PKI ausgegebenen Signatur-Zertifikate können bei einer sicheren Aufbewahrung und ordnungsgemäßen Verwendung der persönlichen Signaturerstellungsdaten[110] für die Erstellung von fortgeschrittenen Signaturen[111] im Haushalts-, Kassen- und Rechnungswesen (HKR) oder in anderen Bereichen[112] genutzt werden. Maßgebend für die schriftformersetzende Verwendung der fortgeschrittenen Signaturen im Bereich HKR ist, dass die in den AFS-HKR vom 30.04.2019 vorgegebenen technischen und organisatorischen Rahmenbedingungen eingehalten werden.

Dadurch soll sichergestellt werden, dass die mit dem persönlichen Signaturschlüssel und Zertifikat erstellte fortgeschrittene elektronische Signatur

- eindeutig dem Unterzeichner (Teilnehmer) zugeordnet werden kann,
- die Identifizierung des Unterzeichners ermöglicht,
- unter Verwendung elektronischer Signaturerstellungsdaten erstellt wird, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann und
- so mit den auf diese Weise unterzeichneten Daten verbunden ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Um beim Erstellungsprozess und der nachfolgenden Prüfung von fortgeschrittenen Signaturen zu gewährleisten, dass

- zum Zeitpunkt der Erstellung nur gültige und nicht gesperrte Zertifikate verwendet (Autorisierungs- und Sperrlistenprüfung),
- die mathematische Gültigkeit der Signaturen ermittelt (Hashwertvergleich),
- die Integrität und Gültigkeit der Zertifikate gemäß dem Gültigkeitsmodell nachvollzogen (Prüfung der Zertifikatskette),
- der korrekte Verwendungszweck überprüft (Signaturzertifikat und Nicht-Abstreitbarkeit) und
- der Zeitpunkt der Signatur festgestellt (Zeitstempel oder zumindest Synchronisation mit einem Zeitserver)

werden können, sind die folgenden Zugangsvoraussetzungen und Rahmenbedingungen zu gewährleisten:

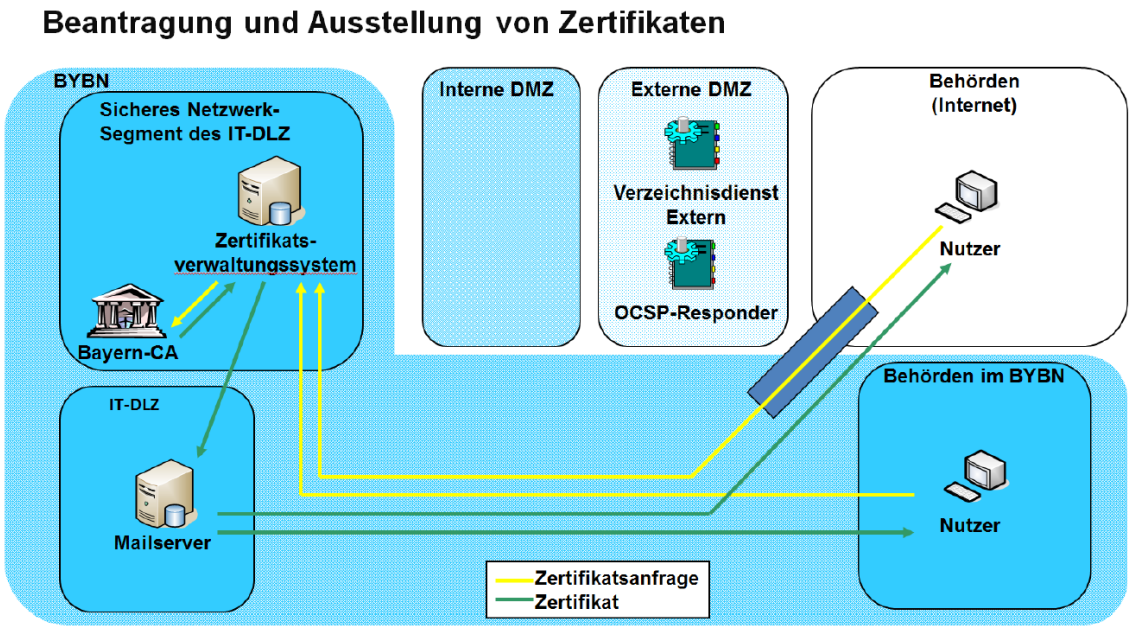
---

[110] Vgl. Art. 3 Nr. 13 eIDAS-VO, insb. der persönliche Signaturschlüssel und das persönliche Signatur-Zertifikat sowie die o.g. AFS-HKR (Fn. 6) und die Zertifizierungsrichtlinie der Bayern-PKI (Fn. 105); dazu ergänzend https://www.itwissen.info/Persoenliche-Sicherheitsumgebung-personal-security-environment-PSE.html.
[111] Vgl. zum Begriff und zu den Anforderungen § 87 Nr. 12 KommHV-Kameralistik/§ 98 Nr. 21 KommHV-Doppik i.V. mit Art. 3 Nr. 11 und Art. 26 eIDAS-VO.
[112] Z.B. fortgeschrittene Dokumentensignatur, Transfervermerke beim ersetzenden Scannen, sichere E-Mail.

a) Erreichbarkeit der Registrierungsstellen, des Zertifikatsverwaltungssystems und insbesondere des OSCP Responders

Damit die zugelassenen Registrierungsstellen und das Zertifikatsverwaltungssystem der Bayern-PKI erreichbar sind und der Status des verwendeten X.509-Zertifikats beim Validierungsdienst online abgefragt werden kann (sog. OCSP Responder)[113], muss die Signaturanwendungskomponente ordnungsgemäß konfiguriert und die dafür benötigten Ports auch an der Firewall freigeschaltet werden.[114] Da der OCSP Responder der Bayern-PKI über das Internet erreicht werden kann, kann die Autorisierungs- und Sperrlistenprüfung auch von Teilnehmern genutzt werden, die ein gültiges Signaturzertifikat, aber keinen Anschluss an das BYBN besitzen. In diesen Fällen muss allerdings eine andere Registrierungsstelle mit Zugang zum BYBN (z.B. eine Kommune) oder ein beauftragter Dritter (z.B. zugelassener IT-Dienstleister) die Beantragung und Verwaltung der Zertifikate übernehmen.

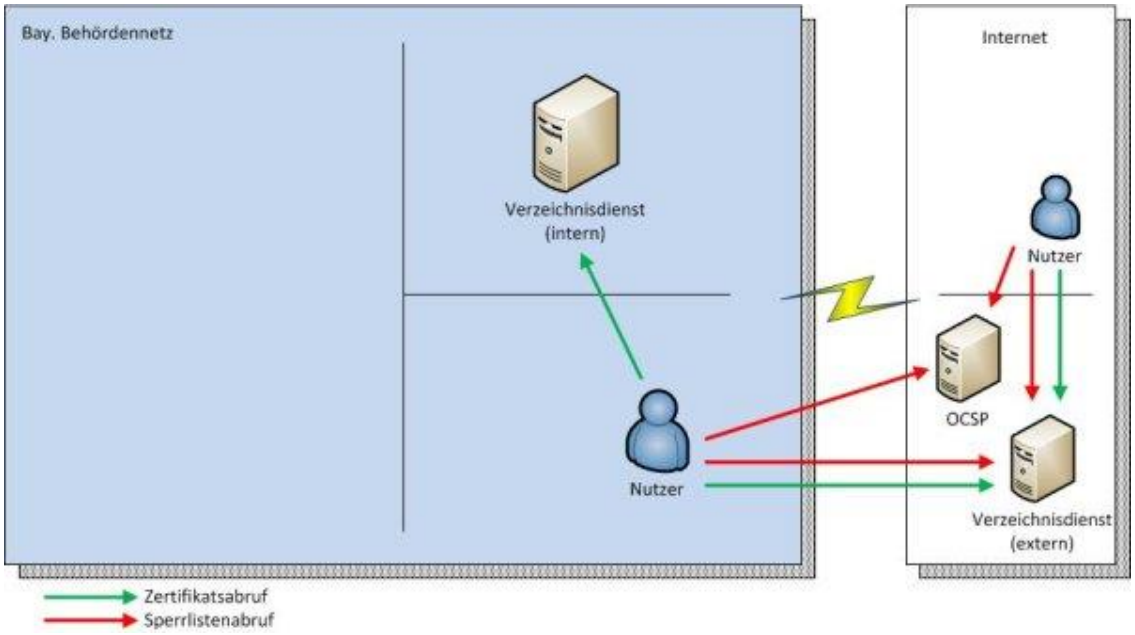
Die Möglichkeiten zur Beantragung und Ausstellung von Zertifikaten durch die vom IT-DLZ zugelassenen Registrierungsstellen soll folgende Graphik verdeutlichen:



Quelle: IT-DLZ/PKI-Bayern, www.pki.bayern.de

[113] Vgl. https://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol.
[114] Vgl. Nr. 4.9.10 „Anforderungen, um OCSP zu nutzen" der Zertifizierungsrichtlinie Bayern-PKI (Fn. 105).

Die Möglichkeiten zum Zertifikats- und Sperrlistenabruf durch Teilnehmer der Bayern-PKI, die sich innerhalb oder außerhalb des Bayerischen Behördennetzes befinden können, soll folgende Graphik veranschaulichen:



Quelle: IT-DLZ/PKI-Bayern, www.pki.bayern.de

Der Sperrlistenabruf in Windows-Systemen erfolgt automatisch, da die benötigte Information aus dem Zertifikat ausgelesen wird. Das genaue Verfahren muss der Dokumentation der jeweiligen Signaturanwendungskomponente entnommen werden. Die hierfür benötigten technischen Informationen können bei Zertifikaten der Bayern-PKI den vom IT-DLZ veröffentlichten Informationen entnommen werden.[115]

b) Verteilung von Stamm-Zertifikaten der CA (Wurzel-Zertifizierungsstelle) für die Offline-Prüfung von fortgeschrittenen elektronischen Signaturen (Prüfung gegen Wurzelzertifikat der CA und deren Vertrauensstellung)

Für die Prüfung der Gültigkeit von fortgeschrittenen Signaturen, die mit Zertifikaten der Bayern-PKI erstellt wurden, empfehlen wir, die Wurzelzertifikate der Zertifizierungsstelle herunterzuladen und auf den Desktop-PC zu verteilen. Wird einer Zertifizierungsstelle vertraut, wird damit allen von ihr signierten Zertifikaten ebenfalls vertraut.[116] Wenn die CA-Zertifikate der Bayern-PKI oder Verwaltungs-PKI ordnungsgemäß in den lokalen Zertifikatsspeicher des Desktop-PC unter den vertrauenswürdigen Stammzertifizierungsstellen importiert bzw. gespeichert werden, ist sichergestellt, dass beim Lesen von signierten Dokumenten oder Offline-Signaturprüfungen keine Fehlermeldungen angezeigt werden. Allerdings setzt dies voraus, dass kein Sperrlisteneintrag vorliegt, der mit einer Statusabfrage über den OCSP-Responder der Zertifizierungsstelle abgefragt werden kann (sog. Online-Signaturprüfung)[117]. Das IT-DLZ bietet auch für kommunale Behörden, die nicht dem Active Directory Bündnisforest des Freistaats Bayern angehören, eine Anleitung zum Erstellen einer entsprechenden Gruppenrichtlinie an, die eine Verteilung der Wurzelzertifikate ermöglicht (vgl. https://www.pki.bayern.de/vpki/allg/cazert/index.html).

[115] Vgl. https://www.pki.bayern.de/vpki/allg/index.html und https://www.pki.bayern.de/vpki/allg/zertabruf/index.html.
[116] Vgl. https://www.pki.bayern.de/vpki/allg/pki/index.html.
[117] Vgl. Nr. 4.10 „Dienst zur Statusabfrage von Zertifikaten (OCSP)“ der Zertifizierungsrichtlinie Bayern-PKI.

c) Synchronisation der Systemzeit des für die Signatur verwendeten Endgeräts mit einem Zeitserver

Nachdem derzeit im Rahmen der Bayern-PKI kein Zeitstempeldienst angeboten wird[118], empfehlen wir, die Systemzeit der für elektronischen Signaturen verwendeten Endgeräte mit einem über das Intranet oder Internet erreichbaren Zeitserver zu synchronisieren.

Zu den Buchstaben a) bis c):

Da die Implementierung und Konfiguration der Signaturanwendungslösungen entsprechende technische Fachkenntnisse erfordert, empfehlen wir, jene grundsätzlich in Abstimmung mit den jeweiligen Verfahrensanbietern oder kommunalen IT-Dienstleistern vorzunehmen.

3.1.3 Können Fernsignaturdienste verwendet werden?

➢ Antwort:

Wie bereits in den Abschn. 3. 3.1 und 3.1.1 kurz erwähnt, können seit Veröffentlichung der neuen AFS-HKR mit IMS vom 30.04.2019 (siehe Fn. 6) auch Fernsignaturdienste für die Erstellung fortgeschrittener Signaturen genutzt werden, wenn diese die in den AFS-HKR genannten technischen und organisatorischen Anforderungen erfüllen. Dies eröffnet neue Möglichkeiten sowohl bei vor Ort betriebenen (on premise) als auch im Rechenzentrum gehosteten (z.B. via Terminal-Server oder Private Cloud) Finanzverfahren oder Workflow-Systemen und bietet darüber hinaus den Vorteil, dass unterschiedliche Endgeräte (Desktop, Tablet, Smartphone, Browser) für die Erstellung von elektronischen Signaturen eingesetzt werden können.

➢ Im Detail:

In Anlehnung an die gesetzlichen Regelungen für die qualifizierte elektronische Signatur (QES)[119] lässt die seit 30.04.2019 geltende AFS-HKR ebenfalls Fernsignaturlösungen für fortgeschrittene Signaturen zu, die nicht mehr lokal am PC-Arbeitsplatz des Teilnehmers, sondern auf einem zentralen Serversystem mit HSM-Modul erstellt werden (vgl. Nr. 10 Buchst. d AFS-HKR und Nr. 1.2 der Begründung zur AFS-HKR). Dies eröffnet die Möglichkeit, dass die im Haushalts-, Kassen- und Rechnungswesen zugelassenen fortgeschrittenen Signaturen auf verschiedenen Endgeräten (z.B. Desktop, Smartphones, Tablets) erstellt werden können, unabhängig davon, ob das Finanzverfahren oder das Workflow-System vor Ort oder im externen Rechenzentrum betrieben wird.[120] Zudem entfallen damit die bei „on premise" eingesetzten Signaturanwendungen notwendigen Hard- oder Software-Token und deren Schutz vor unbefugten Zugriffen.

Aus unserer Sicht bietet diese moderne Signaturvariante eine erhebliche Erleichterung für den jeweiligen PKI-Teilnehmer (Signaturschlüsselinhaber) und die einsetzende Stelle (Registrierungsstelle, IT-Service), da

[118] Vgl. Nr. 6.8 der Zertifizierungsrichtlinie Bayern-PKI (Fn. 105).
[119] Vgl. Erwägungsgrund Nr. 52 eIDAS-VO vom 23.07.2014 a.a.O. und Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten in Anhang II eIDAS-VO.
[120] Ein erheblicher Vorteil, der nicht nur das Ausrollen und die sichere Aufbewahrung der Signaturzertifikate und die Administration der Signaturanwendungen erleichtert, sondern gerade die durch die Covid-19-Pandemie zunehmende Anzahl von mobilen oder dislozierten Arbeitsplätzen leichter mit Signaturlösungen unterstützen lässt.

- die Zertifizierungsstelle sich um die Erstellung und Erneuerung der Signaturzertifikate kümmert,
- der Teilnehmer oder die einsetzende Stelle sich nicht mehr um die sichere Aufbewahrung der Signaturzertifikate kümmern muss,
- keine zusätzliche Hard- und Software benötigt wird und
- insbesondere bei größeren Dokumenten der Signaturvorgang wesentlich beschleunigt wird.

Ein solcher Fernsignaturdienst wird zwischenzeitlich von der AKDB den Nutzern der Finanzsoftware OK.FIS angeboten (sog. Signaturservice, der in unterschiedlichen Ausprägungen verfügbar ist). Dies ist auch unabhängig davon, ob das Finanzverfahren OK.FIS „on premise" oder im AKDB-Rechenzentrum betrieben wird. Die AKDB hat bereits angekündigt, diesen Signaturdienst künftig auch anderen Kommunen oder kommunalen Einrichtungen anzubieten, die Finanzverfahren anderer Hersteller einsetzen. Die hierzu notwendige generische Schnittstelle (Rest-API) soll nach den erhaltenen Auskünften bereits auch für eine Implementierung in Fremdlösungen zur Verfügung stehen.[121]

Natürlich muss beim Einsatz einer Fernsignaturlösung sichergestellt sein, dass der Signaturschlüsselinhaber stets die Verfügungsgewalt über sein Schlüsselmaterial behält und die verfahrensinterne Kommunikation der Signaturanwendungskomponente mit dem zertifizierten kryptographischen Modul sicher und vertrauenswürdig gestaltet ist (vgl. § 87 Nr. 12 KommHV-Kameralistik/§ 98 Nr. 21 KommHV-Doppik i.V. mit Art. 3 Nr. 11 und Art. 26 Buchst. c eIDAS-VO und Nr. 10 Buchst. c und e AFS-HKR). Bei einem Fernsignaturverfahren werden daher etwas andere Sicherheitsanforderungen an das Anwendungsverfahren gestellt. Insbesondere muss der Vertrauensdiensteanbieter verlässlich und vertraulich mit dem Unterzeichner bzw. mit der Signatur-Anwendungskomponente kommunizieren können, damit der Unterzeichner vor Signaturfälschungen geschützt ist und die Verwendung seines Signaturschlüssels durch Dritte verhindert werden kann. Hierbei ist insbesondere auf eine sichere Authentifizierung des Unterzeichners am Fernsignaturdienst zu achten. Außerdem muss das Anwendungsverfahren sicherstellen, dass beim Signaturprozess weder die zu signierenden Daten noch der übertragene Hashwert und die zurückübertragene Signatur unbemerkt verändert werden können.

Bei Fernsignaturen ist – wie bei Signaturen mit Zertifikaten der Bayern-PKI – ebenfalls sicherzustellen, dass

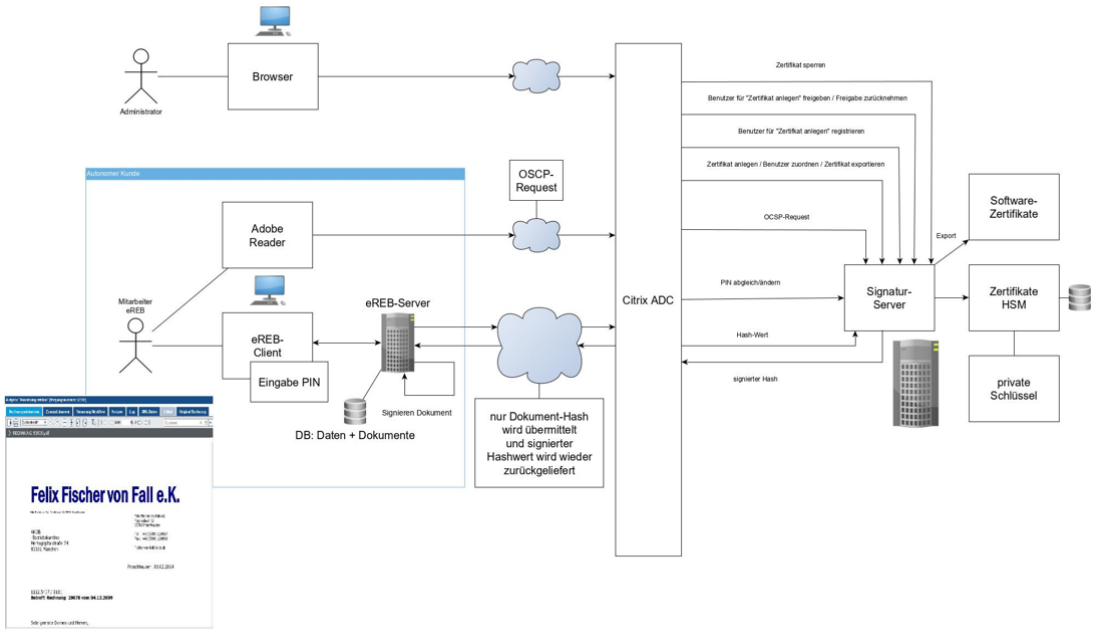
- die Gültigkeit der Signaturen von nachgelagerten Kontrollinstanzen (Feststellungsbefugter, Anordnungsbefugter, Kasse, Rechnungsprüfung) geprüft werden kann (z.B. gängige PDF-Viewer, Governikus),
- die Anforderungen des Art. 3 Nr. 11 i.V. mit Art. 26 eIDAS-VO eingehalten werden,
- die Verkehrsfähigkeit nicht eingeschränkt wird und

[121] Inwieweit diese Möglichkeit in vergleichbarer Weise und Qualität auch von anderen kommerziellen Anbietern von Fernsignaturdiensten (vgl. https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/DE) angeboten wird, können wir nicht beurteilen, da wir nur einen Überblick über diejenigen Zertifizierungsdiensteanbieter haben, die fortgeschrittene Signaturzertifikate für Beschäftigte der bayerischen Kommunen ausstellen; die am Markt verfügbaren Lösungen müsste daher die jeweilige Kommune/Einrichtung im Rahmen der Markterkundung vor einer Auftragsvergabe selbst ermitteln.

– eine Sperrlistenprüfung möglich ist.

Dies setzt, wie in Nr. 4 Buchst. a zweiter Spiegelstrich AFS-HKR betont, einen Vertrauensdiensteanbieter voraus, der einen mit der Bayern-PKI vergleichbar sicheren Betrieb des Vertrauensdienstes gewährleistet, dies mit einer Zertifizierungsrichtlinie nach der RFC 3647[122] dokumentiert und in einer entsprechenden Selbsterklärung bestätigt. Die einsetzende Stelle sollte diese Selbsterklärung mit zum Gegenstand der Freigabeerklärung nach Nr. 10 g AFS-HKR machen.

Nachfolgende Graphik soll die Funktionsweise des Fernsignaturdienstes veranschaulichen:



Quelle: AKDB (www.akdb.de)

3.2 Ordnungsgemäßer Einsatz elektronischer Signaturen und deren Nachprüfbarkeit

Wie bereits in der Einleitung zu Abschn. 3 dargestellt, hat der Einsatz von elektronischen Signaturen im kommunalen Haushalts-, Kassen- und Rechnungswesen stark zugenommen. Der bislang im privaten Bereich nicht so weit verbreitete Vertrauensdienst wirft bei den Anwendern in den Verwaltungen naturgemäß auch einige praktische Anwendungsfragen auf, die wir nachfolgend aufgreifen und beantworten möchten.

[122] https://datatracker.ietf.org/doc/html/rfc3647

3.2.1 Wie kontrolliere ich, ob die elektronischen Signaturen von Kassenanordnungen gültig sind?

Beim Einsatz von elektronischen Signaturen im Haushalts-, Kassen- und Rechnungswesen stellt sich den nachfolgenden Kontroll- und Prüfinstanzen (z.B. Anordnungsberechtigter, Kasse, Rechnungsprüfungsorgane) häufig die Frage, wie die Gültigkeit der fortgeschrittenen oder qualifizierten elektronischen Signaturen und die Integrität des Dokumenteninhalts geprüft werden können.

➢ Antwort:

Eine Kontrolle der Gültigkeit von fortgeschrittenen oder qualifizierten elektronischen Signaturen ist bei einer benutzerfreundlichen Implementierung und korrekten Konfiguration der Signaturanwendungslösung automatisiert möglich, erfordert also in der Regel keine Interaktion des Benutzers.[123] Ohne näher auf die technischen Details einzugehen, ist hier im Vergleich zum manuellen Abgleich anhand der Unterschriftsproben auf den haushaltsrechtlich vorgeschriebenen „Unterschriftslisten"[124] eine echte Erleichterung für die betroffenen Nutzer möglich, da fortgeschrittene oder qualifizierte elektronische Signaturen eine Identifizierung des Unterzeichners ermöglichen und zudem erkennen lassen, ob die signierten Daten nachträglich verändert wurden. Es bedarf daher in der Regel nur einer kurzen Einweisung, wie die im Fachverfahren, Workflow-System oder PDF-Viewer (Signaturkachel/Signaturstempel oder in Signaturfenstern) angezeigten Prüfergebnisse zu interpretieren sind und wie ggf. einzelne Prüfschritte oder ggf. ein neues Prüfprotokoll interaktiv erzeugt und visualisiert werden können.[125]

Da die Form und (Mindest-)Inhalte der Feststellungsbescheinigung und Zahlungsanordnungen haushaltsrechtlich vorgegeben sind und der Umfang der Feststellungs-/Anordnungsbefugnisse nicht nur in der Dienstanweisung geregelt werden muss, sondern diese persönlichen Zugriffsrechte auch in vielen Finanzverfahren hinterlegt und damit automatisch geprüft werden können, lassen sich neben der Gültigkeit der elektronischen Signatur auch diese Befugnisse automatisiert prüfen (z.B. mit entsprechenden Zugriffs- und Plausibilitätsprüfungen oder Wertgrenzen).

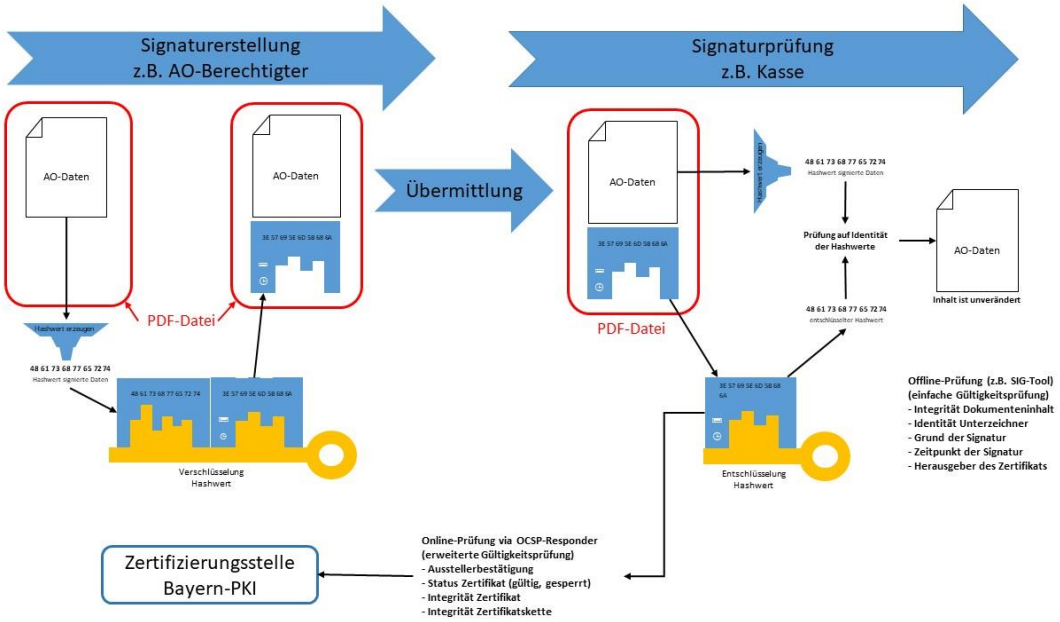
➢ Im Detail:

Aufgrund der unterschiedlichen Signaturlösungen, die wir bislang bei den von uns geprüften Finanzverfahren oder Workflow-Systemen vorgefunden haben, lässt sich diese Frage – mit Ausnahme der in PDF-Dokumente eingebetteten fortgeschrittenen oder qualifizierten elektronischen Signaturen – nicht allgemeingültig beantworten. Zudem lässt die technikneutrale Regelung in § 3 Nr. 10 eIDAS-VO durchaus mehrere Lösungsvarianten zu, da elektronische Signaturen entweder den signierten Daten beigefügt (z.B. eingebettet in XML-Daten oder PDF- Dokumente) oder logisch mit ihnen verbunden werden können (z.B. separate Signaturdatei).[126] Nach unseren

[123] Bei elektronischen Signaturen, die in PDF-Dokumente eingebettet sind, wird die Signaturprüfung bei vielen PDF-Viewern automatisch beim Öffnen des signierten PDF-Dokuments durchgeführt und das Ergebnis in der Signaturkachel oder im Signaturfenster angezeigt; es bedarf in diesen Fällen nicht einmal einer speziellen Signaturprüfsoftware, die z.B. vom IT-DLZ auf Basis von Governikus angeboten wird.
[124] Vgl. für Anordnungsberechtigte § 38 Abs. 2 Satz 2 KommHV-Kameralistik/§ 34 Abs. 2 Satz 2 KommHV-Doppik und für Feststellungsbefugte § 41 Abs. 3 Sätze 1 und 2 KommHV-Kameralistik/§ 37 Abs. 3 Sätze 1 und 2 KommHV-Doppik.
[125] Im Bedarfsfall oder bei Zweifeln kann in Bayern eine erweitere Signaturprüfung mit der vom IT-DLZ/Bayern-PKI zur Verfügung gestellten Anwendung Governikus vorgenommen und ein ausführliches Prüfprotokoll erstellt werden, vgl. https://www.pki.bayern.de/sigp/index.html, diese Seite ist aber nur innerhalb des BYBN erreichbar.
[126] Vgl. dazu ausführlich das BSI-Dokument „Grundlagen der elektronischen Signatur", welches derzeit vom BSI aktualisiert und an das aktuell geltende europäische Recht (eIDAS-VO) und nationale Recht (Vertrauensdienstegesetz und -

bisherigen Erfahrungen werden aber in der Regel bei den in bayerischen Kommunen eingesetzten Finanzverfahren oder Workflowsystemen die qualifizierten oder fortgeschrittenen Signaturen auf Grundlage des PAdES-Standards[127] in die PDF-Dokumente eingebettet. Eine Lösung, die wir ebenfalls favorisieren, zumal damit einerseits eine uneingeschränkte Verkehrsfähigkeit und Prüfung der PDF-Dokumente mit Standard PDF-Viewern und andererseits eine einfachere Aufbewahrung der signierten Belege für die Dauer der gesetzlichen Aufbewahrungsfristen sichergestellt ist.

Da die Signaturerstellungs- und Prüfprozesse i.d.R. im Hintergrund automatisiert ablaufen, möchten wir zum besseren Verständnis anhand der nachfolgenden Graphik kurz darstellen, was dabei im Wesentlichen passiert:



Dazu kurz eine Erläuterung der einzelnen Schritte:

a) Der Unterzeichner (z.B. Anordnungsberechtigter) erzeugt zunächst eine einmalige und eindeutige Prüfsumme der zu signierenden Daten (Hashwert), die er dann mit seinem persönlichen Signaturschlüssel verschlüsselt.[128]

b) In das PDF-Dokument mit den Daten der Kassenanordnung wird die soeben erstellte elektronische Signatur (enthält den verschlüsselten Hashwert der signierten Daten, das Datum der Signatur und das vom Unterzeichner verwendete Zertifikat samt dessen öffentlichem Schlüssel) eingebettet.[129]

verordnung) angepasst wird; die Neu-Veröffentlichung des Dokuments ist lt. BSI-Vermerk voraussichtlich Mitte 2022 geplant, siehe: www.bsi.bund.de.

[127] Vgl. ETSI EN 319142 (abrufbar unter https://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf).

[128] Die hierbei verwendeten Algorithmen sind im Signaturzertifikat des Signierenden hinterlegt.

[129] Der persönliche Signaturschlüssel des Signierenden muss hierbei natürlich geheim bleiben und darf die vom Signaturschlüsselinhaber verwendete PSE nicht verlassen.

c) Beim Öffnen des PDF-Dokuments durch den Empfänger (z.B. Kasse) wird zunächst ebenfalls eine einmalige und eindeutige Prüfsumme der signierten Daten erzeugt und diese anschließend mit dem entschlüsselten Hashwert des Unterzeichners verglichen.[130] Stimmen beide Prüfsummen überein, sind die signierten Daten integer, d.h. unversehrt.
d) Anhand des in die elektronische Signatur eingebetteten Zertifikats können u.a. die Identität des Unterzeichners, die zertifikatsausstellende Stelle und die für die Bildung, Ver- und Entschlüsselung des Hashwerts verwendeten Algorithmen entnommen werden.
e) Für die erweiterte Prüfung der Gültigkeit der Signatur können auch noch online der Status des verwendeten Signatur-Zertifikats, dessen Integrität und der Aussteller des Zertifikats verifiziert werden (sog. Online-Prüfung).[131] Die hierfür notwendigen Informationen (z.B. Prüfpfade und Name des OCSP-Responders) sind ebenfalls im Zertifikat des Unterzeichners gespeichert.

3.2.2 Welche Anforderungen gelten beim Einsatz von Software-Token?

➢ Antwort:

Werden für die fortgeschrittene elektronische Signatur von Wissens- und Willenserklärungen im Haushalts-, Kassen- und Rechnungswesen (z.B. Feststellungsbescheinigungen, Kassenanordnungen, Tagesabschlüsse/Tagesabgleiche) Software-Token (z.B. PKCS#12-Dateien) verwendet, muss insbesondere sichergestellt sein, dass diese

- vom Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwendet werden können (Verfügungsgewalt),
- auf einem Speichermedium/Speicherbereich abgelegt werden, auf das/den nur der Zertifikatsnehmer/Signaturschlüsselinhaber einen Zugriff hat (Besitz),
- mit einem starken und geheimen Passwort vor unbefugter Verwendung geschützt sind (Wissen) und
- Unbefugten weder zugänglich sind noch von diesen kopiert werden können (Zugangs- und Manipulationsschutz).

➢ Im Detail:

Wie bereits in Abschn. 3.1 dargestellt, hängen das Sicherheitsniveau und die Nicht-Abstreitbarkeit von elektronischen Signaturen im Haushalts-, Kassen- und Rechnungswesen (z.B. Feststellungsbescheinigungen, Kassenanordnungen, Tagesabschlüsse/Tagesabgleiche) vor allem davon ab, dass der Signierende die elektronischen Signaturerstellungsdaten mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Um eine vertrauenswürdige Verwendung des Signaturzertifikats samt zugehöriger Schlüssel zu gewährleisten, muss der Zertifikatsnehmer/Signaturschlüsselinhaber einige Sorgfaltspflichten beachten, die in Nr. 4.5.1 der Zertifizierungsrichtlinie der Bayern-PKI (siehe Fn. 105) näher beschrieben sind.

[130] Hierbei werden ebenfalls die im Zertifikat des Unterzeichners hinterlegten Algorithmen verwendet.
[131] Da die Signaturanwendung innerhalb einer freigegebenen Anwendung, also einer geschlossenen, vertrauenswürdigen und sicheren Systemumgebung erfolgt (vgl. Begründung AFS-HKR, Anlage 5 zum IMS vom 30.04.2019, Az. B4-1512-4-17; siehe Fn. 6), ist dies i.d.R. nur stichprobenweise notwendig, insbesondere dann, wenn Zweifel an der Informationssicherheit des örtlichen Betriebs bestehen. Zudem ist bei der Prüfung der Signaturzertifikate zu berücksichtigen, ob diese, abhängig vom verwendeten Algorithmus oder Tool, nach dem Schalen- oder Kettenmodell erfolgt, da beide Verfahren unter Umständen zu unterschiedlichen Ergebnissen führen können. Wir präferieren bei der erweiterten Zertifikatsprüfung das sog. Kettenmodell.

Die AFS-HKR (siehe Fn. 6) ergänzt oder konkretisiert diese in Nr. 6 i.V. mit Nr. 10 Buchst. c AFS-HKR und Anlage 3 AFS-HKR mit den folgenden Anforderungen:

- Beim Einsatz von Software-Token (z.B. PKCS#12-Dateien) ist durch angemessene technische und organisatorische Maßnahmen sicherzustellen, dass die Signaturerstellungsdaten weder exportiert noch unbefugt verwendet und vom rechtmäßigen Unterzeichner verlässlich geschützt werden können.
- Die Signaturerstellungsdaten müssen darüber hinaus vertraulich sein, dürfen nur einmal vorkommen, nicht abgeleitet werden können und verlässlich gegen Fälschung geschützt sein.
- Der Unterzeichner muss von der Registrierungsstelle über den sorgfältigen und sicheren Umgang mit den Signaturerstellungsdaten unterrichtet und entsprechend sensibilisiert werden.

Dies erfordert einerseits geeignete technische und organisatorische Maßnahmen und andererseits einen sorgfältigen und gewissenhaften Umgang des Unterzeichners mit seinem Software-Token und dem Passwort (PIN) für den persönlichen Signaturschlüssel.

Das Nähere über den Einsatz der Software-Token und deren Sicherung[132] ist gem. § 37 Abs. 1 Nr. 9 und Abs. 2 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 9 und Abs. 2 KommHV-Doppik in einer schriftlichen Dienstanweisung zu regeln, auf die wir etwas ausführlicher in Abschn. 3.2.3 eingehen.

Zum sicheren Umgang mit dem Passwort bzw. der PIN, die den persönlichen Signaturschlüssel vor missbräuchlicher Nutzung schützen soll, empfehlen wir, sich hierbei an den Basis-Anforderungen ORP.4.A8 „Regelung des Passwortgebrauchs", ORP.4.A22 „Regelung zur Passwortqualität" und ORP.4.A23 „Regelung für passwortverarbeitende Anwendungen und IT-Systeme" des BSI-Grundschutz-Kompendiums (siehe Fn. 48), Edition 2023, und den hierzu veröffentlichten Umsetzungshinweisen zu orientieren.

3.2.3 Welche Regelungen sind beim Einsatz fortgeschrittener Signaturen zu erlassen?

➢ Antwort:

Neben den schon in Abschn. 2.1.1 dargestellten Änderungen der Dienstanweisung für das Finanz- und Kassenwesen empfehlen wir, die Aufgaben und Sorgfaltspflichten der Registrierungsstelle und des Zertifikatsnehmers/Signaturschlüsselinhabers in einer eigenen, an die örtlichen Verhältnisse angepassten Dienstanweisung zu regeln. Insbesondere sollten darin die Unterrichtungspflichten der Registrierungsstelle, der sorgfältige und sichere Umgang des Unterzeichners mit seinen Signaturerstellungseinheiten/Signaturerstellungsdaten und die beim Abhandenkommen oder bei Kompromittierung des privaten Schlüssels notwendigen Maßnahmen näher festgelegt werden. Als Hilfestellung haben wir unter Nr. 4 und separat in der Anlage 1 eine Muster-Dienstanweisung beigefügt, die den Einsatz und den Umgang mit den Signaturzertifikaten und dem persönlichen Signaturschlüssel bzw. dem Software-Token der Bayern-PKI näher beschreibt.

[132] § 37 Abs. 1 Nrn. 3, 7 und 9 KommHV-Kameralistik/§ 33 Abs. 1 Nrn. 3, 7 und 9 KommHV-Doppik

➢ Im Detail:

Wie bereits im vorhergehenden Abschn. 3.2.2 dargestellt, ergeben sich aus den Nrn. 6, 8 und 10 AFS-HKR (siehe Fn. 6) und der Zertifizierungsrichtlinie der Bayern-PKI (siehe Fn. 105) einige Kontroll- und Sorgfaltspflichten für die Registrierungsstelle und den jeweiligen Zertifikatsnehmer/Signaturschlüsselinhaber[133]. Demzufolge muss auch der Einsatz sowie der sorgfältige und sichere Umgang mit den persönlichen Signaturerstellungseinheiten und -daten (z.B. Chipkarte, USB-Stick, TPM-Modul, PKCS#12-Datei oder OS-Zertifikatsspeicher) in einer schriftlichen Dienstanweisung geregelt werden (vgl. § 37 Abs. 2 KommHV-Kameralistik i.V. mit § 86 KommHV-Kameralistik/§ 33 Abs. 2 KommHV-Doppik i.V. mit § 97 KommHV-Doppik).

In einer solchen Dienstanweisung sollten insbesondere

- die Aufgaben der Registrierungsstelle,
- das Antragsverfahren,
- der Umfang der Nutzung,
- die Sorgfaltspflichten des Zertifikatsnehmers/Signaturschlüsselinhabers und
- der Umgang mit den Signaturerstellungsdaten bzw. Hard- oder Software-Token

näher geregelt werden.

Darüber hinaus sollten darin Regelungen aufgenommen werden, was bei

- Verlust oder Kompromittierung des persönlichen Signaturschlüssels oder
- Sperrung und ggf. Vernichtung von Signaturerstellungsdaten oder Signaturerstellungseinheiten

zu beachten ist und wer hierfür zuständig ist.

Um unsere Mitglieder bei der Erstellung einer solchen Signatur-Dienstanweisung (DA-Signatur) zu unterstützen, haben wir unter der Nr. 4 und separat in der Anlage 1 ein Muster beigefügt, dem der Einsatz von Software-Token zugrunde liegt, die von der Bayern-PKI nach der o.g. Zertifizierungsrichtlinie erstellt wurden.

Beim Einsatz von Hardware-Token oder Nutzung der PKI-Infrastruktur einer anderen Zertifizierungsstelle (z.B. AKDB für Fernsignaturen) wäre die DA-Signatur entsprechend anzupassen.

Hinsichtlich der beim Einsatz von schriftformersetzenden elektronischen Signaturen notwendigen Änderungen in der Dienstanweisung für das Finanz- und Kassenwesen dürfen wir auf die Ausführungen in Abschn. 2.1.1 verweisen.

[133] Bei Signaturzertifikaten mit persönlichen Signaturschlüsseln sind Zertifikatsnehmer, Zertifikatsverantwortlicher und Signaturschlüsselinhaber ein und dieselbe natürliche Person.

3.2.4 Welche Vorgehensweise empfiehlt sich für eine ordnungsgemäße Nutzung von Stapel- bzw. Komfortsignaturen?

➢ Antwort:

Damit auch bei einer Stapel- bzw. Komfortsignatur die Warn- und Hinweisfunktion der Unterschrift erhalten bleibt, muss vor Auslösung des Signaturvorgangs gewährleistet sein, dass

- die Zahl der im Stapel signierten Kassenanordnungen für den Unterschriftsbefugten überschaubar bleibt,
- die zu signierenden Daten vollständig und gut lesbar angezeigt werden und
- die Stapelsignaturen sich nur auf die zuvor angezeigten Daten beziehen.

Bei der Stapelsignatur von Zahlungsanordnungen sollte weder die hierfür maximal vorgegebene Zeitspanne noch die maximal vorgegebene Anzahl von Anordnungen überschritten werden.

Nach Ablauf des örtlich vorgegebenen Zeitintervalls oder bei Überschreitung der zulässigen Anzahl von Belegen muss sichergestellt sein, dass eine weitere Stapelsignatur nur durch die erneute Eingabe des Signaturschlüssel-Passworts ausgelöst werden kann.

➢ Im Detail:

Bereits mit Veröffentlichung der AFS-HKR vom 10.08.2010 war es zulässig, mehrere aufeinander folgende elektronische Kassenanordnungen im Stapel zu signieren (sog. Stapel- bzw. Komfortsignatur).[134] Daran hat sich auch mit der Veröffentlichung der neuen AFS-HKR vom 30.04.2019[135] nichts geändert. In der Praxis wird diese Möglichkeit gerne für die schnelle Abwicklung des „Massengeschäfts" im Anordnungswesen genutzt, zumal dies eine effiziente Sichtung und Signatur mehrerer Geschäftsvorfälle (Kassenanordnungen samt zahlungsbegründender Unterlagen) ermöglicht.

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. In der Begründung zu den AFS-HKR vom 30.04.2019, Abschn. 2.10, S. 11, wird dazu Folgendes ausgeführt:

„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."

Leider sind wir zwischenzeitlich in der Praxis auf Verfahrensweisen gestoßen, bei denen dieses Prinzip unterlaufen und die Visualisierung der Zahlungsanordnungen samt begründender Unterlagen umgangen werden konnte. In den von uns beanstandeten Fällen wurden die im Finanz-

[134] Vgl. Begründung zur AFS-HKR vom 10.08.2010, Abschn. 2.10, S. 11.
[135] Vgl. Begründung zur AFS-HKR vom 30.04.2019 (Fn. 6), Abschn. 2.10, S. 11.

verfahren oder elektronischen Workflow bereitgestellten Kassenanordnungen dem Unterzeichner lediglich in Listenform angezeigt und er konnte diese – auch ohne Visualisierung der Belege samt zahlungsbegründender Unterlagen – trotzdem im Stapel signieren und für die Zahlbarmachung durch die Kasse freigeben. Demnach bestand die Gefahr, dass Feststellungsbescheinigungen oder Zahlungsanordnungen erteilt werden, die vom jeweiligen Feststellungsbefugten oder Anordnungsberechtigten vorher nicht angesehen, also in Unkenntnis des Inhalts „blind" unterschrieben wurden.

Auch bei Anwendung der Stapel- bzw. Komfortsignatur ist daher programmtechnisch sicherzustellen, dass die Feststellungs- bzw. Anordnungsbefugten ihren Prüfpflichten im notwendigen Umfang nachkommen können, um den mit der elektronischen Signatur beabsichtigten Kontroll- und Sicherungszweck zu gewährleisten. Dies bedingt zwingend, dass dem jeweiligen Unterschriftsberechtigen die zu signierenden Daten vollständig angezeigt werden müssen (vgl. Nr. 10 Buchst. f AFS-HKR i.V. mit Anlage 3 Buchst. a zu den AFS-HKR und die Begründung zu Nr. 10 AFS-HKR).

Damit auch bei einer Stapel- bzw. Komfortsignatur die Warn- und Hinweisfunktion der Unterschrift erhalten bleibt,[136] muss vor Auslösung des Signaturvorgangs durch entsprechende technische und organisatorische Maßnahmen gewährleistet sein, dass

- die Zahl der im Stapel signierten Kassenanordnungen für den Anwender überschaubar bleibt[137],
- dem Unterzeichner die zu signierenden Daten vollständig und leicht lesbar angezeigt werden[138],
- sich die Stapelsignaturen nur auf die zuvor angezeigten Daten beziehen.[139]

Das Zeitfenster für Signiervorgänge und die Anzahl von Belegen, die nach der Überprüfung durch den Signierenden mit einer sog. Stapelsignatur verarbeitet werden können, sind örtlich festzulegen. Die Anzahl der zu signierenden Belege sollte vom jeweiligen Unterschriftsbefugten mit der vorhandenen IT-Ausstattung noch gut überblickt werden können. Bei einer Stapel- bzw. Komfortsignatur von Zahlungsanordnungen empfehlen wir eine Zeitspanne von max. 45 - 60 Min. Dabei sollte die Anzahl von maximal 30 bis 40 Anordnungen (entspricht rd. 90 - 120 Belegdokumenten)[140] nicht überschritten werden.

Nach Ablauf des vorgegebenen Zeitintervalls oder bei Überschreitung der zulässigen Anzahl von Belegen muss sichergestellt sein, dass eine weitere Stapelsignatur nur durch die erneute Eingabe des Signaturschlüssel-Passworts ausgelöst werden kann.

Im Übrigen verweisen wir auf die Regelungen und Hinweise in unserer Muster-Dienstanweisung-Signatur (vgl. Anlage 1 dieser FAQs).

---

[136] Vgl. Anlage 3 zur AFS-HKR (Fn. 6), Buchst. a Spiegelstrich fünf.
[137] Max. 30 - 40 Kassenanordnungen.
[138] Z.B. ausreichend großes Bildschirmfenster mit Bildlauf (Scrollfunktion).
[139] Kassenanordnungen mit den zu deren Verständnis notwendigen zahlungsbegründenden Unterlagen (= Belegdokumente).
[140] Diese Anzahl von Dokumenten orientiert sich an dem Maximalwert, der bei Stapelsignaturen in anderen Anwendungsgebieten festgelegt wurde (z.B. Empfehlungen der Bundesrechtsanwaltskammer zur Nutzung des besonderen elektronischen Anwaltspostfachs, https://www.brak.de/zur-rechtspolitik/newsletter/bea-newsletter/2019/ausgabe-2-2019-v-17012019.news.html).

3.2.5 Ist eine Benutzeranmeldung mit Passwort und Protokollierung der Benutzeraktivitäten als Unterschriftsersatz erlaubt?

➢ Antwort:

Die im Haushalts-, Kassen- und Rechnungswesen bei formgebundenen Wissens- und Willenserklärungen vorgeschriebenen Unterschriften (z.B. sachliche und rechnerische Feststellungen, förmliche und allgemeine Zahlungsanordnungen, elektronische Zahlungsverkehrsaufträge und Tagesabschlüsse/Tagesabgleiche) können nach den aktuell geltenden haushaltsrechtlichen Bestimmungen nur durch fortgeschrittene oder qualifizierte elektronische Signaturen ersetzt werden. Eine (einfache) Benutzerauthentifizierung mit Benutzerkennung und Passwort und verfahrensinterner Protokollierung der im Finanzverfahren oder elektronischen Workflow dokumentierten Benutzeraktivitäten vermag die vielfältigen Funktionen einer händischen Unterschrift oder die Funktions- und Sicherheitsmerkmale einer fortgeschrittenen bzw. qualifizierten elektronischen Signatur nicht zu ersetzen.

➢ Im Detail:

Seit Inkrafttreten der neuen Kommunalhaushaltsverordnungen (KommHV-Kameralistik und KommHV-Doppik) mit Wirkung vom 01.01.2007 können die Unterschriften bei sachlichen und rechnerischen Feststellungen[141], förmlichen und allgemeinen Zahlungsanordnungen[142], elektronischen Zahlungsverkehrsaufträgen[143] oder bei den Tagesabschlüssen/Tagesabgleichen[144] durch fortgeschrittene oder qualifizierte elektronische Signaturen i. S. von § 87 Nr. 12 KommHV-Kameralistik oder § 98 Nr. 21 KommHV-Doppik ersetzt werden. Die ergänzenden Merkmale der fortgeschrittenen elektronischen Signaturen[145] werden in den AFS-HKR vom 30.04.2019[146] näher bestimmt.

Auch bei rein elektronisch abgewickelten Vorgängen wird aufgrund der herausragenden Bedeutung der im Haushaltsrecht vorgeschriebenen Schriftform ein sicheres, vertrauenswürdiges, beweiskräftiges und verkehrsfähiges elektronisches Mittel als Unterschriftsersatz benötigt, welches der Verwender mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle nutzen kann. Gerade mit fortgeschrittenen oder qualifizierten elektronischen Signaturen kann die Warn-, Hinweis- und insbesondere Perpetuierungsfunktion der händischen Unterschrift besonders gut in elektronischer Form nachgebildet werden. Die Verbindung der elektronischen Signatur mit den Kassenanordnungen bewahrt deren Belegcharakter und ermöglicht eine retrograde und progressive Prüfung der elektronischen Buchführung, die unabhängig vom eingesetzten Finanzwesen und der verfahrensinternen Protokollierung ist. Sie ermöglicht, ähnlich wie die handschrift-

[141] Vgl. § 41 Abs. 1 Satz 2 KommHV-Kameralistik/§ 37 Abs. 1 Satz 2 KommHV-Doppik.
[142] Vgl. § 39 Abs. 1 Satz 2 KommHV-Kameralistik/§ 35 Abs. 1 Satz 2 KommHV-Doppik.
[143] Vgl. § 43 Abs. 3 Satz 2 KommHV-Kameralistik/§ 39 Abs. 3 Satz 2 KommHV-Doppik.
[144] Vgl. § 72 Abs. 1 Satz 2 KommHV-Kameralistik/§ 68 Abs. 1 Satz 3 KommHV-Doppik.
[145] Die fortgeschrittenen elektronischen Signaturen sind in der eIDAS-VO, wie schon im zwischenzeitlich außer Kraft getretenen SigG, nur legaldefiniert, aber im Gegensatz zu den qualifizierten elektronischen Signaturen (eIDAS-VO, Vertrauensdienstegesetz, Vertrauensdiensteverordnung) nicht näher gesetzlich geregelt.
[146] Siehe Fn. 6.

liche Unterschrift, die Identifizierung des Unterzeichners selbst dann, wenn der Benutzer im Finanzverfahren oder elektronischen Workflow ein Funktions-[147] oder Sammel-Benutzerkonto[148] nutzt, was in der Praxis gar nicht so selten anzutreffen ist.[149]

Dieser besonderen Bedeutung wird vom Verordnungsgeber in den Begriffsbestimmungen der aktuell geltenden Kommunalhaushaltsverordnungen (vgl. § 87 Nr. 12 KommHV-Kameralistik/ § 98 Nr. 21 KommHV-Doppik) und durch die Verweise auf die Legaldefinitionen in Art. 3 Nr. 11 und Nr. 12 eIDAS-VO dahingehend Rechnung getragen, dass sowohl bei den fortgeschrittenen als auch qualifizierten elektronischen Signaturen die folgenden Anforderungen erfüllt sein müssen:

a) Die Signaturen müssen Daten in elektronischer Form sein, die den unterzeichneten elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die vom Inhaber des Signaturschlüssels (Unterzeichner) zum Unterzeichnen verwendet werden.
b) Die Signaturen müssen zuverlässig die Identifizierung des Unterzeichners ermöglichen und diesem eindeutig zugeordnet sein.
c) Die Signaturen werden unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
d) Die Signaturen müssen so mit den auf diese Weise unterzeichneten Daten verbunden sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Diese Anforderungen werden durch eine normale Authentisierung des Benutzers (Kennung und Passwort) und die Protokollierung der Benutzeraktivitäten nicht erfüllt, da diese

- vom Unterzeichner weder beeinflusst noch mit einem hohen Maß an Vertrauen allein kontrolliert werden können,
- die Unversehrtheit oder eine nachträgliche Veränderung der elektronischen Feststellungsbescheinigungen, Zahlungsfreigaben, Tagesabschlüsse/Tagesabgleiche oder Kassenanordnungen nicht erkennen lassen,
- im Gegensatz zur Unterschrift keine Warn-, Hinweis-, Perpetuierungs- oder Abschlussfunktion besitzen,[150]
- oftmals nicht mit dem Kassenbeleg verbunden oder uneingeschränkt verkehrsfähig ist,
- in der Regel nicht mit vertrauenswürdigen kryptographischen Techniken gegen Manipulationen abgesichert sind und

[147] Funktionskonten sind ausschließlich der jeweiligen Stelle und keiner natürlichen Person zugeordnet (z.B. Steuer_1 bis Steuer_x, Kasse_1 bis Kasse_x). Werden diese anonymisierten Konten über mehrere Jahre von verschiedenen Stelleninhabern genutzt, ist weder eine klare Zuordnung noch eine maschinelle Auswertbarkeit der Benutzeraktivitäten sichergestellt.
[148] Sammel-Benutzerkonten sind Benutzerkonten, die zum Teil über mehrere Jahre von mehreren natürlichen Personen, ggf. sogar externen IT-Dienstleistern, genutzt werden (sog. shared user accounts). In diesen Fällen ist weder eine personenbezogene Zuordnung noch eine maschinelle Auswertbarkeit der Benutzeraktivitäten gewährleistet. Da es sich hierbei oftmals um privilegierte Standard- bzw. Built-In-Konten handelt, gefährdet dies zudem die IT-Sicherheit.
[149] Beispielsweise bei einer Authentifizierung mit einem nicht personenbezogenen Funktions- oder Sammel-Benutzerkonto die zuverlässige Identifizierung des Unterzeichners zumindest erheblich erschwert, ggf. sogar unmöglich macht; damit lässt sich im Nachhinein nicht oder nur schwer nachvollziehen, welche natürliche Person („Wer") den Anspruch oder die Zahlungsverpflichtung tatsächlich geprüft oder zur Zahlbarmachung freigegeben hat.
[150] Vgl. dazu die Begründung der AFS-HKR vom 30.04.2019 (Fn. 6), Abschn. 1.2 u. 2.10; zu den Funktionen der Unterschrift und deren Abbildung bei elektronischen Signaturen vgl. LT-Drs. 14/9960, S. 11.

– die Funktion des Belegs als Nachweis und Kontrollinstrument für eine ordnungsgemäße Buchführung in Frage stellen, insbesondere dann, wenn die Protokolldaten (Sicht-, Prüf-, Kontierungs- und Anordnungsinformationen) nur noch in dem für die Führung der Bücher eingesetzten Verfahrens gespeichert sind.[151]

3.2.6 Müssen Eigenbetriebe, Körperschaften oder Einrichtungen, für die § 10 Abs. 1 Satz 3 EBV gilt, ebenfalls elektronische Signaturen verwenden?

➢ Antwort:

Auch bei kommunalen Unternehmen, die gem. § 10 Abs. 1 EBV eine gesonderte Kasse nach den Grundsätzen ordnungsmäßiger Buchführung führen, können die Unterschriften der Feststellungsbefugten, Anordnungsberechtigten oder mit dem Zahlungsverkehr beauftragten Beschäftigten (z.B. bei der Bescheinigung der sachlichen und rechnerischen Richtigkeit von Ansprüchen oder Zahlungsverpflichtungen, Erteilung von förmlichen oder allgemeinen Zahlungsanordnungen, Legitimation elektronischer Zahlungsverkehrsaufträge) durch fortgeschrittene oder qualifizierte elektronische Signaturen ersetzt werden.

Damit lassen sich im Kassen- und Rechnungswesen der kommunalen Unternehmen ebenfalls vertrauenswürdige, vollständig digitalisierte und damit friktionslose Geschäftsprozesse realisieren. Zudem lässt sich damit, unabhängig vom eingesetzten Finanzverfahren oder Workflowsystem, die ordnungsgemäße Wahrnehmung der Prüf- und Kontrollpflichten bei Ein- und Auszahlungen, der Anordnungsbefugnis oder der Befugnis zum Zahlungsverkehr nachvollziehbar im elektronischen Belegarchiv dokumentieren.[152]

➢ Im Detail:

Nach § 10 Abs. 1 Sätze 1 und 2 EBV hat der Eigenbetrieb eine gesonderte Kasse einzurichten, die nach den Grundsätzen ordnungsmäßiger Buchführung zu führen ist. Eine generelle Anwendung der Kommunalhaushaltsverordnungen auf das gesamte Rechnungswesen des Eigenbetriebs ist allerdings ausgeschlossen. Bei unbaren Zahlungen sind nur die enumerativ aufgezählten (vorwiegenden) Sicherheitsbestimmungen der Kommunalhaushaltsverordnungen anwendbar (vgl. § 10 Abs. 1 Satz 3 EBV). Auf bare Ein- und Auszahlungen finden dagegen die die Abschnitte 8 bis 12 der KommHV-Doppik sowie die Abschnitte 9 bis 13 der KommHV-Kameralistik entsprechende Anwendung.[153]

Für den Einsatz von elektronischen Signaturen bei den kommunalen Unternehmen, die außerhalb der allgemeinen Verwaltung als Sondervermögen ohne eigene Rechtspersönlichkeit geführt werden (Eigenbetriebe, Art. 88 GO),[154] bedeutet dies konkret:

---

[151] Es kann und darf u.E. nicht sein, dass beispielsweise bei einem Wechsel des Finanzverfahrens alle bisher protokollierten Wissens- und Willenserklärungen nicht mehr nachvollziehbar sind und nicht mehr maschinell ausgewertet werden können.

[152] Somit bleibt auch bei vollständig digitalisierten Geschäftsprozessen der Belegcharakter der förmlichen Gedankenerklärungen erhalten.

[153] Vgl. hierzu ausführlich die Gemeindekasse Bayern (GK) 2002 RdNr. 34 und Wager, Eigenbetriebsverordnung Bayern (EBV), Erl. 3 zu § 10 EBV.

[154] Oder für diejenigen kommunalen Körperschaften oder Einrichtungen, auf die die EBV aufgrund spezialgesetzlicher Bestimmungen, z.B. gem. Art. 40 Abs. 2 KommZG, ebenfalls anwendbar ist.

- Sowohl bei baren als auch unbaren Zahlungen ist insbesondere jeder Anspruch und jede Zahlungsverpflichtung auf Grund und Höhe zu prüfen. Die Richtigkeit ist schriftlich oder durch eine fortgeschrittene oder qualifizierte elektronische Signatur zu bescheinigen (sachliche und rechnerische Feststellung).[155]
- Sowohl bei baren als auch unbaren Ein- und Auszahlungen sind der gesonderten Kasse, entsprechend den haushaltsrechtlichen Bestimmungen, förmliche oder allgemeine Zahlungsanordnungen zu erteilen. In vielen örtlichen Regelungen sind darüber hinaus Kassenanordnungen i.S. des § 38 KommHV-Kameralistik/§ 34 KommHV-Doppik[156] vorgeschrieben.[157] Bei Einsatz automatisierter Verfahren kann die Unterschrift des Anordnungsberechtigten daher ebenfalls durch elektronische Signaturen ersetzt werden.[158]
- Zahlungsverkehrsaufträge, die über die kontoführenden Institute (Banken oder Sparkassen) abgewickelt werden, können gleichfalls mit Hilfe von elektronischen Signaturen autorisiert und freigegeben werden.[159]

Dies ermöglicht Eigenbetrieben oder anderen kommunalen Körperschaften und Einrichtungen, deren gesonderte Kasse nach der EBV und damit nach den Grundsätzen ordnungsgemäßer Buchführung (GoB) geführt wird, ebenfalls eine friktionslose elektronische Abwicklung der Geschäftsvorfälle sowie der Anordnungs- und Kassengeschäfte. Da die Eintragungen in den Büchern auch nach den GoB/GoBD vollständig, richtig, zeitgerecht und geordnet erfolgen müssen (vgl. § 239 Abs. 2 HGB, § 146 Abs. 1 AO), muss weiterhin für jede Buchung, auch für jede Kassenbuchung, ein schriftlicher oder elektronischer Beleg vorhanden sein. Aus diesem muss sich der materielle Gehalt des gebuchten Geschäftsvorfalls eindeutig ergeben; er muss datiert und in der papiergebundenen Form handschriftlich unterzeichnet oder in der schriftformersetzenden digitalen Form elektronisch signiert sein. Der Beleg muss, unabhängig vom Format, auf die Buchungen hinweisen (z.B. durch die sog. Kontierung des Beleges). Außerdem hat jede Buchung einen Hinweis auf den Beleg und seine Fundstelle zu enthalten.[160] Im Übrigen dürfen wir in diesem Zusammenhang auf die ausführliche Darstellung der zu beachtenden gesetzlichen Rahmenbedingungen in der Gemeindekasse 2002 RdNrn. 34, 44 und 54 und bei Wager, Eigenbetriebsverordnung in Bayern (EBV) mit Verwaltungsvorschriften und Musterbetriebssatzung, 4. Fassung, Februar 2021, Erl. 1 zu § 10 EBV verweisen.

Auch wenn dies in § 10 Abs. 1 Satz 3 und Abs. 2 EBV nicht explizit geregelt ist, müssen die verwendeten fortgeschrittenen elektronischen Signaturen dem in den Kommunalhaushaltsverordnungen vorgegebenen Qualitätsniveau entsprechen. Dies stellt u.E. eine einheitliche Handhabung schriftformersetzender elektronischer Signaturen im Haushalts-, Kassen- und Rechnungswesen der bayerischen Kommunen und deren Einrichtungen sicher, erhöht deren Beweiswert, erleichtert deren Prüfbarkeit (Integrität und Authentizität) und schafft somit das für die Nicht-Abstreitbarkeit der elektronischen Signatur erforderliche Sicherheits- und Vertrauensniveau.

---

[155] Vgl. § 10 Abs. 1 Satz 3 und Abs. 2 EBV i.V. mit § 41 Abs. 1 Sätze 1 und 2 KommHV-Kameralistik/§ 37 Abs. 1 Sätze 1 und 2 KommHV-Doppik.
[156] Sofern bei Einzahlungen wg. der kaufmännischen Buchführung darauf nicht gem. § 84 Satz 3 Halbsatz 1 KommHV-Kameralistik/§ 95 Satz 3 Halbsatz 1 KommHV-Doppik verzichtet wird.
[157] Die ergänzenden Bestimmungen einer Betriebssatzung gelten gem. § 1 Abs. 1 EBV ergänzend zur EBV.
[158] Vgl. § 10 Abs. 1 Satz 3 und Abs. 2 EBV i.V. mit § 84 Satz 3, § 39 Abs. 1 Satz 2 und § 40 Abs. 1 Satz 1 KommHV-Kameralistik/§ 95 Satz 3, § 35 Abs. 1 Satz 2 und § 36 Abs. 1 Satz 1 KommHV-Doppik und Schreml/Bauer/Westner, a.a.O., Erl. 4 zu § 84 KommHV-Kameralistik/Erl. 4 zu § 95 KommHV-Doppik.
[159] Vgl. § 10 Abs. 1 Satz 3 i.V. mit § 43 Abs. 3 Satz 2 KommHV-Kameralistik/§ 39 Abs. 3 Satz 2 KommHV-Doppik.
[160] Vgl. hierzu ausführlich GK 2002 RdNr. 34 und Wager, a.a.O., Erl. 3 zu § 10 EBV.

3.3 Elektronische Signaturen beim Electronic Banking

Im BKPV-Geschäftsbericht 2010 haben wir uns ausführlich mit dem Thema „Einsatz von Electronic-Banking-Systemen" im kommunalen Bereich befasst. Mit Blick auf die damals geltenden haushaltsrechtlichen Bestimmungen (KommHV-Kameralistik und KommHV-Doppik vom 05.10.2007, AFS-HKR vom 10.08.2010) kamen wir zum Ergebnis, dass sich für den beleglosen elektronischen Zahlungsverkehr mit den kontoführenden Instituten (Banken und Sparkassen) für Kommunen aus rechtlicher und technischer Sicht grundsätzlich die beiden Sicherungs- und Übertragungsverfahren FinTS/HBCI oder EBICS mit dem Sicherungsmedium Chipkarte eignen (vgl. BKPV-Geschäftsbericht 2010, „Hinweise zum Einsatz von Electronic-Banking-Systemen", Abschn. 4.6, S. 80 ff. und Abb. 5).

Im Vergleich zu den damals betrachteten Electronic-Banking-Lösungen haben sich aufgrund der zunehmenden Digitalisierung zwischenzeitlich zahlreiche neue Varianten etabliert, die vor allem im Privat-, Geschäfts- und Gewerbekundenbereich zu einem geänderten Nutzungsverhalten geführt haben (z.B. browsergestütztes oder App-basiertes Internet-Banking mit mobilen Endgeräten, Smartphones und Tablets). Diese neuen Nutzungsformen, aber auch zahlreiche Schadensfälle[161] haben auf europäischer Ebene zu neuen regulatorischen Vorgaben geführt, die u.a. die Sicherheit im elektronischen Zahlungsverkehr erhöhen und die Rechte von Zahlungsdienstnutzern, insbesondere bei nicht autorisierten Zahlungsvorgängen, stärken sollen.[162] Die EU-Richtlinie wurde mit dem Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie vom 17.07.2017 mit Wirkung ab 13.01.2018 in nationales Recht umgesetzt. Mit diesen gesetzlichen Vorgaben wurde insbesondere eine verbesserte Sicherheit bei der Zahlungsabwicklung angestrebt, bei der der Zahlungsdienstleister eine starke Kundenauthentifizierung sicherstellen muss, wenn der Kunde online auf sein Zahlungskonto zugreift, einen elektronischen Zahlungsvorgang auslöst oder über einen Fernzugang eine Handlung vornimmt, die ein Betrugs- oder Missbrauchsrisiko in sich birgt.[163]

Hinzu kommt, dass das signaturbasierte Sicherheitsverfahren FinTS/HBCI (mit ZKA Banken-Signaturkarte oder DDV-Chipkarte mit ec-Karten-Betriebssystem) aufgrund der geringen Nachfrage von Privatkunden und des geänderten Nutzungsverhaltens des Ziel-Kundenkreises sowohl von den Sparkassen als auch von vielen Banken zwischenzeitlich eingestellt wurde. Im Zuge dieser Umstellung wurden auch einigen Kommunen entweder andere FinTS Sicherungsverfahren/Sicherheitsmedien (z.B. chipTAN-USB, chipTAN optisch/manuell, chipTAN QR, pushTAN) oder sehr häufig der Umstieg auf das bereits bei vielen anderen Kommunen und Unternehmenskunden eingesetzte, signaturbasierte EBICS Sicherungs- und Übertragungsverfahren mit unterschiedlichen Sicherungsmedien[164] (Chipkarte, USB-Stick oder Sicherheitsdatei) angeboten.

Aus kommunalrechtlicher Sicht lassen aber auch die seit Ende April 2019 geänderten haushaltsrechtlichen Rahmenbedingungen zum Einsatz von fortgeschrittenen Signaturen neue Gestaltungsmöglichkeiten beim Online-Banking zu, da die ursprüngliche Verpflichtung zur Nutzung chipkartenbasierter Signaturlösungen entfallen ist und demzufolge sowohl der Einsatz eines

[161] Vgl. Cybercrime Bundeslagebild 2015 und 2016, www.bka.de
[162] Vgl. insb. die Erwägungsgründe 7, 69 bis 73 und insb. 95 und 96 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25.11.2015 über Zahlungsdienste im Binnenmarkt - Zweite Zahlungsdiensterichtlinie (Payments Services Directive 2 - PSD2).
[163] Vgl. BR-Drs. 158/17, S. 88 und BT-Drs. 18/11495, S. 81.
[164] Vgl. PPI/Travic EBICS-Kompendium vom 28.12.2021, S. 21 (https://www.ppi.de/payments/ebics/ebics-kompendium).

weiteren Hardware-Tokens (passwortgesicherter und verschlüsselter USB-Stick mit Sicherheitsdatei) als auch eines Software-Tokens (z.B. passwortgeschützte kryptographische Sicherheitsdatei in besonders geschütztem Speicherbereich) möglich ist. Dies und die Tatsache, dass bei EBICS die an das kontoführende Institut übertragenen Zahlungsverkehrsaufträge mit zwei verteilten Auftragssignaturen[165] freigegeben werden können, ermöglichte insbesondere bei den durch die COVID-19 Pandemie bedingten Einschränkungen und den daraus resultierenden Anforderungen eine reibungslose Abwicklung des beleglosen elektronischen Zahlungsverkehrs.

Vor diesem Hintergrund möchten wir nachfolgend unsere Einschätzungen und Empfehlungen zum Online-Banking aus dem Jahr 2010 fortschreiben und zugleich einige Fragen aus der Praxis beantworten.

3.3.1 Erfüllen EBICS-Signaturen die haushaltsrechtlichen Anforderungen?

➢ Antwort:

Beim beleglosen elektronischen Zahlungsverkehr mit den Sparkassen und Banken können die mit dem EBICS Sicherungs- und Übertragungsstandard an das jeweilige Rechenzentrum des kontoführenden Instituts übertragenen Zahlungsverkehrsdaten[166] mit zwei Auftragssignaturen[167] (sog. elektronische Unterschrift), die zwei gemeinschaftlich verfügungsberechtigte Beschäftigte[168] unabhängig voneinander erstellen, bankfachlich legitimiert werden. Dies setzt neben einer sicheren Authentisierung der zeichnungsbefugten Benutzer[169] die ordnungsgemäße Verwendung und sichere Aufbewahrung der persönlichen Signaturerstellungsdaten durch die beiden am elektronischen Zahlungsverkehr beteiligten Beschäftigten voraus.[170] Zudem sind die bei der Abwicklung der o.g. Geschäftsvorfälle erzeugten Ausgabeprotokolle für die Dauer der Aufbewahrungsfristen wie elektronische Belege aufzubewahren.[171]

➢ Im Detail:

Mit den seit 01.01.2007 geltenden Kommunalhaushaltsverordnungen wurde auch beim unbaren Zahlungsverkehr mit den kontoführenden Kreditinstituten (Sparkassen und Banken) der beleglose elektronische Zahlungsverkehr mit Hilfe von elektronischen Zahlungsverkehrssystemen[172] und der Ersatz der im „Vier-Augen-Prinzip" zu leistenden Unterschriften durch hierfür geeignete elektronische Signaturen zugelassen.

---

[165] Dies setzt die Vereinbarung einer gemeinschaftlichen Verfügungsbefugnis für das Giro- bzw. Kontokorrentkonto und entsprechende Berechtigungen der Signaturschlüsselinhaber voraus (z.B. A+A, A+B).
[166] Überweisungsaufträge, Abbuchungsaufträge, Einzugsermächtigungen i.S. von § 43 Abs. 3 Satz 1 KommHV-Kameralistik/§ 39 Abs. 3 KommHV-Doppik.
[167] Nach den bankfachlichen kryptographischen Verfahren A005 oder A006, vgl. PPI/Travic EBICS Kompendium, Abschn. 5.2.2, S. 22, vgl. Fn. 165.
[168] Beschäftigte mit gemeinschaftlicher Verfügungsbefugnis oder einer reinen Mitzeichnungsbefugnis (bankfachlich: A- oder B-Berechtigung).
[169] Bankfachlich als Einreicher bezeichnet.
[170] Vgl. hierzu BKPV-Geschäftsbericht 2010, Abschn. 6, S. 86 f.
[171] Vgl. § 37 Abs. 1 Nr. 7 i.V. mit § 82 Abs. 2 Satz 5 KommHV-Kameralistik/ § 33 Abs. 1 Nr. 7 i.V. mit § 69 Abs. 2 Satz 6 KommHV-Doppik.
[172] Automatisierte Verfahren i.S. von § 37 Abs. 1 KommHV-Kameralistik/§ 33 Abs. 1 KommHV-Doppik, die neben den bankfachlichen Anforderungen auch die haushaltsrechtlichen Sicherheitsanforderungen erfüllen und gem. § 37 Abs. 1 Nr. 1 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 1 KommHV-Doppik örtlich zur Nutzung freigegeben wurden.

Wie bereits im BKPV-Geschäftsbericht 2010, Abschn. 6 S. 86 f. dargestellt, handelt es sich bei den bankfachlichen Auftragssignaturen um fortgeschrittene Signaturen i.S. von Art. 3 Nr. 11 eIDAS-VO, die aus unserer Sicht bei einer ordnungsgemäßen und sicheren Anwendung der im EBICS Sicherungs- und Übertragungsstandard (kurz: EBICS-Standard) vorgesehenen Sicherheitsmedien[173] die Anforderungen des Art. 26 eIDAS-VO erfüllen. Allerdings handelt es sich bei den für die Erzeugung der bankfachlichen Signaturen verwendeten Kryptodaten um keine X.509-Zertifikate[174], denen eine PKI-Infrastruktur i.S. der AFS-HKR vom 30.04.2019 (siehe Fn. 6) zugrunde liegt. Dennoch gehen wir davon aus, dass die in den aktuellen EBICS-Spezifikationen V 3.0.1 festgelegten bankfachlichen Anforderungen und die Orientierung an internationalen und nationalen Krypto-Standards (z.B. BSI-Krypto-Katalog) ein gleichwertiges Sicherheits- und Vertrauensniveau gewährleisten.

Zudem gewährleistet die bei EBICS vorgeschriebene Authentifizierungssignatur eine zuverlässige und sichere Identifizierung des jeweiligen Benutzers (Zwei-Faktor-Authentifizierung des Einreichers), bevor dieser die elektronischen Zahlungsverkehrsaufträge mit seiner Auftragssignatur legitimieren kann.

Beim Einsatz von Chipkarten als EBICS-Sicherheitsmedium kann u.E. von einem hohen Sicherheitsniveau und bei der Verwendung von verschlüsselten und passwortgeschützten USB-Sticks mit Sicherheitsdatei von einem substantiellen Sicherheitsniveau ausgegangen werden. Beim Einsatz von passwortgeschützten, kryptographisch gesicherten Sicherheitsdateien muss durch flankierende technische und organisatorische Maßnahmen sichergestellt werden, dass der Verwender der elektronischen Signaturerstellungsdaten (Signaturschlüsselinhaber) diese mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Wir empfehlen hierzu eine Orientierung an den Sicherheitsempfehlungen der Deutschen Kreditwirtschaft für Firmenkunden vom 03.09.2018.[175]

Sind die vorstehend genannten Anforderungen sichergestellt, kann auch weiterhin auf den Ausdruck und die zweifache Unterzeichnung der automatisiert erstellten Ausgabeprotokolle verzichtet werden. Allerdings sollten Letztere – wie bisher – für die Dauer der haushaltsrechtlichen Aufbewahrungsfristen in elektronischer Form aufbewahrt werden, da es sich hier um Unterlagen handelt, die als Nachweis für die ordnungsgemäße Abwicklung des unbaren elektronischen Zahlungsverkehrs (vgl. § 37 Abs. 1 Nr. 7 KommHV-Kameralistik/33 Abs. 1 Nr. 7 KommHV-Doppik) und ggf. als Auszahlungsnachweise herangezogen werden können.

Insoweit sind auch diese elektronischen Dokumente wie Belege i.S. von § 71 Abs. 1 KommHV-Kameralistik/§ 67 Abs. 1 KommHV-Doppik aufzubewahren, also in einer Weise zu speichern, die deren Unveränderbarkeit gewährleistet. Wir empfehlen nach unseren langjährigen Erfahrungen

[173] Vorzugsweise Chipkarte, alternativ gehärtetes USB-Speichermedium oder Sicherheitsdatei.

[174] Obwohl diese im EBICS Sicherungs- und Übertragungsstandard vorgesehen und offenbar in Frankreich bereits eine entsprechend geregelte PKI-Infrastruktur betrieben wird – vgl. das von der PPI AG veröffentlichte EBICS Kompendium vom 28.12.2021, Abschn. 5.3, S 23, vgl. Fn. 165.

[175] Die Deutsche Kreditwirtschaft (kurz DK) ist als Zusammenschluss des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken, des Bundesverbandes deutscher Banken, des Bundesverbandes Öffentlicher Banken Deutschlands, des Deutschen Sparkassen- und Giroverbandes und des Verbandes deutscher Pfandbriefbanken die Interessenvertretung der kreditwirtschaftlichen Spitzenverbände. Sie ist im August 2011 hervorgegangen aus dem Zentralen Kreditausschuss (ZKA) und führt dessen Arbeit fort (Quelle: Die Deutsche Kreditwirtschaft, https://die-dk.de/).

eine Aufbewahrung in einem dafür geeigneten elektronischen Belegarchiv oder Dokumentenmanagementsystem. Eine Aufbewahrung der Ausgabeprotokolle im Dateisystem[176] oder im Online-Banking-Verfahren[177] ohne zusätzliche technische und organisatorische Schutzmaßnahmen würde der o.g. haushaltsrechtlichen Anforderung nicht gerecht. Außerdem wäre sicherzustellen, dass die in § 37 Abs. 1 KommHV-Kameralistik/§ 33 Abs. 1 KommHV-Doppik genannten Anforderungen gewährleistet sind.

3.3.2 Können beim Electronic Banking anstelle des signaturbasierten EBICS oder FinTS/HBCI auch andere Sicherheitsverfahren und -medien als Ersatz für die Unterschriften der Einreicher eingesetzt werden?

Oftmals werden wir gerade von kleinen Kommunen oder Einrichtungen gefragt, ob beim beleglosen elektronischen Zahlungsverkehr mit den Sparkassen und Banken alternativ zum bisher verwendeten FinTS/HBCI-Verfahren[178] die im Privatkundenbereich üblichen Sicherungsverfahren und -medien[179] eingesetzt werden können.

➢ Antwort:

Nach den aktuell geltenden haushaltsrechtlichen Bestimmungen können die Unterschriften der am beleglosen elektronischen Zahlungsverkehr beteiligten Beschäftigten (Einreicher) nur durch qualifizierte oder fortgeschrittene elektronische Signaturen ersetzt werden. Daraus folgt, dass für das Electronic Banking in Kommunalkassen ausschließlich signaturbasierte Legitimierungsverfahren in Betracht kommen, die seit der Einstellung von FinTS/HBCI[180] nur noch mit dem multibankfähigen Sicherungs- und Übertragungsverfahren EBICS[181] abgebildet werden können.

Die vor allem im Privatkundenbereich bei kleineren Geschäfts- oder Gewerbekunden verbreiteten TAN-Sicherungsverfahren[182] scheiden damit als Ersatz für die Unterschrift beim beleglosen, elektronischen Zahlungsverkehr in Kommunalkassen aus.

Die im BKPV-Geschäftsberichtsbeitrag 2010, „Hinweise zum Einsatz von Electronic-Banking-Systemen", Abschn. 6, beschriebene Behelfslösung, die automatisch generierten Ausgabeprotokolle auszudrucken und diese von den beiden am Legitimations- bzw. Freigabevorgang beteiligten Beschäftigten handschriftlich unterzeichnen zu lassen, hat sich in der Vergangenheit nicht bewährt und verursacht erneute Medienbrüche. Mit Blick auf die fortschreitende Digitalisierung der Verwaltung und insbesondere um friktionslose elektronische Arbeitsprozesse zu gewährleisten, empfehlen wir diese Behelfslösung daher nicht mehr.

[176] Mit eingeschränkten Zugangs- und Zugriffsrechten (z.B. NTFS-Berechtigungen).
[177] Mit verfahrensspezifischen Sicherungsmaßnahmen (z.B. Verschlüsselung).
[178] Mit Kartenleser und Chipkarte.
[179] Z.B. chipTAN-USB, chipTAN optisch/manuell, chipTAN QR, pushTAN oder smsTAN.
[180] Dieses chipkartenbasierte Sicherungs- und Übertragungsverfahren wurde von den Sparkassen, Landesbanken und vielen anderen Banken Ende 2021 aus technischen und rechtlichen Gründen eingestellt.
[181] EBICS = Electronic Banking Internet Communication Standard
[182] Vgl. hierzu Fn. 180.

➢ Im Detail:

Wie bereits im vorstehenden Abschn. 3.3 und 3.3.1 sowie im BKPV-Geschäftsbericht 2010, a.a.O., Abschn. 2.3 und 6 dargestellt, können nach den aktuell geltenden haushaltsrechtlichen Bestimmungen die Unterschriften der beiden Einreicher bei den in § 43 Abs. 3 Satz 1 KommHV-Kameralistik/§ 39 Abs. 3 Satz 1 KommHV-Doppik genannten Zahlungsverkehrsaufträgen[183] nur durch qualifizierte oder fortgeschrittene elektronische Signaturen ersetzt werden. Daraus folgt, dass für das Electronic Banking in Kommunalkassen ausschließlich signaturbasierte Legitimierungsverfahren in Betracht kommen, die seit der Einstellung von FinTS/HBCI nur noch mit dem multibankfähigen Sicherungs- und Übertragungsverfahren EBICS abgebildet werden können.

Insoweit kann dahingestellt bleiben, ob die mit dem Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie vom 17.07.2017 festgelegten Anforderungen an eine sichere Benutzerauthentifizierung (Zwei-Faktor-Authentisierung) mit bestimmten TAN-Verfahren (z.B. chipTAN-USB oder chipTAN optisch/manuell) und besonderen technischen und organisatorischen Rahmenbedingungen ein technisch vergleichbares Vertrauensniveau wie eine fortgeschrittene Signaturlösung mit einem Software-Token bieten können (substantielles Vertrauensniveau, vgl. BSI TR 03107 vom 07.05.2019 [siehe Fn. 99], Abschn. 7.3 und 10.3). Das Vertrauensniveau eines TAN-basierten Mechanismus hängt, sofern sich damit das haushaltsrechtlich vorgeschriebene Vier-Augen-Prinzip überhaupt praxisgerecht nachbilden lässt, im Wesentlichen von der Einbettung des TAN-Verfahrens in das Gesamtsystem ab und muss daher nach Ansicht des BSI im Einzelfall betrachtet werden. Inwieweit ein für Firmenkunden und verteilte elektronische Unterschriften geeignetes TAN-Verfahren ggf. Gegenstand einer Ausnahmegenehmigung i.S. des Art. 117a GO sein könnte, haben wir daher nicht näher untersucht. Dies wäre ggf. im Benehmen mit dem Bayerisches Staatsministerium des Innern, für Sport und Integration zu klären.

Die im GB-Beitrag 2010, a.a.O., Abschn. 6, beschriebene Behelfslösung (Unterzeichnung der Ausgabeprotokolle) halten wir zwischenzeitlich aus verwaltungsökonomischen Gründen und zur Vermeidung von unnötigen Medienbrüchen nicht mehr für zeitgemäß. Denn mit Blick auf die fortschreitende elektronische Aktenführung in den Kommunalverwaltungen, insbesondere die weit verbreiteten elektronischen Belegarchive, sind bei einer solchen Lösung drei zusätzliche Arbeitsschritte nötig (Ausdruck des Ausgabeprotokolls, Unterschrift der am elektronischen Zahlungsverkehr beteiligten Beschäftigten und anschließende Digitalisierung des papiergebundenen Hilfsbelegs), die beim Einsatz von EBICS entfallen.

Hinzu kommen die weiteren Vorteile des EBICS Sicherungs- und Übertragungsverfahrens (z.B. verteilte elektronische Unterschrift, standortunabhängige Freigabe von Zahlungsverkehrsaufträgen, keine Limitierung bei den Transaktionsdatensätzen, Multibankfähigkeit, Abdeckung aller bankfachlichen Auftragsarten, erhöhte Übertragungssicherheit durch bankfachliche Authentifizierungs- und Auftragssignaturen und Ende-zu-Ende Verschlüsselung auf Transportebene)[184], die aus unserer Sicht eindeutig für den Einsatz dieses Sicherungs- und Übertragungsverfahrens sprechen.

[183] Seit der Umstellung auf den einheitlichen Euro-Zahlungsverkehrsraum SEPA: SEPA-Überweisungen und -Lastschriften.
[184] Vgl. hierzu ergänzend das von PPI AG veröffentlichte EBICS-Kompendium vom 28.12.2021, Abschn. 1.1, S. 6 ff., vgl. Fn. 165.

4 Anlage 1 - Muster-Dienstanweisung zum Einsatz fortgeschrittener elektronischer Signaturen im Haushalts-, Kassen- und Rechnungswesen

Muster-Dienstanweisung
zum
Einsatz fortgeschrittener elektronischer Signaturen
im Haushalts-, Kassen- und Rechnungswesen
der Gemeinde *xxx*

(Stand: 19.06.2023)

BKPV-Anmerkung: Die Muster-Dienstanweisung ist an die örtlichen Verhältnisse anzupassen. Die Muster-Dienstanweisung wurde für das Beispiel erstellt, dass die Zertifikate für die elektronischen Signaturen auf Basis der Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung (Bayern-PKI) ausgestellt wurden. Wenn die Zertifikate von einer anderen Zertifizierungsstelle i.S. von Nr. 4 Buchst. a, zweiter Spiegelstrich AFS-HKR vom 30.04.2019 (z.B. AKDB) ausgestellt werden, müssen die Verweise entsprechend angepasst werden. Anpassungsbedarf dürfte sich dann ggf. bei den grau hinterlegten Texten ergeben.

1. Allgemeines/Präambel

Die nachfolgende Dienstanweisung regelt die sichere und ordnungsgemäße Verwendung von fortgeschrittenen elektronischen Zertifikaten der Bayern-PKI und berücksichtigt die mit IMS vom 30.04.2019, Az.: B4-1512-4-17, veröffentlichten Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen- und Rechnungswesen der bayerischen Kommunen (AFS-HKR).

2. Geltungsbereich

Diese Dienstanweisung gilt für alle Zertifikatsnehmer/Signaturschlüsselinhaber der Gemeinde xxx, die nach den geltenden haushaltsrechtlichen Vorschriften mit fortgeschrittenen elektronischen Signaturen i.S. von § 87 Nr. 12 KommHV-Kameralistik/§ 98 Nr. 21 KommHV-Doppik die sachliche und rechnerische Richtigkeit von Ansprüchen oder Zahlungsverpflichtungen bescheinigen, Zahlungsanordnungen erteilen oder Tagesabschlüsse/Tagesabgleiche elektronisch unterzeichnen.

3. Zertifizierungsstelle

Für die Ausstellung fortgeschrittener elektronischer Zertifikate, die dem X.509-Standard entsprechen müssen, ist das IT-Dienstleistungszentrum (IT-DLZ) beim Bayerischen Landesamt für Digitalisierung, Breitband und Vermessung zuständig.

4. Registrierungsstelle

a. Zuständigkeit

Zuständige Registrierungsstelle für die Gemeinde xxx ist das Amt/Abteilung/Referat/Sachgebiet xxx.

b. Aufgaben und Pflichten

Der Registrierungsstelle obliegt insbesondere die Identifizierung und Registrierung von neuen Zertifikatsnehmern (PKI-Teilnehmern), der Widerruf oder die Sperrung von fortgeschrittenen Zertifikaten bei der Zertifizierungsstelle, die Kontrolle der in Nr. 7 beschriebenen Löschprozesse sowie die Pflege der eigenen Registrierungsstellen- und Behördendaten. Sie verfährt hierbei nach der geltenden Zertifizierungsrichtlinie der Public Key Infrastructure der Bayerischen Verwaltung (kurz: Zertifizierungsrichtlinie Bayern-PKI) und ist insbesondere für die zuverlässige Identifizierung des Zertifikatsnehmers, die Richtigkeit der bei der Antragstellung erfassten Daten und die Dokumentation der Antragsdaten verantwortlich.

c. Zusammenarbeit mit der zentralen IT-Stelle der Gemeinde

Die Zusammenarbeit der Registrierungsstelle mit der bei der Gemeinde xxx für den Einsatz und den Betrieb der IT verantwortlichen Stelle (zentrale IT-Stelle) richtet sich nach der IT-Dienstanweisung der Gemeinde xxx vom *[Datum]*. Insbesondere ist die zentrale IT-Stelle rechtzeitig über die Beantragung oder den Widerruf von Zertifikaten zu informieren.

5. Antragsverfahren

Das für den Betrieb der Fachanwendung/Signaturanwendungskomponente zuständige Amt/Abteilung/Referat/Sachgebiet xxx legt den Bedarf an fortgeschrittenen Zertifikaten fest und teilt dies der zuständigen Registrierungsstelle schriftlich mit. Die Registrierungsstelle stellt die zuverlässige Identifizierung der Zertifikatsnehmer, die korrekte Eingabe und Richtigkeit der Daten im Zertifikatsverwaltungssystem Nexus Prime sicher.

6. Rechte und Pflichten der Zertifikatsnehmer

a. Umfang der Nutzung

Das für fortgeschrittene Signaturen ausgestellte Zertifikat (Signaturzertifikat) darf nur zu dienstlichen Zwecken im Rahmen der dem Zertifikatsnehmer zugewiesenen Anordnungsbefugnis (§ 38 Abs. 2, § 39 Abs. 1 Satz 2 KommHV-Kameralistik/§ 34 Abs. 2, § 35 Abs. 1 Satz 2 KommHV-Doppik), Feststellungsbefugnis (§ 41 Abs. 1 Satz 2, Abs. 3 Satz 1 KommHV-Kameralistik/§ 37 Abs. 1 Satz 2, Abs. 3 Satz 1 KommHV-Doppik) oder Unterschriftsbefugnis für den Tagesabschluss/Tagesabgleich (§ 72 Abs. 1 Satz 2 KommHV-Kameralistik/§ 68 Abs. 1 Satz 3 KommHV-Doppik) zur elektronischen Unterzeichnung der vorstehend genannten Wissens- und Willenserklärungen verwendet werden. Nr. xxx der Dienstanweisung für das Finanz- und Kassenwesen der Gemeinde xxx findet entsprechende Anwendung.

b. Verbot der Weitergabe an andere Personen

Das Hard- oder Software-Token mit dem Signaturzertifikat und dem persönlichen Signaturschlüssel darf keiner anderen Person zugänglich gemacht oder überlassen werden.

c. Sichere Aufbewahrung der Zertifikate und Schutz des privaten Signaturschlüssels

Beim Einsatz von fortgeschrittenen Signaturen muss sichergestellt sein, dass der Unterzeichner die Signaturerstellungsdaten (Zertifikat, persönlicher und öffentlicher Signaturschlüssel) mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Aus diesem Grund muss gewährleistet sein, dass die Signaturerstellungsdaten, auch wenn sie z.B. lediglich als Software-Token im Format PKCS#12 vorliegen, weder unbefugt kopiert noch exportiert oder verwendet werden können (vgl. Art. 26 Buchst. c eIDAS-VO i.V. mit Nr. 10 Buchst. c und Anlage 3 Buchst. a AFS-HKR).

Der Zugriff auf den privaten und geheimen Signaturschlüssel muss daher stets gesichert (mittels Passwort) erfolgen. Das Passwort für die Nutzung des privaten Signaturschlüssels ist verantwortungsvoll zu wählen (Länge und Komplexität), darf nur dem jeweiligen Zertifikatsnehmer persönlich bekannt sein und muss geheim gehalten werden. Es muss vom Zertifikatsnehmer so aufbewahrt werden, dass auch andere Personen nicht darauf zugreifen können und darf daher nicht auf lokalen oder zentralen Rechnersystemen, programmierbaren Funktionstasten von Tastaturen oder Mäusen, in der Anwendungssoftware oder auf externen Speichermedien gespeichert werden. Dies gilt auch bei administrativen Tätigkeiten oder bei der Behebung von Störungen.

d. Anwendung der Komfortsignatur (Stapelsignatur)

Damit auch bei einer Komfort-/Stapelsignatur die Warn- und Hinweisfunktion der Unterschrift erhalten bleibt (vgl. Anlage 3 zur AFS-HKR, Buchst. a, fünfter Spiegelstrich), muss vor Auslösung des Signaturvorgangs gewährleistet sein, dass

- die Zahl der im Stapel signierten Kassenanordnungen für den Anwender überschaubar bleibt (max. 30 – 40 Anordnungen),
- dem Unterzeichner die zu signierenden Daten vollständig und leicht lesbar angezeigt werden (z.B. ausreichend großes Bildschirmfenster mit Scrollfunktion),
- sich die Stapelsignaturen nur auf die zuvor angezeigten Daten (Kassenanordnungen mit zahlungsbegründenden Unterlagen = Belegdokumente) beziehen.

Bei der Stapelsignatur von Zahlungsanordnungen sollten die hierfür vorgegebene Zeitspanne (max. 45 - 60 Min.) und die o.g. Anzahl von Anordnungen (entspricht rd. 90 - 120 Belegdokumenten) nicht überschritten werden. Die hierbei signierten Anordnungen sollten vom jeweiligen Unterschriftsbefugten mit der vorhandenen IT-Ausstattung noch gut überblickt werden können.

Nach Ablauf des vorgegebenen Zeitintervalls oder bei Überschreitung der zulässigen Anzahl von Belegen muss sichergestellt sein, dass eine weitere Stapelsignatur nur durch die erneute Eingabe des Signaturschlüssel-Passworts ausgelöst werden kann.

e. Verpflichtungen aus der Zertifizierungsrichtlinie

Im Übrigen muss der Zertifikatsnehmer die in der Zertifizierungsrichtlinie der Bayerischen Verwaltungs-PKI festgelegten persönlichen Melde- und Sorgfaltspflichten (vgl. insb. Abschn. 4.5, 4.7 und 4.9 der Zertifizierungsrichtlinie Bayern-PKI) beachten.

7. Anzeige und Prüfung von Signaturdaten

a. Aufgaben und Pflichten

Die zu signierenden Daten müssen sowohl dem Unterzeichner als auch den prüfenden Instanzen vollständig und richtig angezeigt werden (kurz: what you see is what you sign). Außerdem sollte bei jedem Signiervorgang automatisch die Gültigkeit des Zertifikats überprüft werden.

Auch bei Komfortsignaturen ist sicherzustellen, dass sich der Signierende die im Stapel bereitgestellten Signaturdaten (z.B. Kassenanordnungen samt zahlungsbegründender Unterlagen) erst vollständig anzeigen lassen muss, um seinen Kontroll- und Prüfpflichten im erforderlichen Umfang nachzukommen.

b. Einweisung der Zertifikatsnehmer

Der Zertifikatsnehmer und die Anordnungsbefugten müssen darin eingewiesen werden, wie sie die zu signierenden Daten kontrollieren und die Gültigkeit von elektronischen Signaturen schnell überprüfen können (z.B. Signaturstempel in PDF-Dokumenten).

c. Einweisung der Kontrollinstanzen

Die Beschäftigten der Kasse sowie die örtlichen und überörtlichen Rechnungsprüfungsorgane müssen in die für die Integritäts- und Signaturprüfung notwendigen Verfahren und Schritte eingewiesen werden, damit sie diese beiden Aspekte stichprobenweise untersuchen können (z.B. Signaturstempel in PDF-Dokumenten, manuelle Signaturprüfung im PDF-Viewer, elektronischen Rechnungsworkflow oder über den Data Pavonis Service der Governikus KG des Freistaats Bayern - vgl. https://sigtest.bayern.de/).

d. Vorrang von maschinellen Kontrollen

Grundsätzlich sollte die Integritäts- und Gültigkeitsprüfung von signierten Dokumenten vollautomatisch im Verfahren für das Haushalts-, Kassen- und Rechnungswesen (HKR-Verfahren) oder in der eingesetzten Workflow-Komponente sowie den für die Anzeige von Dokumenten verwendeten Viewern erfolgen. Das Ergebnis dieser Prüfung sollte dem Anwender auf einfache Weise angezeigt werden (z.B. Flag über erfolgreiche Signaturprüfung und Gültigkeit der elektronischen Signatur).

e. Statusabfrage und Zertifizierungspfade

Die Statusabfrage von Zertifikaten (z.B. Verteilpunkte-Sperrlisteninformationen oder Online OCSP-Abfrage) und die Online-Erreichbarkeit der in den Zertifizierungspfaden angegebenen Zertifizierungsstellen zur Prüfung der Gültigkeit und Anwendbarkeit des Signaturzertifikats (z.B. Zertifikatskette) sind zu gewährleisten. Die Wurzelzertifikate der Zertifizierungsstelle sind manuell zu importieren, wenn sonst nicht sichergestellt ist, dass die für den Zertifikatsnehmer ausgestellten und für die Signaturerstellung verwendeten Zertifikate als gültig erkannt werden.

8. Widerruf, Sperren und Löschen von Signaturzertifikaten

Ein Widerruf und das Sperren des Signaturzertifikats sind insbesondere erforderlich, wenn

- der persönliche (private) Signaturschlüssel verloren oder kompromittiert (z.B. ausgespähtes Passwort) wurde,
- der Verdacht besteht, dass die Signaturerstellungsdaten auch Unbefugten zugänglich sind (z.B. durch Kopie oder Schadsoftware),
- die bei der Signatur verwendeten Algorithmen oder Parameter (z.B. Schlüssellänge, Hash-Wert-Algorithmen) allgemein als unsicher gelten,
- dem Zertifikatsnehmer die Unterschriftsbefugnis entzogen wurde oder
- er aus anderen Gründen nicht mehr berechtigt ist, ein Signaturzertifikat zu besitzen (z.B. beim Wechsel der Stelle oder Ausscheiden des Zertifikatsnehmers aus dem Dienst- oder Arbeitsverhältnis).

Gleiches gilt, wenn die Angaben im Zertifikat nicht mehr gültig sind (z.B. Änderung des Namens).

Der zuständigen Registrierungsstelle sind die o.g. Gründe rechtzeitig mitzuteilen, damit sie die notwendigen technischen und organisatorischen Maßnahmen umgehend veranlassen kann.

Wegen der weiteren Widerrufs- und Sperrgründe wird auf die in Nr. 4.9.1 der Zertifizierungsrichtlinie der Bayern-PKI genannten Widerrufsgründe verwiesen.

Wenn trotz des umgehend veranlassten Widerrufs und der Sperrung des Zertifikats eine missbräuchliche Verwendung nicht ausgeschlossen werden kann, ist das Software-Token oder das in den Zertifikatsspeicher importierte Signaturzertifikat samt persönlichem Signaturschlüssel umgehend durch den Zertifikatsnehmer oder die zentrale IT-Stelle zu löschen und dies in geeigneter Weise zu dokumentieren.

9. Inkrafttreten

Diese Dienstanweisung tritt mit Wirkung vom *[Datum]* in Kraft.

Gemeinde xxx, den *[Datum]*

Unterschrift
Verwaltungsleitung