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

(Stand: 03.11.2022)

Allgemeines/Präambel

Die nachfolgende Dienstanweisung regelt die sichere und ordnungsmäßige 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).

Kommentiert [GH1]: Wichtiger Hinweis:
Oder einer anderen Zertifizierungsstelle (CA), die einen vergleichbar sicheren Betrieb des Vertrauensdienstes gewährleistet (vgl. Nr. 4 Buchst. a, zweiter Spiegelstrich AFS-HKR vom 30.04.2020)

1. 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.

2. 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.

Kommentiert [GH2]: Wichtiger Hinweis:
Oder ggf. andere Zertifizierungsstelle i.S. von Nr. 4 Buchst. a, zweiter Spiegelstrich AFS-HKR vom 30.04.2019 (z.B. AKDB)

3. 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.

Kommentiert [GH3]: Wichtiger Hinweis:
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, muss an dieser Stelle auf die Zertifizierungsrichtlinie dieser CA verwiesen werden

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.

4. 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.

Kommentiert [GH4]: Wichtiger Hinweis:
Ist statt dem IT-DLZ des Freistaats Bayern eine andere Zertifizierungsstelle zuständig (z.B. AKDB), ist dieser Text entsprechend anzupassen

5. 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.

Kommentiert [GH5]: Wichtiger Hinweis:
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. Sie sollte vom jeweiligen Unterschriftsbefugten mit der vorhandenen IT-Ausstattung noch gut überblickt werden können. In dem vorgegebenen Zeitintervall sind bereits auch kürzere Unterbrechungen berücksichtigt.

Kommentiert [GH6]: Wichtiger Hinweis:
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)

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.

6. 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.

7. 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.

Kommentiert [GH7]: Wichtiger Hinweis:
Bei einer anderen Zertifizierungsstelle ist an dieser Stelle auf deren Zertifizierungsrichtlinie zu verweisen

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.

8. Inkrafttreten

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

Gemeinde xxx, den *[Datum]*

Unterschrift
Verwaltungsleitung