

Dienstanweisung

zum Einsatz von elektronischen Signaturen im Landratsamt (Dienstanweisung elektronische Signaturen)

des

Landratsamtes Unstrut-Hainich-Kreis

- Der Landrat –



Dienstanweisung Nr.:	05/2021
Stand:	15.12.2021
Änderungen:	
Version:	
Verteiler:	An alle Mitarbeiter/-innen des Landratsamtes Unstrut-Hainich- Kreis

Präambel

Die elektronische Abwicklung von Verwaltungsdienstleistungen nimmt permanent zu. Dabei besteht immer häufiger die Zielstellung bzw. die gesetzliche Anforderung, für den Bürger die Möglichkeit der vollständig medienbruchfreien Realisierung dieser Leistungen in digitaler Form zu schaffen. Hierzu bedarf es innerhalb der Behörde in verstärktem Maße des Einsatzes von elektronischen Signaturen, welche die bisherige schriftliche Unterschrift ersetzen und eine eindeutige persönliche Identifikation der Bediensteten ermöglichen.

Diese Dienstanweisung verfolgt den Zweck, grundlegende Festlegungen für einen rechtssicheren Einsatz von elektronischen Signaturen im Landratsamt zu treffen.

Die Entscheidung über den tatsächlichen Einsatz einer elektronischen Signatur erfolgt separat im fortschreitenden Ausbau der elektronischen Kommunikation je nach den Aufgabenstellungen und Erfordernissen am einzelnen Arbeitsplatz.

Inhaltsverzeichnis:

1. Begriffsbestimmungen, Definition
2. Stammzertifizierungsstelle des Landratsamtes
3. Antragsverfahren für elektronische Zertifikate
4. Rechte und Pflichten der Zertifikatsinhaber
5. Bestandsverzeichnis über ausgestellte elektronische Zertifikate
6. Geltung, Inkrafttreten

1. Begriff der elektronischen Signatur

Unter einer elektronischen Signatur versteht man mit elektronischen Informationen - i. d. R. sind dies elektronische Dokumente - verknüpfte Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann. Die elektronische Signatur erfüllt hierbei den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten.

Elektronische Signaturen können überall dort eingesetzt werden, wo bei herkömmlichen Verwaltungsverfahren bislang die Schriftform bzw. Unterschrift gefordert war. Gemäß Thüringer Verwaltungsverfahrensgesetz kann die Schriftform durch ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur versehen ist, ersetzt werden. Dabei hat die qualifizierte elektronische Signatur nach Zivilprozessordnung uneingeschränkte Beweiskraft vor Gericht.

Sofern es durch Rechtsvorschrift zugelassen ist, können auch fortgeschrittene elektronische Signaturen oder andere geeignete und sichere Verfahren die Schriftform ersetzen.

2. Arten von elektronischen Signaturen

2.1 Einfache elektronische Signatur

Eine einfache elektronische Signatur ist in Form und Inhalt an keine strengen gesetzlichen Regeln oder abschließende Vorgaben gebunden. Ihr Zweck ist es, den Urheber einer Mitteilung oder Nachricht kenntlich zu machen, z. B. nach Vorgaben der Dienststellenleitung. Die einfache elektronische Signatur findet Anwendung im hausinternen Schriftverkehr. Sie hat bei juristischen Streitfällen unter Umständen keine bzw. eine nur geringe Beweiskraft.

2.2 Fortgeschrittene elektronische Signatur

Eine fortgeschrittene elektronische Signatur ist eine elektronische Signatur, die es ermöglicht, die Authentizität und Unverfälschtheit der jeweils signierten Daten zu prüfen.

Als grundlegende Anforderung an eine fortgeschrittene elektronische Signaturen gilt, dass

- sie eindeutig dem Unterzeichner zugeordnet ist,
- sie die Identifizierung des Unterzeichners ermöglicht,
- unter Verwendung elektronischer Signaturerstellungsdaten erzeugt wird, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann und
- sie mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

2.3 Qualifizierte elektronische Signatur

Eine qualifizierte elektronische Signatur kann durch Verwendung eines qualifizierten Zertifikats erzeugt werden. Das qualifizierte Zertifikat wird durch hierfür autorisierte Trustcenter d.h. zertifizierte Vertrauensdienste-Anbieter vergeben. Sofern ein elektronisches Dokument qualifiziert elektronisch signiert wird, hat dies im Rechtsverkehr dieselbe Wirkung, als wäre das Dokument mit einer handschriftlichen Unterschrift versehen worden. Die qualifizierte elektronische Signatur ermöglicht es, die Identität des Gegenübers und die Integrität der Inhalte zweifelsfrei festzustellen.

Jede mit einem qualifizierten Zertifikat erzeugte elektronische Signatur wird direkt der Person des Zertifikatinhabers zugeordnet. Daher gelten für die Beantragung, die Aufbewahrung und den Umgang mit qualifizierten Zertifikaten und qualifizierten elektronischen Signaturen besonders hohe rechtliche und technisch-organisatorische Anforderungen.

3. Stammzertifizierungsstelle des Landratsamtes

3.1. Zur Erzeugung von einfachen elektronischen Zertifikaten betreibt das Landratsamt in seiner Infrastruktur eine eigene Stammzertifizierungsstelle.

3.2. Die Stammzertifizierungsstelle des Landratsamtes wird durch den Fachdienst IT betrieben.

3.3. Folgende Festlegungen werden für den Betrieb der eigenen Stammzertifizierungsstelle getroffen:

- Die Zertifikate der Stammzertifizierungsstelle des Landratsamtes werden mit einer maximalen Gültigkeit von 5 Jahren ausgestellt.
- Die Zertifikatsdateien sind an das Benutzerkonto des jeweiligen Bediensteten gebunden und werden dort im dedizierten Benutzerzertifikatsspeicher abgelegt.

- Die von der Stammzertifizierungsstelle erzeugten Zertifikate gelten innerhalb aller Dienststellen der gesamten Behörde als vertrauenswürdig.
- Die Zertifikate der eigenen Stammzertifizierungsstelle sind ausschließlich im Rahmen innerbehördlicher Abläufe wirksam (keine Außenwirkung).
- Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass für die mit einfachen Zertifikaten der eigenen Stammzertifizierungsstelle erzeugten Signaturen ein durchgängig praktiziertes substanzielles Vertrauensniveau gegeben ist.

4. Antragsverfahren für elektronische Zertifikate

4.1 Erhalt der einfachen elektronischen Signaturen

Die einfachen elektronischen Signaturen werden durch den Fachdienst IT jedem Mitarbeiter automatisiert – ohne Antragstellung - zur Verfügung gestellt zur verpflichtenden Verwendung bei

- Abzeichnung bzw. Mitzeichnung bei jeweils hausinternen Vermerken, Verfügungen, Formularen, Protokollen
- Unterzeichnung hausinterner personalrechtlicher Anträge

4.2 Beantragung fortgeschrittener elektronischer Zertifikate

Die Beantragung fortgeschrittener elektronischer Zertifikate erfolgt beim Fachdienst IT durch schriftliche Anforderung des jeweiligen unmittelbaren Vorgesetzten unter Darlegung von Person, Nutzungserfordernis und -umfang nach dem Formblatt gemäß Anlage.

4.3 Beantragung qualifizierter elektronischer Zertifikate

Die Beantragung qualifizierter elektronischer Zertifikate erfolgt in Eigenverantwortung des jeweiligen Fachdienstes. Der Fachdienst IT unterstützt bei Problemen im Beantragungsprozess.

Das qualifizierte Zertifikat soll ein Attribut im Sinne des Vertrauensdienstegesetzes enthalten, das explizit auf die Zugehörigkeit des Signaturinhabers zum Landratsamt verweist.

4.4 Änderungsanzeige für vorhandene elektronische Zertifikate

Sofern sich persönliche oder dienstliche Veränderungen bei der Person des Zertifikatsinhabers ergeben, die Auswirkung auf die Wirksamkeit oder Geltung eines elektronischen Zertifikats haben, werden diese im Rahmen der Mitarbeiterdatenveränderungsmitteilung im Intranet den zuständigen Stellen mitgeteilt.

Sofern Bedienstete aus dem aktiven Arbeits- oder Dienstverhältnis mit dem Landratsamt ausscheiden, erlischt in diesem Zuge die Gültigkeit etwaiger vorhandener Zertifikate.

5. Rechte und Pflichten der Zertifikatsinhaber

5.1 Nutzungsumfang der Zertifikate

Elektronische Zertifikate dürfen durch die jeweiligen Bediensteten ausschließlich zu dienstlichen Zwecken im Rahmen der übertragenen Aufgaben verwendet werden.

5.2 Sicherer Umgang mit den elektronischen Zertifikaten

Das Medium mit dem hinterlegten qualifizierten Zertifikat (i. d. R. Signaturkarte des Trust-centers) ist stets in persönlichen Gewahrsam zu nehmen.

Zertifikatsdatei und PIN sind ausschließlich im persönlichen Zugriffsbereich zu führen bzw. zu speichern; die PIN darf nur dem Zertifikatsinhaber bekannt sein.

Eine Weitergabe oder Überlassung dienstlicher elektronischer Zertifikate bzw. der PIN an Dritte ist untersagt. Die Geheimhaltung gegenüber Dritten ist auch bei der Verrichtung der Arbeitsvorgänge (z. B. Dateneingabe) zu beachten.

Die konkrete Definition der Anforderungen an die PIN (Länge, Groß-/ Kleinschreibung, Sonderzeichen, Anwendungsbefristung, Nutzungsdauer etc.) obliegt dem Fachdienst IT i. V. m. dem IT-Sicherheitsbeauftragten des Hauses.

6. Verlust, Widerruf, Sperrung, Vernichtung

6.1 Der Verlust eines qualifizierten Signaturzertifikats ist unverzüglich dem beantragenden Fachdienst anzuzeigen. Dieser veranlasst den sofortigen Widerruf des Zertifikats beim zertifizierten Vertrauensdienste-Anbieter, ggf. unter Mitwirkung des Zertifikatsinhabers.

6.2 Bei Kenntnis oder Verdacht einer Manipulation durch Dritte ist unverzüglich ein Widerruf des qualifizierten Signaturzertifikats bzw. eine Sperrung des fortgeschrittenen Signaturzertifikats oder der PIN vorzunehmen.

6.3 Der Verlust des fortgeschrittenen Signaturzertifikats (z. B. durch Löschung) ist unverzüglich dem Fachdienst IT anzuzeigen. Dieser veranlasst die sofortige Sperrung des Zertifikats, ggf. unter Mitwirkung des Zertifikatsinhabers.

6.4 Ein Medium mit einem nicht mehr benötigten Zertifikat ist unverzüglich dem Fachdienst IT zu übergeben. Nicht mehr benötigte qualifizierte Zertifikate sind durch den Fachdienst IT mittels physischer Zerstörung unbrauchbar zu machen.

6.5 Über sicherheitsrelevante Vorfälle im Zusammenhang mit der Nutzung von elektronischen Zertifikaten ist der IT-Sicherheitsbeauftragte des Landratsamtes unverzüglich zu informieren.

7. Nachprüfbarkeit der Signaturen; langfristige Beweiserhaltung der Daten

Es ist sicherzustellen, dass elektronische Signaturen mindestens während der Dauer der Aufbewahrungsfristen nachprüfbar sind.

8. Bestandsverzeichnis über ausgestellte elektronische Zertifikate

Im Rahmen des Zertifikatsmanagements führt der Fachdienst IT ein Bestandsverzeichnis über ausgestellte qualifizierte elektronische Zertifikate sowie über ausgestellte fortgeschrittene Zertifikate.

9. Geltung, Inkrafttreten

9.1 Diese Dienstanweisung ist allen Bediensteten des Landratsamtes zur Kenntnis zu geben.

9.2 Die Dienstanweisung tritt am 01.01.2022 in Kraft. Gleichzeitig tritt die Dienstanweisung

zur Regelung der internen Verfahrensweise bei der Verfahrensabwicklung mit qualifizierter elektronischer Signatur (DA 01/2011) außer Kraft.

- 9.3** Personenbezogene Funktionsbezeichnungen in dieser Dienstanweisung gelten jeweils für alle Geschlechtsformen.

Anlage: Formblatt Beantragung elektronischer Zertifikate

Zanker
Landrat

Mühlhausen, den 16.12.2021

Beantragung elektronischer Zertifikate

☐

Neuantrag für ein elektronisches Zertifikat

☐

Änderungsantrag für ein bereits vorhandenes elektronisches Zertifikat



1. Beantragende Organisationseinheit:

Fachbereich:

Fachdienst / Einrichtung:

Zuständige Führungskraft:

2. Beantragtes bzw. zu änderndes Zertifikat:

☐

fortgeschrittenes elektronisches Zertifikat

☐

qualifiziertes elektronisches Zertifikat

☐

beantragen
(weiter mit Punkt 3.)

☐

ändern
(weiter mit Punkt 4.)

3. Nutzungserfordernis / -umfang für ein elektronisches Zertifikat:

Zertifikatsinhaber (Name, Vorname)

Nutzungserfordernis / -umfang

4. Änderungsanzeige für vorhandenes elektronisches Zertifikat:

Zertifikatsinhaber (Name, Vorname)

Darlegung der Änderung/en (Erläuterung / Begründung)

Datum

Unterschrift / Signatur der zuständigen Führungskraft