Beweiswerterhaltung von Signaturen

vom Arbeitskreis Elektronische Signatur, Mai 2022

Verweise auf andere Verfahren z. B. BeBPo oder De-mail

Für den Ersatz einer Schriftform können im Verwaltungsverfahren, anstelle qualifizierter elektronischer Signaturen, verschiedene andere Verfahren für spezifische Zecke eingesetzt werden.

So listet das Verwaltungsverfahrensgesetz NRW für den Ersatz einer gesetzlich geforderten Schriftform in § 3a sinngemäß folgende Alternativen auf:

1. Unmittelbare Abgabe einer Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird. Wobei bei der Nutzung über öffentlich zugängliche Netze die Identifikation des Absendenden durch die eID-Funktion des Personalausweises erfolgen muss.

2. Versand von Anträgen und Anzeigen als elektronisches Dokument an die Behörde, wobei eine sichere Anmeldung am De-Mail-Konto erforderlich ist.

3. Versand von elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden als eine De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Dienstanbieters die erlassende Behörde als Nutzer des DE-Mail-Kontos erkennen lässt.

4. Sonstige sichere Verfahren, die durch Rechtsverordnung im Sinne von § 3a Absatz 2 Satz 4 Nummer 4 des Verwaltungsverfahrensgesetzes festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten.

Bei Schreiben entsprechend 2. oder 3. werden qualifizierte elektronische Signaturen des De-Mail-Providers eingesetzt, die bestätigen, dass das Dokument von dem sicher authentifizierten Absender stammt und auf dem Zustellweg durch das Netz der De-Mail-Provider zwischen Einlieferung und Zustellung nicht verändert wurde.

Gibt es Ablauf- oder Gültigkeitsfristen?

Qualifizierte elektronische Signaturen werden mit einem Zertifikat erstellt, welches seitens der ausgebenden Stelle (certification authority) mit einer zeitlich begrenzten Gültigkeit versehen wurde.

Ablauf der Zertifikate

Die in einem Signaturzertifikat hinterlegte Gültigkeit definiert, zwischen welchem Beginn- und Enddatum mit diesem Zertifikat Signaturen erstellt werden dürfen. Zugelassene Signatursoftwareprodukte interpretieren diese Daten so, dass nur in diesem Zeitraum mit den Signaturzertifikaten Signaturen erzeugt werden können. Vor oder nach diesem Zeitpunkt verweigert die Software die Signatur.

Wird innerhalb dieses Zeitraums mit einem solchen Signaturzertifikat eine Signatur erzeugt, ist diese auch nach Ablauf des Gültigkeitseitraumes weiterhin gültig, da die Signatur zum Zeitpunkt der Erstellung gültig war.

Fälschungssicherheit der mathematischen Algorithmen

So lange die verwendeten Signaturalgorithmen selbst nicht als unsicher/fälschbar gesperrt wurden, werden die erzeugten Signaturen auch als nicht fälschbar angesehen und sind weiterhin gültig. Um zu vermeiden, dass unsichere Signaturalgorithmen verwendet werden, werden diese regelmäßig durch eine internationale Expertenkommission geprüft und für weiterhin verwendbar oder aber ab einem bestimmten Zeitpunkt als nicht mehr verwendbar erklärt. Hierzu gibt es den sogenannten SOG-IS-Kryptokatalog.[1]

Übersignieren - revisionssichere Speicherung

Um zu vermeiden, dass nicht mehr nachweisbar ist, ob ein Dokument gefälscht wurde, müssen Dokumente vor Sperrung eines Signaturalgorithmus erneut mit einem sicheren Signaturalgorithmus übersigniert werden. Dies erfolgt in der Regel über geeignete Softwareprodukte automatisch mittels fortgeschrittener Signaturzertifikate und der Abspeicherung der Nachweiskette in sogenannten

[1] https://www.elektronische-vertrauensdienste.de/EVD/SharedDocuments/Downloads/QES/Algorithmen/Empfehlungen2018.pdf?__blob=publicationFile&v=1

evidence records, die zusammen mit einem Dokument oder in einer hierfür aufgebauten Datenbank gespeichert werden.

TR-ESOR

Seitens des BSI wurde mit der Richtlinie TR 03125 *„Beweiswerterhaltung kryptografisch signierter Dokumente (TR-ESOR)“* eine mögliche Umsetzung für eine beweiswerterhaltende Speicherung von kryptografisch signierten Dokumenten vorgestellt. Diese stellt nicht die einzige mögliche Umsetzung eines solchen Konzeptes dar, erleichtert aber die Argumentation, dass eine beweiswerterhaltende Aufbewahrung erfolgt ist.

Schnittstelle zur Elektronischen Akte

Für den Nachweis einer beweiswerterhaltenden elektronischen Speicherung eines Dokumentes empfiehlt sich das Führen einer Verfahrensdokumentation (siehe z.B. GOBD).

Werden in einer elektronischen Akte Dokumente mit einer qualifizierten elektronischen Signatur gespeichert, sind bei Abgabe einer solchen elektronischen Akte zur Akteneinsicht durch die Justiz die Nachweise der durchgängigen Beweiswerterhaltung beizufügen. Der Nachweis der Unverfälschtheit obliegt jedoch dem Empfänger und nicht der abgebenden Behörde.