LANDESHAUPTSTADT SCHWERIN

Qualifizierte elektronische Signatur für Nutzer

Datum: 18. September 2019

Verfasser: Ulf Nörenberg

FD/FB: 10/10.4

Inhaltsverzeichnis

Vorbemerkung

In Zeiten der papierlosen und damit meist elektronischen Vorgangsbearbeitung entsteht bei der Mitzeichnung eines Dokuments ein Problem. Die frühere eigenhändige Unterschrift des Unterzeichners lässt sich auf ein elektronisches Dokument nicht mehr ohne weiteres anbringen. Ausdrucken, Unterschreiben und wieder Einscannen ist keine Lösung, da so die elektronische Bearbeitung ad absurdum geführt wird.

Auch das Eintippen des Namens oder das Einfügen eines Faksimiles der Unterschrift des Unterzeichners löst das Problem nicht, da das elektronische Dokument danach noch beliebig geändert werden kann und nicht mehr dem entspricht, was der Unterzeichner seinerzeit unterzeichnet hat. Diese Änderung ist, im Gegensatz zur alten Papier-Tinte-Form, später nicht mehr erkennbar und ein Nachweis der nachträgliche Änderung bzw. Fälschung unmöglich.

Es wird für das Unterschreiben eines elektronischen Dokuments eine andere Technologie benötigt als das althergebrachte Anbringen eines Schriftzuges der Unterschrift an dem Dokument. Diese Technologie ist die sogenannte elektronische Signatur.

Prinzip der elektronischen Signatur

Bei der elektronischen Signatur wird einem elektronischem Dokument eine eindeutige Bestätigung angehängt, mit der der Nachweis erbracht werden kann, dass

- einer bestimmte Person
- zu einem bestimmten Zeitpunkt
- ein bestimmter Dokumenteninhalt

vorgelegen hat.

Eine nachträgliche Änderung des Dokumenteninhalts ist bei einer Prüfung der Signatur erkennbar. Unter bestimmten Voraussetzungen ersetzt die elektronische Signatur die eigenhändige Unterschrift. So heißt es z.B. in § 126 a Absatz 1 im Bürgerlichen Gesetzbuch „*Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen.*“

Technischer Ablauf

Im Gegensatz zur Papierform kann eine Signatur nicht einfach auf ein Dokument aufgebracht werden. Es handelt sich um digitale Daten, die beliebig oft kopiert und geändert werden, und somit auch nach Anbringen der Signatur geändert werden können.

Bei einer digitalen Signatur wird zunächst eine Quersumme des Dokuments gebildet. Dabei handelt es sich um eine Zeichenkette, die eindeutig zum Inhalt des Dokuments passt. Wird nur ein Buchstabe im Dokumententext verändert, so ergibt dies eine völlig andere Quersumme.

Die gebildete Quersumme wird mit dem Zertifikat verschlüsselt und zusammen mit Datum und Uhrzeit dem Dokument angehängt. Bei einer Prüfung wird wieder die Quersumme des Dokuments gebildet und die verschlüsselte Quersumme mit dem Schlüssel des Zertifikatsinhabers (nur mit

diesem ist eine Entschlüsselung möglich!!) entschlüsselt. Sind die beiden Quersummen gleich, so ist das Dokument mit genau diesem Inhalt vom Zertifikatsinhaber unterzeichnet worden.

Unterscheiden sich beide Quersummen, so ist das mitgelieferte Dokument nicht das, was dem Zertifikatsinhaber seinerzeit vorgelegen hat. Es ist ggf. auch nachträglich geändert worden.

Arten der elektronischen Signatur

Einfache Signatur

Die einfache Signatur besteht aus Daten, die dem Dokument hinzugefügt werden. Dies kann der Name des Unterzeichners oder auch eine gescannte Unterschrift sein. Der Beweiswert ist gering.

Fortgeschrittene Signatur

Bei der fortgeschrittenen Signatur lässt sich die Signatur einer Person zuordnen. Die Daten werden verschlüsselt und nur eine Person hat die dafür benötigten Schlüssel in seinem Besitz. Da die Person aber nicht identifizierbar sein muss, ist der Beweiswert zwar höher als bei der einfachen Signatur, sie ersetzt aber nicht die gesetzliche Schriftform und kann daher vor Gericht nur als Indiz gewertet werden.

Qualifizierte Signatur

Die qualifizierte Signatur erweitert die fortgeschrittene Signatur um eine eindeutige Identifizierung des Schlüsselinhabers durch Ausstellung eines Zertifikates durch einen staatlich zugelassenen Zertifizierungsdiensteanbieter. Letzterer überprüft die Identität des Antragstellers und bestätigt (wieder durch eine digitale Signatur) die Zugehörigkeit eines Schlüssels zu der Person des Antragstellers. Weiterhin muss eine qualifizierte Signatur durch ein Signatursystem erfolgen, welches nicht manipulierbar ist. Hierbei handelt es sich meist um eine Chipkarte mit dem Schlüssel (wird vom Zertifizierungsdiensteanbieter erstellt und an die Person übergeben) sowie um einen Kartenleser. Die Signierung eines Dokumentes erfolgt dann auf dem Kartenleser und mit der Chipkarte. Nur wenn diese Voraussetzungen gegeben sind, ist eine elektronische Signatur eine qualifizierte Signatur und ersetzt die Schriftform.

Voraussetzungen für die Nutzung der qualifizierten elektronischen Signatur

Soll die qualifizierte elektronische Signatur (Abkürzung: qeS) im Geschäftsleben genutzt werden, so sind drei Dinge Voraussetzung:

1. eine Chipkarte mit dem Zertifikat des Ausstellers
2. ein Kartenleser
3. Signatursoftware

Chipkarte

Die Chipkarten bzw. Signaturkarten müssen bei einem zugelassenen Vertrauensdiensteanbieter beantragt werden. Dabei ist die Identität des Antragstellers nachzuweisen. Das Verfahren hierfür legt der Anbieter fest. Die Signaturkarten gibt es für Gültigkeitszeiträume von 1 – 5 Jahren. Nach den Gültigkeitszeiträumen richtet sich auch der Preis für die Signaturkarten. Diese liegen etwa zwischen 100 und 200 Euro für den gesamten Zeitraum. Nach Ablauf der Gültigkeit gibt es meist eine günstigere Verlängerungskarte.

Das Zertifikat ist mit einer PIN gesichert. Erst nach Eingabe dieser PIN gewährt die Chipkarte Zugriff auf das Zertifikat.

Die Kosten werden für den Betrieb der Zertifikatserstellung und -verwaltung erhoben. Da diese Zertifikate sehr sensible Daten sind, deren Missbrauch schwere rechtliche Folgen haben kann, sind die technischen und Sicherheitsanforderungen an die Vertrauensdiensteanbieter sehr hoch, was zu entsprechenden Betriebskosten führt, die an die Antragssteller weitergegeben werden müssen.

Eine Liste der in Deutschland zugelassenen Vertrauensdiensteanbieter finden Sie hier:

https://www.bundesnetzagentur.de/DE/Service-Funktionen/ElektronischeVertrauensdienste/QualifizierteVD/QualifizierteSignatur/Anbieterliste/AnbieterliseQeSignatur_node.html

Beispiel einer Signaturkarte der Bundesdruckerei

Kartenleser

Um Signaturen für ein Dokument zu erstellen wird ein Kartenleser benötigt. Mit diesem wird auf das Zertifikat der Signaturkarte zugegriffen und die Signatur auf dem Dokument erzeugt.

Kartenleser sollten der Klasse 3 angehören. Dies bedeutet, der Kartenleser verfügt über ein eigenes Display sowie eine eigene numerische Tastatur. Dies ist eine wichtige Sicherheitseingenschaft, da so die Eingabe der PIN nicht von anderen Programmen (sog. Keylogger) abgefangen werden kann.

Kartenleser gibt es von verschiedenen Herstellern, wie z.B. Reiner-SCT, Cherry oder SCM. In Deutschland weit verbreitet ist Reiner-SCT.

Kartenleser Cherry

Kartenleser Reiner-SCT

Signatursoftware

Die Signatursoftware hat zwei Aufgaben. Es kann eine Signatur für ein ausgewähltes Dokument erzeugt sowie die Signatur eines bereits signierten Dokumentes geprüft werden. Die Software greift über den angeschlossenen Kartenleser auf die Signaturkarte zu.

Signatursoftware gibt von verschiedenen Herstellen mit unterschiedlichen Funktionen.

Governikus Signer	https://www.governikus.de/sichere-daten/governikus-signer/
SecSigner	https://seccommerce.com/secsigner/
DigiSeal office	https://www.secrypt.de/produkte/digiseal-office/
Intarsys Sign Live CC	http://shop.intarsys.com/epages/78339456.sf/de_DE/?ObjectPath=/Shops/78339456/Categories/Signatursoftware
OpenLimit CC Sign	https://www.chipkartenleser-shop.de/openlimit

Aufzählung nur als Beispiel. Kein Anspruch auf Vollständigkeit

Anwendung der Signatur

Die Anbringung der Signatur kann auf zwei Arten erfolgen:

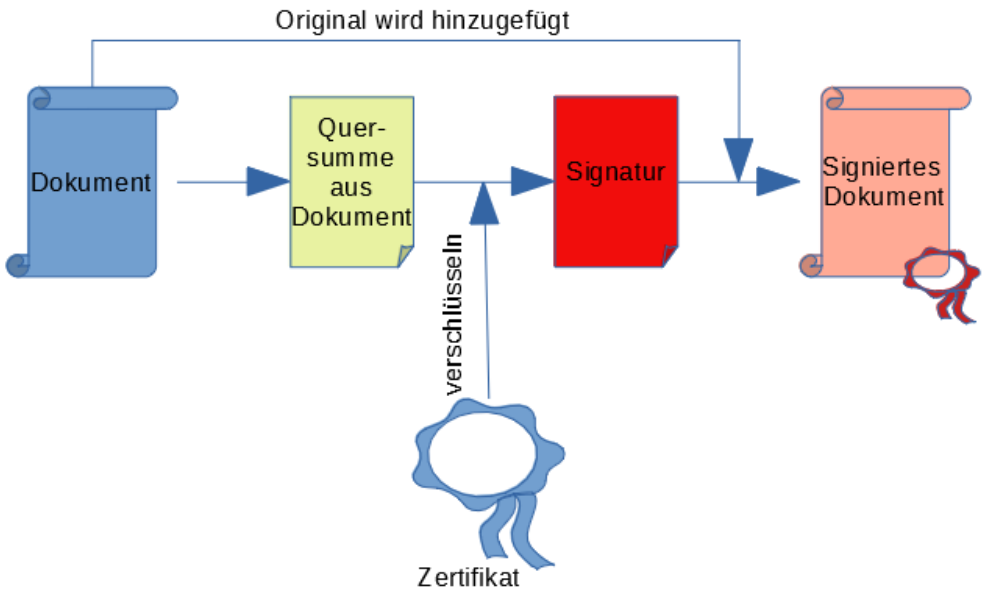
a) Einbettung der Signatur im zu signierenden Dokument. In diesem Fall wird das Dokument samt Signatur neu erzeugt. Das nicht signierte Dokument existiert neben dem signierten Dokument. Es braucht nur die signierte Datei weitergegeben zu werden.

b) Separate Signatur als eigene Datei. Dabei wird nur die Signatur in einer eigenen Datei (ohne das signierte Dokument) abgelegt. Bei dieser Variante ist sowohl das (unsignierte) Originaldokument UND Datei mit der Signatur weiterzugeben. I.d.R. hat die Signaturdatei die Endung „.pk7“.

Signieren eines Dokuments

Die Signierung eines Dokuments läuft nach folgendem Schema ab:

1. Start der Signatursoftware
2. Auswahl des zu signierenden Dokumentes und Öffnen bzw. Verschieben in die Signatursoftware
3. Prüfung des Zugriffs auf Kartenleser und Vorhandensein einer Signaturkarte
4. Anzeige des Inhalts des Dokuments zur Prüfung
5. Start des Signaturvorgangs durch Abfrage der PIN der Chipkarten
6. Signatursoftware erzeugt die Signatur und bettet sie in das Dokument ein bzw. erzeugt eine separate Signatur-Datei
7. Kontrolle des Dokuments inkl. eingebettete Signatur durch Anzeige des Inhalts.



Ablauf einer Signaturerstellung

Prüfen eines signierten Dokumentes

Der Empfänger eines signierten Dokuments wird die Signatur irgendwann prüfen wollen. Dabei werden zwei Prüfschritte unterschieden:

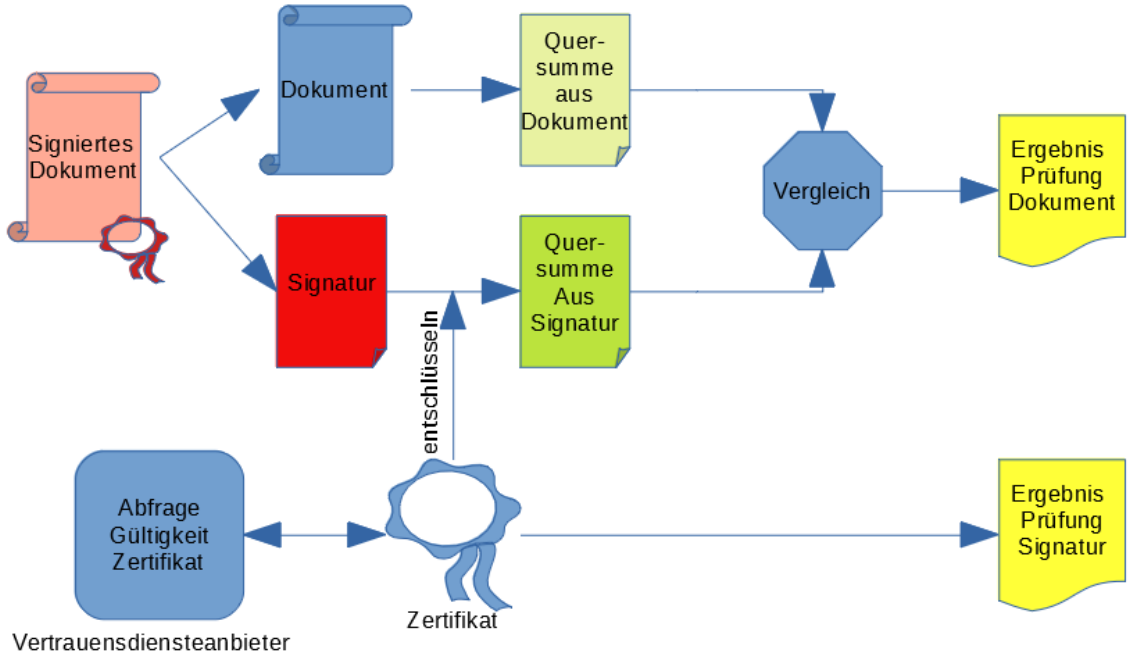
a) Prüfung auf nachträgliche Veränderung des Dokuments

b) Prüfung der Gültigkeit des Zertifikats der Signatur

Bei der Prüfung des Zertifikats ist eine Internetverbindung zum Vertrauensdiensteanbieter erforderlich, um die Gültigkeit des Zertifikats dort abzufragen. Wurde das Zertifikat gesperrt oder ist abgelaufen, so wird die Prüfung negativ ausfallen. Eine Prüfung auf Veränderung des Dokuments ist auch ohne Internetverbindung möglich.

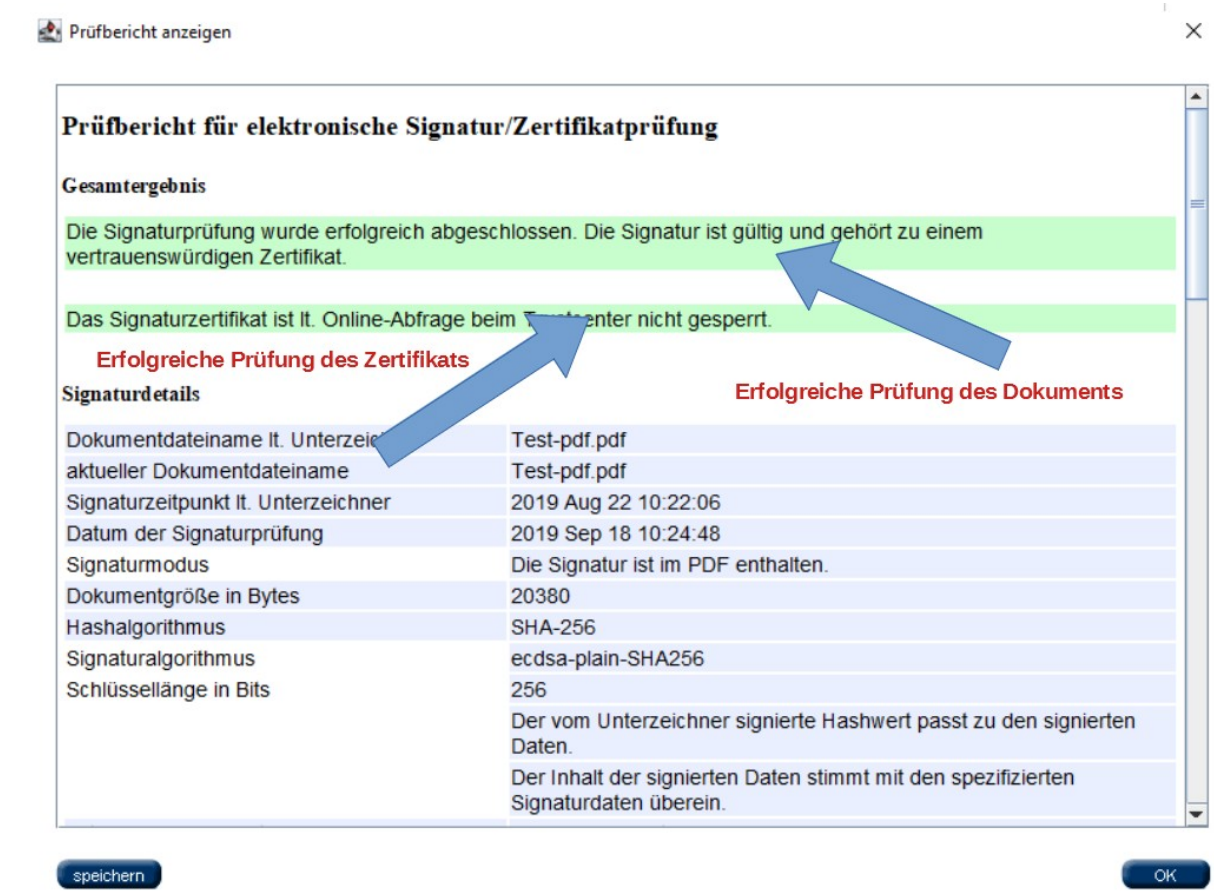
Die Prüfung erfolgt nach folgendem Schema:

1. Start der Signatursoftware
2. Auswahl des signierten Dokuments und Öffnen bzw. Verschieben in die Signatursoftware. Bei separater Signaturdatei müssen bei der Prüfung sowohl das Originaldokument als auch die separate Signaturdatei vorliegen und in der Signatursoftware geöffnet werden.
3. Prüfung auf Veränderungen am Dokument und Anzeige des Ergebnisses
4. ggf. Prüfung des Zertifikats und Anzeige des Ergebnisses.



Prüfung einer Signatur

Bei den meisten Signatursoftwareprodukten kann ein Prüfprotokoll angezeigt und/oder ausgedruckt werden, um die Echtheit der Signatur belegen zu können.



Beispiel eines Prüfprotokolls

Weitere Informationen

https://www.bundesnetzagentur.de/DE/Service-Funktionen/ElektronischeVertrauensdienste/QualifizierteVD/QualifizierteSignatur/QualZertifikateSignatur_node.html

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeSignatur/elektronischesignatur_node.html

https://www.pc-magazin.de/ratgeber/digitale-unterschrift-elektronische-signatur-3200650.html