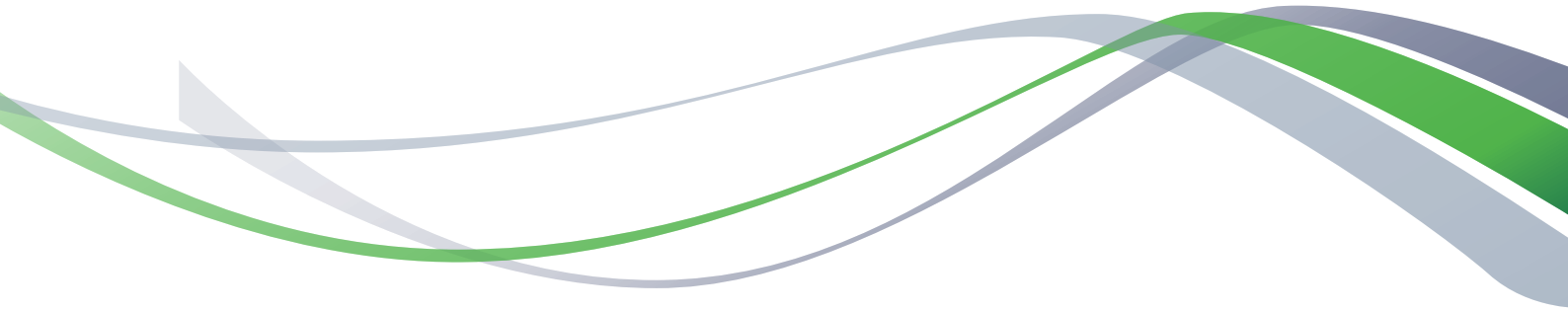
BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Elektronische Signaturen

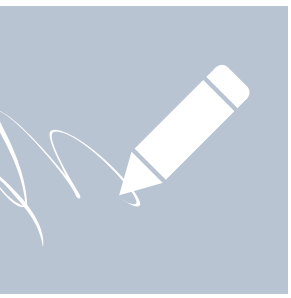


Was Sie vor dem Start wissen müssen

Sehr geehrter Anwender,
sehr geehrte Anwenderin,

mit Ihrer Entscheidung für die elektronische Signatur der Bundesnotarkammer, die den Anforderungen der eIDAS-Verordnung sowie des Vertrauensdienstegesetzes entspricht, haben Sie eine Entscheidung für die Zukunft getroffen. Damit Sie alle Vorteile der elektronischen Signatur nutzen können, finden Sie in dieser Broschüre Informationen rund um die elektronische Signatur und Ihr Signaturzertifikat. Die Broschüre erklärt auch, was Sie als Inhaber eines Signaturzertifikats zu beachten haben. Bitte lesen Sie daher diese Informationen aufmerksam durch. Ihr Signaturzertifikat wird Ihnen zur Verfügung gestellt, wenn Sie vorher durch Ihre Unterschrift oder per Mausklick im Rahmen des Online-Antrages bestätigen, die vorliegenden Informationen zur Kenntnis genommen zu haben.

Inhaltsverzeichnis



1. Was ist eine elektronische Signatur?

Eine elektronische Signatur sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet (Art. 3 Nr. 10 eIDAS-Verordnung).

Die eIDAS-Verordnung unterscheidet zwischen zwei Arten von elektronischen Signaturen:

- die fortgeschrittene elektronische Signatur sowie
- die qualifizierte elektronische Signatur.

Diese unterscheiden sich in den an sie gestellten rechtlichen Anforderungen.

Eine fortgeschrittene elektronische Signatur ist eine elektronische Signatur, die die Anforderungen des Art. 26 eIDAS-Verordnung erfüllt (Art. 3 Nr. 11 eIDAS-Verordnung). Sie muss daher die folgenden Anforderungen erfüllen:

a) Sie ist eindeutig dem Unterzeichner zugeordnet.

b) Sie ermöglicht die Identifizierung des Unterzeichners.

c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Eine qualifizierte elektronische Signatur erfüllt dieselben Anforderungen wie eine fortgeschrittene elektronische Signatur. Darüber hinaus bestehen besondere Anforderungen hinsichtlich der Verwendung einer (qualifizierten) Signaturerstellungseinheit zur Erzeugung der qualifizierten Signatur sowie an das der Signatur zugrunde liegende (qualifizierte) Zertifikat (vgl. Art. 28 ff. eIDAS-VO i.V.m. Anhang I bzw. II eIDAS-VO). Eine qualifizierte elektronische Signatur unterliegt damit strengeren rechtlichen Vorgaben als eine fortgeschrittene elektronische Signatur und muss technisch und organisatorisch die höchsten Sicherheitsstandards erfüllen.

Dementsprechend knüpft das Gesetz unterschiedliche Rechtswirkungen an eine fortgeschrittene und an eine qualifizierte elektronische Signatur. Nur die qualifizierte elektronische Signatur erfüllt besondere Formerfordernisse im materiellen Recht (§ 126a BGB) sowie im Verfahrensrecht (darunter § 130a ZPO und § 3a Abs. 2 VwVfG). Vgl. zu den Rechtswirkungen einer qualifizierten elektronische Signatur Frage 3.

2. Wozu benötigt man elektronische Signaturen?

Die Digitalisierung ist zu einem Kernthema unserer Gesellschaft geworden. Sie betrifft nicht mehr nur klassische IT-Unternehmen, sondern erfasst inzwischen viele Bereiche des Geschäfts- sowie des Privatlebens. Die technologischen Entwicklungen verändern die Art, wie wir uns informieren, wie wir kommunizieren und uns vernetzen. Die Gewährleistung von Vertrauen und Integrität ist dabei mehr denn je von zentraler Bedeutung. Dies zeigt sich insbesondere beim elektronischen Datenaustausch über Netzwerke. Hierbei können wir nicht sicher sein, dass unsere Kommunikationspartner wirklich immer diejenigen sind,

für die sie sich ausgeben. Auch ist nicht sichergestellt, dass die Daten so ankommen, wie sie abgesendet wurden. Mangelndes Vertrauen in unsere Kommunikationspartner und in deren Kommunikationsinhalte erschwert jedoch ein rechtsverbindliches elektronisches Handeln. Dies gilt insbesondere für die Verfahren des elektronischen Rechtsverkehrs, in denen es elementare Voraussetzung ist, die Identität und verfahrenstechnische Legitimation des Ausstellers einer Erklärung sicherzustellen. Die Technik der elektronischen Signatur kann die zentralen Fragen nach der Identität des Gegenübers und der Integrität der Inhalte lösen. Sie ermöglicht die eindeutige Feststellung, wer der tatsächliche Aussteller einer elektronischen Erklärung ist, und ob die übermittelten Daten unversehrt angekommen sind oder unterwegs verändert wurden. Mit der beweissicheren Zuordnung der signierten Daten zu einer Person schafft die elektronische Signatur damit die Voraussetzung für ein rechtsverbindliches elektronisches Handeln.

3. Welche Rechtswirkungen hat eine elektronische Signatur?

Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift (Art. 25 Abs. 2 eIDAS-Verordnung). Daher kann die schriftliche Form durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt (§ 126 Abs. 3 BGB). 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 (§ 126a Abs. 1 BGB).

Ferner erlaubt die qualifizierte elektronische Signatur es, besondere Formerfordernisse im Verfahrensrecht zu erfüllen (vgl. z.B. § 130a ZPO oder § 3a VwVfG).

Hinsichtlich der Beweiswirkung einer qualifizierten elektronischen Signatur sieht § 371a Abs. 1 ZPO für das Zivilrecht vor, dass auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung finden. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich aufgrund der Prüfung der qualifizierten elektronischen Signatur nach Art. 32 der eIDAS-Verordnung ergibt, kann daher nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung von der verantwortenden Person abgegeben worden ist.

Für qualifizierte Zeitstempel gilt die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

4. Was muss ich tun, um ein Dokument elektronisch zu signieren?

Das konkrete Vorgehen bei der Signatur eines Dokuments ist von der verwendeten Software abhängig. Die grundlegenden Schritte bei der Erstellung einer Signatur sind aber immer gleich.

In XNotar können Dokumente mithilfe der Signaturmappe qualifiziert elektronisch signiert werden. Weitere Informationen hierzu finden Sie unter https://onlinehilfe.bnotk.de/display/XNP/Signaturmappe.

.

5. Was ist zu tun, wenn signierte Daten über einen längeren Zeitraum benötigt werden?

Der Zeitraum, in dem elektronische signierte Dokumente aufzubewahren sind, kann sehr unterschiedlich sein. Eine langfristige Aufbewahrung kann bspw. aus langen Gewährleistungs- oder Verjährungsfristen resultieren oder eine Rolle spielen, wenn das Dokument zukünftig als Beweismittel dienen soll. Bei einer gewünschten oder erforderlichen langen Aufbewahrungszeit ist daher zu beachten, dass die Sicherheit der einer elektronischer Signatur zugrundliegenden Algorithmen und der zugehörigen Parameter im Laufe der Zeit aufgrund neuer wissenschaftlicher Erkenntnisse oder infolge des technischen Fortschritts abnimmt.

Aus diesem Grund werden die Berechnungsroutinen und Parameter zur Erzeugung elektronischer Signaturen nur für einen bestimmten Zeitraum im Voraus als geeignet beurteilt, danach einer erneuten Prüfung unterzogen und wenn nötig den veränderten technischen Gegebenheiten angepasst. Die Bundesnetzagentur veröffentlicht daher unter der Adresse https://www.bundesnetzagentur.de regelmäßig eine Übersicht der geeigneten mathematischen Verfahren und legt den Zeitpunkt fest, bis zu dem deren Eignung gilt.

Qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten sind daher, sofern hierfür Bedarf besteht, erneut qualifiziert zu signieren, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen (vgl. § 15 VDG).

6. Was muss ich tun, um eine elektronische Signatur zu prüfen?

Zum Prüfen einer elektronischen Signatur müssen die mathematische Korrektheit der Signatur, der Zertifizierungspfad (Zertifikatskette) unter Berücksichtigung des zugrunde liegenden Gültigkeitsmodells und die Gültigkeit des Zertifikats zum Signaturzeitpunkt geprüft werden. Diese Verifikationsschritte werden üblicherweise von Softwarekomponenten, sogenannten Signaturanwendungskomponenten, durchgeführt – beispielweise XNotar.

Im Programm XNotar ist eine Signaturprüfung über den integrierten PDF-Viewer möglich. Weitere Informationen hierzu finden Sie in der Onlinehilfe unter https://onlinehilfe.bnotk.de/display/XNP/PDF-Viewer.

7. Was macht ein (qualifizierter) Vertrauensdiensteanbieter?

Generierung der Schlüssel

Das zum elektronischen Signieren verwendete Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel, muss erstellt (generiert) werden. Sehr wichtig ist in diesem Zusammenhang, dass es jedes Schlüsselpaar nur einmal geben darf. Weiterhin darf niemand – auch nicht der Vertrauensdiensteanbieter selbst – Kenntnis von dem privaten Schlüssel erlangen. Die an der Schlüsselgenerierung beteiligten Systeme wurden eingehend auf diese Anforderungen überprüft und als vollumfänglich geeignet beurteilt. Hinzu kommen regelmäßige Überprüfungen der vorgeschriebenen Sicherheitsmechanismen. Ein weiteres wichtiges Sicherheitsmerkmal ist das Speichermedium des Schlüsselpaares. Dieses Speichermedium – die qualifizierte elektronische Signaturerstellungseinheit (QSCD) – stellt sicher, dass der private Schlüssel das Speichermedium niemals verlässt. Die Bundesnotarkammer verwendet im Fall von Signaturkarten eigens für diesen Zweck geprüfte und zertifizierte Chipkarten. Bei Fernsignaturen verbleibt der private Schlüssel beim Vertrauensdiensteanbeiter auf einem remote-QSCD, dem Hardware-Sicherheitsmodul (HSM). Nachdem das Schlüsselpaar beim Vertrauensdiensteanbieter generiert wurde, wird es einem registrierten Anwender zugeordnet (Personalisierung), indem die persönlichen Daten des Anwenders mit dem öffentlichen Schlüssel durch eine elektronische Signatur der Zertifizierungsstelle verbunden werden.

Zertifizierung des öffentlichen Schlüssels

„Zertifizierung" bedeutet wörtlich genommen „Bescheinigung". Vertrauensdiensteanbieter bescheinigen, dass ein öffentlicher Schlüssel zu dem Inhaber des Schlüsselpaares gehört. Um dieses leisten zu können, muss der Vertrauensdiensteanbieter die Identität des Anwenders zuverlässig feststellen. Hierzu bedient sich die Bundesnotarkammer unter anderem der notariellen Unterschriftsbeglaubigung, bei der der Notar den Anwender identifiziert. Wenn der Vertrauensdiensteanbieter die Identität des Anwenders festgestellt hat, erstellt er individuell für den Anwender eine Chipkarte sowie das Schlüsselpaar zum elektronischen Signieren. Dass der öffentliche Schlüssel dem Anwender zugeordnet wurde, bescheinigt der Vertrauensdiensteanbieter durch das Zertifikat (in der eIDAS- Verordnung als „qualifiziertes Zertifikat für elektronische Signaturen" bezeichnet und nachfolgend auch das Zertifikat). Ein Zertifikat enthält zum einen Daten, die es dem Empfänger elektronisch signierter Daten möglich machen, den Aussteller der Erklärung zu identifizieren. Hierzu gehört in jedem Fall der Name und Vorname des Zertifikatsinhabers (Ausnahme: der Zertifikatsinhaber hat statt seines Namens ein Pseudonym in das Zertifikat aufnehmen lassen). Als weitere Daten im Zertifikat finden sich insbesondere Angaben zu dem Vertrauensdiensteanbieter, von dem das Zertifikat ausgestellt wurde, der Identitätscode des Zertifikates, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss, sowie Angaben zu Beginn und Ende der Gültigkeitsdauer des Zertifikates. Schließlich enthält das Zertifikat den öffentlichen Schlüssel des Zertifikatsinhabers, die Bezeichnung der Algorithmen und möglicherweise Angaben zu bestimmten Beschränkungen oder Berechtigungen (siehe auch den nächsten Abschnitt: Attribute). Hiermit ist es jedermann möglich, die elektronischen Signaturen des Zertifikatsinhabers zu prüfen. Eine Übersicht über alle in den Zertifikaten der Zertifizierungsstelle der Bundesnotarkammer enthaltenen Angaben findet sich in dem auf der Internetseite der Zertifizierungsstelle

verfügbaren Zertifizierungskonzept für qualifizierte Zertifikate (CPS) unter folgendem Link: https://zertifizierungsstel bnotk.de/veroeffentlichungen.

Damit der Empfänger eines Zertifikates sicher sein kann, dass das Zertifikat nicht verändert wurde und alle Angaben korrekt sind, wird jedes elektronische Zertifikat von dem Vertrauensdiensteanbieter, der das Zertifikat ausgibt, elektronisch signiert. Damit kann jeder Empfänger zweifelsfrei feststellen, dass das Zertifikat von dem Vertrauensdiensteanbieter stammt und dass dieses nicht manipuliert wurde oder unvollständig ist.

Ein Zertifikat ist somit mit einem elektronischen Ausweis des Zertifikatsinhabers vergleichbar. Es enthält Informationen zum Zertifikatsinhaber, zum Zertifikatsaussteller und dient der Zuordnung eines öffentlichen Schlüssels zu einer Person. Die Echtheit dieses Zertifikates wird durch den Vertrauensdiensteanbieter mittels elektronischer Signatur bescheinigt.

Attribute

Ein Attribut steht für eine besondere Eigenschaft oder Stellung des Zertifikatsinhabers. Die Attribute werden in das Zertifikat aufgenommen (vgl. dazu § 12 Abs. 1 VDG).

Attribut: Vertretungsmacht für eine dritte Person

Wenn Sie berechtigt sind, eine (natürliche oder juristische) Person zu vertreten, können Sie diese Berechtigung in ein Zertifikat aufnehmen lassen. Die Aufnahme von Angaben über das Bestehen einer Vertretungsmacht für eine dritte Person in das Zertifikat setzt voraus, dass dem qualifizierten Vertrauensdiensteanbieter die Einwilligung der dritten Person nachgewiesen wird. Wenn Sie für eine juristische Person vertretungsberechtigt sind, ist die Befugnis der Person, die die Einwilligung für die juristische Person abgibt, nachzuweisen (z. B. durch Vorlage eines Handelsregisterauszugs).

Attribut: Amts- und berufsbezogene oder sonstige Angaben zur Person

Es ist möglich, eine Amts- oder Berufsbezeichnung sowie sonstige Angaben zur Person in ein Zertifikat aufzunehmen. Die Aufnahme erfolgt nur, wenn ein entsprechender Nachweis erfolgt. Wenn eine Amts- oder Berufsbezeichnung bzw. eine sonstige Angabe zur Person in ein Zertifikat aufgenommen werden soll, ist daher eine Bestätigung der jeweils zuständigen Stelle den Antragsunterlagen beizulegen. Für die Bestätigung der Eigenschaft als Notar oder Notariatsverwalter sind gemäß § 67 Abs. 3 S. 5 BNotO die Notarkammern zuständig.

Attribut: Weitere personenbezogene Angaben

Es ist ferner möglich, weitere personenbezogene Angaben in das Zertifikat aufzunehmen, vorausgesetzt dass der Betroffene eingewilligt hat.

In jedem Fall, in dem ein Dritter in die Aufnahme eines Attributs einwilligt, hat dieser die Befugnis, das Zertifikat, das das entsprechende Attribut enthält, widerrufen zu lassen, soweit das zugrunde liegende Rechtsverhältnis (Berufsträgereigenschaft, Vertretungsmacht) erloschen ist.

Aufnahme von Beschränkungen

In einem Zertifikat können zudem beliebige Beschränkungen abgebildet werden. Sie müssen selbst dafür sorgen, dass die von Ihnen angegebene Beschränkung sinnvoll ist, eine inhaltliche Prüfung durch den Vertrauensdiensteanbieter findet nicht statt. Ein Beispiel ist eine monetäre Beschränkung. Hier können Sie Eintragungen vornehmen lassen, wenn Sie nur finanzielle Transaktionen bis zu einer bestimmten Höhe mit Ihrer elektronischen Signatur tätigen wollen. Aus technischen Gründen werden nur die ersten beiden Stellen Ihrer Angaben berücksichtigt, die folgenden Stellen werden aufgerundet.

Bitte beachten Sie, dass bei der Verwendung von elektronischen Signaturen im elektronischen Rechtsverkehr nicht abschließend geklärt ist, welche Bedeutung monetäre Zertifikatsbeschränkungen haben.

Bereitstellen der Zertifikate (Verzeichnisdienst)

Um eine elektronische Signatur zu überprüfen, muss es möglich sein, jederzeit von einer vertrauenswürdigen Stelle zu erfahren, ob das qualifizierte Zertifikat für elektronische Signaturen existiert, gültig und nicht widerrufen ist. Diese Aufgabe erfüllt die Zertifikatsdatenbank der Bundesnotarkammer (auch genannt der Verzeichnisdienst) für die von der Bundesnotarkammer ausgegebenen (qualifizierten) Zertifikate. Wenn der Zertifikatsinhaber bei Beantragung seiner Signaturkarte angegeben hat, dass sein Zertifikat nicht abrufbar sein soll, erhält man bei der Abfrage des Verzeichnisdienstes lediglich die Auskunft, dass ein Zertifikat für die Person existiert, und ob dieses gültig oder ungültig ist (vergleichen Sie hierzu den nächsten Punkt).

Entgegennahme und Ausführung von Widerrufen durch den Vertrauensdiensteanbieter (Sperr- bzw. Widerrufsdienst)

Zertifikate können bereits vor dem Ende des Gültigkeitszeitraumes durch Widerruf des Zertifikats ungültig werden. Einen Widerruf des Zertifikats kann zunächst der Zertifikatsinhaber jederzeit selbst verlangen (§ 14 Abs. 1 Nr. 1 VDG). Wenn der Zertifikatsinhaber feststellt, dass z. B. seine Signaturkarte verloren gegangen ist oder ihm gestohlen wurde, muss er das Zertifikat widerrufen lassen, um einem Missbrauch vorzubeugen. Ein Widerruf des Zertifikates kann auch durch den Vertrauensdiensteanbieter erfolgen (vgl. § 14 Abs. 1 VDG). Neben den gesetzlichen Widerrufsgründen sind in den Allgemeinen Geschäftsbedingungen oder dem maßgeblichen Rahmenvertrag weitere Widerrufsgründe vertraglich vereinbart. Der Vertrauensdiensteanbieter kann ein Zertifikat insbesondere auch dann widerrufen, wenn der Zertifikatsinhaber seinen vertraglichen Pflichten nicht nachkommt. Enthält ein Zertifikat ein Attribut, das eine Bestätigung eines Dritten verlangt, hat ferner dieser Dritte das Recht, den Widerruf des Zertifikats zu verlangen, wenn die Vertretungsmacht oder die Voraussetzungen für die amts- und berufsbezogenen oder die sonstigen Angaben zur Person entfallen sind (vgl. § 14 Abs. 2 VDG). Ferner kann unter bestimmten Voraussetzungen die Aufsichtsstelle den Widerruf eines Zertifikates anordnen (§ 14 Abs. 3 VDG).

Der Widerruf eines Zertifikats wird im Verzeichnisdienst registriert und der Widerrufsstatus zeitnah, jedenfalls innerhalb von 24 Stunden, veröffentlicht, damit eine Abfrage des widerrufenen Zertifikates den jeweils aktuellen Status des Zertifikates anzeigt. Diese Möglichkeit des Widerrufs existiert bei der Bundesnotarkammer an sieben Tagen in der Woche und an vierundzwanzig Stunden jeden Tages.

Ein Widerrufsverlangen kann telefonisch unter der kostenlosen Rufnummer:

0800 - 3550 400

oder schriftlich unter:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

eingericht werden.

Per E-Mail eingehende Widerrufsaufträge können leider nicht bearbeitet werden. Bitte kontrollieren Sie vier Tage nach der schriftlichen Beantragung, ob der Widerruf im Verzeichnisdienst eingetragen ist. Bei einem telefonischen Widerrufsverlangen sollten Sie, falls möglich, Ihre Produktnummer angeben, welche sich in unseren Benachrichtigungen befindet oder auf der Chipkarte aufgedruckt ist, sowie Ihr Widerrufs- bzw. Sperrkennwort.

8. Was geschieht in technischer Hinsicht beim elektronischen Signieren?

Nachdem die Funktion „Signieren“ gewählt wurde, berechnet das Signaturprogramm eine Kurzform der Datei. Dieser sogenannte „Hash-Wert“ wird durch eine mathematische Funktion erzeugt und ist mit einem Fingerabdruck vergleichbar: Jede Datei hat ihren individuellen Hash-Wert. Jede auch noch so geringe Veränderung in der Datei (und sei es nur ein zusätzliches Leerzeichen zwischen zwei Worten) führt dazu, dass ein veränderter Hash-Wert berechnet wird. Der Hash-Wert ist damit eine individuelle Kurzform der zu signierenden Datei. Dieser Hash-Wert ist keine inhaltliche Zusammenfassung der Datei, sondern eine Zeichenkette.

Der individuelle Hash-Wert wird dann zum eigentlichen elektronischen Signieren übergeben. Dabei wird der Hash-Wert mit Hilfe des privaten Schlüssels der qualifizierten Signatur verschlüsselt und in dieser verschlüsselten Form wieder zurück an das Signaturprogramm übergeben. Der private Schlüssel wird entweder direkt auf der verwendeten Signaturkarte angewendet oder im sicheren Rechenzentrum mit der dort hinterlegten Fernsignatur (dafür wird der Hash an das Rechenzentrum gesendet, dort verschlüsselt und verschlüsselt zurückgesandt) verwendet. Der verschlüsselte Hash-Wert der Datei ist die eigentliche elektronische Signatur. Da jede Änderung der Datei zu einer Änderung des Hash-Wertes führt, kann durch einen Vergleich des einem Empfänger zugegangenen verschlüsselten Hash-Wertes mit einem erneut erstellten Hash-Wert der ebenfalls übertragenen Datei in unveränderter Form festgestellt werden, ob die Datei unverändert beim Empfänger angekommen ist.

Das Zertifikat enthält den öffentlichen Schlüssel. Der Empfänger erhält daher zusammen mit Ihrer Datei auch den Schlüssel, mit dem er den verschlüsselten Hash entschlüsseln kann, um diesen dann mit dem selbst ermittelten Hash des erhaltenen Dokumentes für die Prüfung der Unveränderlichkeit zu vergleichen. Dadurch, dass jedes Schlüsselpaar nur einmal vergeben wird, können die Daten nur so entschlüsselt und damit eindeutig einem Aussteller (und Inhaber eines privaten Schlüssels) zugeordnet werden.

Der Signaturvorgang

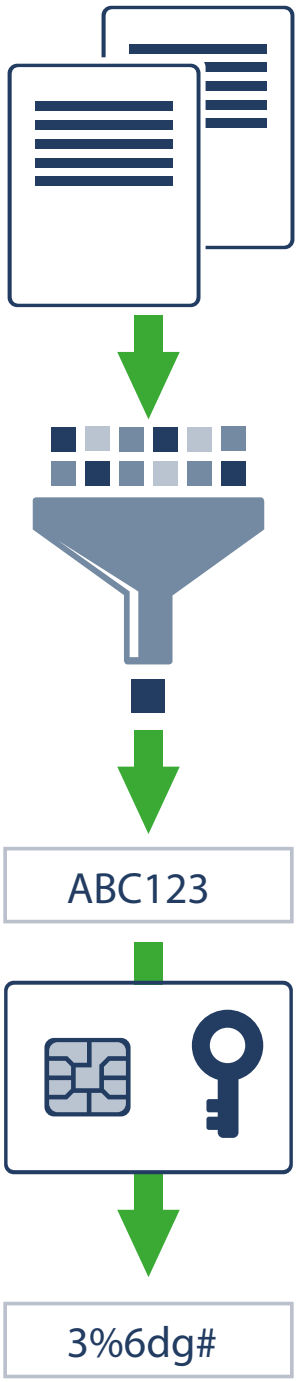
Textdokument (z. B. Vertragsentwurf)

„Hash"-Funktion: Schrumpft große Datenmengen auf einen „Fingerabdruck" klein. Jedem Dokument ist eindeutig ein „Fingerabdruck" zugeordnet.

„Fingerabdruck" (="Hash"-Wert)

Der„Fingerabdruck" wird mit dem geheimen Schlüssel der Signaturkarte verschlüsselt.

Der verschlüsselte Fingerabdruck ist die elektronische Signatur.

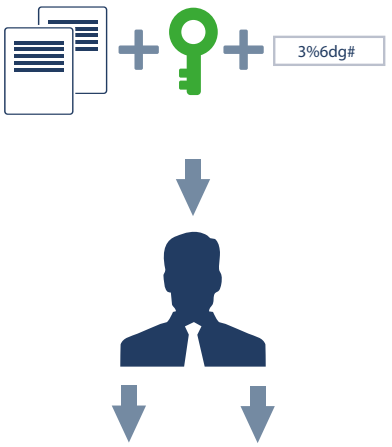


Die Signaturprüfung

Der Empfänger erhält das Dokument nebst elektronischer Signatur und öffentlichem Schlüssel des Absenders. Er muss nun zwei Fragen prüfen:

1. Von wem stammt das Dokument?

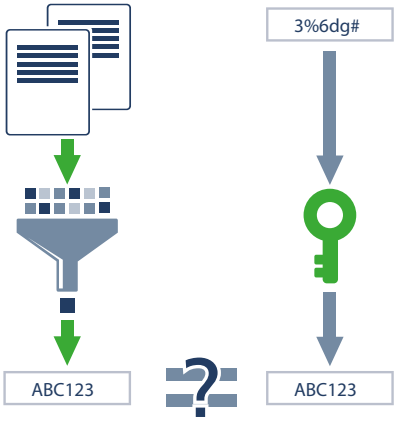
2. Ist der Inhalt des Dokumentes unverändert?



Er ermittelt selbst mit der Hash-Funktion den „Fingerabdruck" des übermittelten Dokumentes.

Mit dem öffentlichen Schlüssel entschlüsselt er die übermittelte elektronische Signatur.

Stimmen beide Werte überein, ist das signierte Dokument unverändert übermittelt worden.



Die Signaturprüfung: Zertifikatsabfrage

Der Empfänger fragt im Verzeichnisdienst der Zertifizierungsstelle online nach, ob der Absender der Nachricht dort mit den übersendeten Daten (Zertifikatsnummer, öffentlicher Schlüssel) gespeichert ist.

Die Informationen werden im Verzeichnisdienst überprüft. Darüber hinaus wird die Gültigkeit des verwendeten Zertifikates gesprüft und das Ergebnis entsprechend bereitgestellt.

Die Zertifizierungsstelle teilt das Ergebnis der Zertifikatsprüfung dem Anfragenden mit.

9. Was muss ich beim elektronischen Signieren beachten?

Die Chipkarte und das qualifiziertes Zertifikat sind sichere Werkzeuge zum elektronischen Unterschreiben und Verschlüsseln. Im Umgang mit der Technik der elektronischen Signatur müssen jedoch bestimmte Regeln beachtet werden, damit diese Sicherheit nicht beeinträchtigt wird.

Überprüfen Sie vor dem elektronischen Signieren den Inhalt der Daten, die elektronisch signiert werden sollen. Verwenden Sie hierzu z. B. die Darstellungskomponente Ihrer Software (bspw. XNotar), die sicherstellt, dass Sie wirklich die Daten zur Prüfung angezeigt bekommen, auf die sich die Signatur beziehen soll. Es können deshalb Unsicherheiten und Beweisprobleme auftreten, wenn signierte Anlagen ihren Inhalt über Makros oder Feldfunktionen automatisch verändern. Dateien, die Makros oder Feldfunktionen enthalten, sind für die elektronische Signatur nicht geeignet (dies kann insbesondere Textverarbeitungsdateien wie Word-Dokumente betreffen). Das Programm XNotar ermöglicht die Signatur von PDF-Dokumenten, die dem PDF/A-Standard entsprechen. Darüber hinaus ist auch das Signieren von Multipage-TIFF-Dateien möglich, deren Inhalte weitgehend eindeutig dargestellt werden können, und die keine aktiven Elemente enthalten. Sie haben immer die Möglichkeit, die von Ihnen erstellten elektronischen Signaturen selbst zu prüfen, um die Richtigkeit des Inhaltes der elektronisch signierten Daten festzustellen. Ein effizienter Einsatz der elektronischen Signatur in großem Umfang erfordert die Erzeugung mehrerer Signaturen unter einmaliger Eingabe der PIN (Mehrfachsignatur). Die Signatur- und Chipkarten der Bundesnotarkammer ermöglichen deshalb die Erzeugung von bis zu 100 Signaturen mit einer PIN-Eingabe.

Bei der Mehrfachsignatur sind allerdings besonders hohe Sicherheitsanforderungen einzuhalten, um sicherzustellen, dass nur Daten signiert werden, die Sie tatsächlich signieren wollen. Die Einsatzumgebung muss unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein Missbrauch der Signaturfunktionalität der mehrfachsignaturfähigen Karte und die Ausspähung der zugehörigen Identifikationsdaten (PIN) praktisch ausgeschlossen sind und damit die alleinige Kontrolle des Karteninhabers über den Prozess der Signaturerzeugung gegeben ist. Zu den physischen Sicherungsmaßnahmen gehört der physikalische Schutz gegen unbefugten Zugriff auf die Chipkarte. Da die qualifizierte elektronische Signatur Ihrer Unterschrift entspricht, werden Ihnen Erklärungen zugerechnet, die mit Ihrer qualifizierten elektronischen Signatur versehen sind. Der entscheidende Schutz gegen die irrtümliche oder missbräuchliche Erstellung von Signaturen ist Ihre jederzeitige Kontrolle über den Signaturvorgang und der Schutz Ihrer Chipkarte vor der Verwendung durch Andere.

10. Welchen Anforderungen müssen die technischen Komponenten zum elektronischen Signieren nach der eIDAS-Verordnung genügen?

Die Sicherheit der elektronischen Signatur wird auf Seiten der Zertifizierungsstelle durch eine strenge Prüfung aller technischen Gerätschaften, eingesetzten Programme und sogar der Beschäftigten sichergestellt.

Eine sichere Erstellung elektronischer Signaturen setzt jedoch voraus, dass auch der Inhaber einer Signaturkarte als Anwender zum Erstellen von Signaturen sichere Geräte und Programme verwendet. Das durch das Vertrauensdienstegesetz abgelöste Signaturgesetz legte in Verbindung mit der ebenfalls aufgehobenen Signaturverordnung Mindestanforderungen für die technische Sicherheit von Produkten zu Erstellung qualifizierter elektronischer Signaturen fest. Die Hersteller der jeweiligen Produkte mussten in einer sogenannten Herstellererklärung darlegen, wie die jeweiligen Anforderungen umgesetzt wurden. Darüber hinaus gab es für die Hersteller die Möglichkeit, ihre Produkte und die Einhaltung der gesetzlichen Anforderungen durch eine unabhängige Bestätigungsstelle prüfen zu lassen. Eine vergleichbare Regelung beinhalten weder die eIDAS-Verordnung noch das Vertrauensdienstegesetz. Lediglich für die qualifizierten elektronischen Signaturerstellungseinheiten ergeben sich Mindestanforderungen aus der Regelung in Anhang II der eIDAS-Verordnung. Aufgrund der durch unabhängige Stellen durchgeführten Prüfung empfehlen wir daher, für den Einsatz von qualifizierten elektronischen Signaturen soweit möglich weiterhin bestätigte Komponenten, also bestätigte Chipkartenleser und bestätigte Anwendersoftware, einzusetzen. Die Bewertung als sicher bezieht sich allerdings immer nur auf den Zustand, in dem Sie das Produkt oder das Programm erhalten haben. Jede Veränderung oder jeder Eingriff in die Geräte oder die Software führt dazu, dass die Sicherheitseinstufung als bestätigtes Produkt oder hinreichend geprüftes Produkt erlischt.

Zudem sind Produkte und Programme vor unbefugtem Zugriff zu schützen und nur innerhalb einer vertrauenswürdigen Umgebung einzusetzen. Achten Sie insbesondere darauf, dass sich auf dem Computer, mit dem Sie Ihre elektronischen Signaturen erzeugen, keine Viren oder andere schädliche Programme wie Trojaner oder Würmer befinden. Überprüfen Sie vor dem elektronischen Signieren den Inhalt der Daten, die elektronisch signiert werden sollen. Verwenden Sie hierzu die Darstellungskomponente der jeweiligen Signaturanwendung, die sicherstellt, dass Sie wirklich das zum Prüfen angezeigt bekommen, was Sie im Folgenden elektronisch signieren. Sie haben immer die Möglichkeit, die von Ihnen erstellten elektronischen Signaturen selbst zu prüfen, um die Richtigkeit des Inhaltes der elektronisch signierten Daten festzustellen.

Stellen Sie sicher, dass sich alle Geräte und Programme, die Sie zum elektronischen Signieren benötigen, in ordnungsgemäßem Zustand befinden. Verhindern Sie den Zugriff von Unberechtigten auf diese Komponenten durch den Einsatz von geeigneten Sicherungsmaßnahmen. Stellen Sie sicher, dass Geräte und Programme zum elektronischen Signieren und zum Prüfen elektronischer Signaturen vertrauenswürdig und zuverlässig installiert werden, und betreiben Sie diese nur gemäß ihrer Spezifikation und Dokumentation. Vergewissern Sie sich, dass der von Ihnen am Arbeitsplatz verwendete Rechner vertrauenswürdig installiert und administriert wurde, und dass nur vertrauenswürdige

Software eingesetzt wird.

Setzen Sie Sicherheitsprodukte wie Virenscanner und Firewalls ein, um die Integrität der von Ihnen zum elektronischen Signieren verwendeten Systeme zu schützen. Eine zuverlässige Sicherung der Einsatzumgebung gegen Gefahren aus dem Internet gewährleistet für Notare insbesondere die Anbindung an das Notarnetz. Informationen zum Notarnetz finden Sie unter https://notarnet.de/.

11. Was muss ich im Umgang mit der Signaturkarte beachten?

Die elektronische Signatur ist Ihre persönliche elektronische Unterschrift. Im Umgang mit Ihrer Chipkarte ist daher sicherzustellen, dass Signaturen ausschließlich durch Sie persönlich angebracht werden können. Besonders hohe Sicherheitsanforderungen gelten, da Sie mit der Signaturkarte bzw. Chipkarte und Fernsignatur der Bundesnotarkammer mehrere Signaturen mit einer PIN-Eingabe erzeugen können. Jeder Signaturschlüssel einer Signaturkarte ist vor seiner ersten Nutzung mit einer fünfstelligen Transport-PIN geschützt, mit der nur der Wechsel zu einer individuellen mindestens sechsstelligen Signatur-PIN möglich ist. Dieser Wechsel ist durch den Karteninhaber unverzüglich vorzunehmen, sobald er eine Signaturkarte und Transport-PIN besitzt. Hierbei ist zu prüfen, ob die Signaturkarte mit der fünfstelligen Transport-PIN geschützt ist, da nur dann sichergestellt ist, dass mit der Karte noch keine Signaturen erzeugt wurden. Die Signatur-PIN sollte hierbei unterschiedlich zu der PIN für Verschlüsselung und Authentisierung gewählt werden. Bei der Kombination Chipkarte und Fernsignatur erfolgt das Auslösen der qualifizierten elektronischen (Fern)Signatur mit der einzigen auf der Karte befindlichen PIN für Verschlüsselung und Authentisierung. Da es sich hierbei um eine Wirk-PIN handelt, die direkt nach Erhalt für das Signieren genutzt werden kann, empfiehlt die Bundesnotarkammer die sofortige Änderung der PIN nach Empfang des PIN-Briefes. Die Chipkarte ist von Ihnen diebstahlgesichert, ausschließlich in persönlichem Besitz zu behalten und nicht an andere zu übergeben.

Für Notare legt§ 33 BNotO ausdrücklich fest, dass diese die zur Erzeugung amtlicher qualifizierter Signaturen bestimmten elektronischen Signaturerstellungsdaten nur selbst verwalten dürfen. Der Notar darf die hierzu bestimmte qualifizierte elektronische Signaturerstellungseinheit keiner anderen Person überlassen und er darf keine Wissensdaten preisgeben, die er zur Identifikation gegenüber seiner qualifizierten elektronischen Signaturerstellungseinheit benutzt. Er hat die Signatureinheit vor Missbrauch zu schützen. Elektronische notarielle Beglaubigungen nach § 39a BeurkG sind daher unwirksam, wenn die Signatur nicht durch den Notar persönlich vorgenommen wurde. Sollten Sie Ihre Chipkarte einmal verlieren, müssen Sie umgehend deren Sperrung und damit einhergehend den Widerruf der darauf befindlichen Zertifikate veranlassen. Für Notare ergibt sich dies bereits aus der Regelung des § 2 DNotO.

Das Widerrufsverlangen können Sie bei der Bundesnotarkammer wie folgt stellen:

Telefonisch unter der kostenlosen Nummer:
0800 - 3550 400

oder per Brief an die Anschrift:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

Benutzen Sie Ihre Signaturkarte nur mit Geräten, die Ihnen bekannt sind und von deren Zuverlässigkeit Sie sich überzeugt haben. Beachten Sie die Sicherheitshinweise und verwenden Sie alle Geräte und Programme nur gemäß deren Spezifikation und Dokumentation. Überprüfen Sie regelmäßig die Integrität der Produkte und der zugrundeliegenden Plattform (Hardware und Betriebssystem) und schützen Sie Ihre IT-Plattform vor Schadsoftware. Sorgen Sie für eine vertrauenswürdige Sicherheitsadministration des Systems. Sollte Ihre Signaturkarte beschädigt sein, besteht die Möglichkeit, dass versucht wurde, sie zu manipulieren. Wenn Sie die Beschädigung nicht zuordnen können, nehmen Sie zur Sicherheit eine Sperrung des Signaturschlüssel-Zertifikates vor.

12. Was muss ich im Umgang mit der PIN beachten?

Elektronisches Signieren ist nur möglich, wenn man den Signiervorgang durch Eingabe der PIN aktiviert. Wer im Besitz der PIN und der Chipkarte ist, kann also elektronisch signieren. Die PIN ist daher von Ihnen unter allen Umständen geheim zu halten. Sollte ein Dritter Kenntnis von Ihrer PIN erhalten haben oder haben Sie die Vermutung, dass dieses geschehen ist, muss die PIN unverzüglich geändert werden. Dies ist z.B. in XNP möglich. Gegebenenfalls sollten Sie die Chipkarte sperren und die darauf befindlichen Zertifikate widerrufen lassen.

Achten Sie bei der Wahl Ihrer PIN darauf, dass es Dritten nicht möglich sein darf, die von Ihnen gewählte PIN zu erraten. Zahlen aus Ihrem persönlichen Umfeld (Geburtsdaten, Telefonnummern und Ähnliches) sollten daher nicht als PIN verwendet werden. Vermeiden Sie es, nur eine Zahl als PIN für unterschiedliche Anwendungen, Chipkarten oder Authentisierungsvorgänge zu verwenden. Nach der dreimaligen Eingabe einer falschen PIN können Sie unter Verwendung der Ihnen bekannten PUK, den Fehlerzähler zurücksetzen und erneut die PIN eingeben. Haben Sie Ihre PUK 10mal verwendet, kann diese nicht mehr verwendet werden und Sie müssen eine neue Chipkarte bestellen.

13. Welche Bedeutung hat die Aufnahme eines Pseudonyms in das Zertifikat?

Wenn Sie sich dafür entscheiden, ein Pseudonym in das Zertifikat aufzunehmen, wird NUR das Pseudonym und keine weiteren persönlichen Daten in das Zertifikat aufgenommen. Zur Vornahme elektronischer Beglaubigungen sind Signaturkarten mit Pseudonym daher nicht geeignet. Pseudonyme sind durch den Eintrag „:PN“ im Zertifikat gekennzeichnet. Pseudonyme können innerhalb des Anwenderkreises der Bundesnotarkammer nur einmal vergeben werden. Beantragen mehrere Teilnehmer das gleiche Pseudonym, so werden diese durchnummeriert, z. B. „Pseudonym :1 PN“, „Pseudonym :2 PN“, etc.

Gemäß § 8 Abs. 2 VDG darf die Bundesnotarkammer unter bestimmten Voraussetzungen

und zu bestimmten Zwecken personenbezogene Daten einer Person, die Vertrauensdienste nutzt, einschließlich Daten über die Identität eines Anwenders mit Pseudonym, auf Ersuchen an die zuständigen Stellen übermitteln. Die Übermittlung ist durch die Bundesnotarkammer zu dokumentieren. Die Behörde, die um die Übermittlung der Daten ersucht, hat die betroffene Person über die Übermittlung der Daten zu unterrichten. Von der Unterrichtung kann abgesehen werden, solange die Wahrnehmung der gesetzlichen Aufgaben gefährdet würde und solange das Interesse der betroffenen Person an der Unterrichtung nicht überwiegt. Fünf Jahre nach der Übermittlung kann endgültig von der Benachrichtigung abgesehen werden, wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

14. Was sind die Bedingungen dafür, dass mir eine elektronische Signatur im Rechtsverkehr zugeordnet wird?

Erforderlich ist hierfür, dass der Anwender einer elektronischen Erklärung seinen Namen hinzufügt und das elektronische Dokument mit einer qualifizierten elektronischen Signatur, die durch Verwendung der Chipkarte der Bundesnotarkammer erzeugt werden kann, versieht. Da Sie die PIN geheim halten und diese zum qualifizierten elektronischen Signieren unbedingt eingeben müssen, werden Ihnen nach soweit ersichtlich herrschender Meinung alle mit Ihrem privaten Signaturschlüssel erzeugten qualifizierten elektronischen Signaturen grundsätzlich zugeordnet, wenn das dazugehörige Zertifikat zum Zeitpunkt der Erzeugung der qualifizierten elektronischen Signatur gültig war.

15. Wie beantrage ich eine Signaturkarte der Bundesnotarkammer?

Ausgangspunkt für die Antragstellung ist der Online-Antrag unter

https://zertifizierungsstelle.bnotk.de/produkte/alle-produkte.

Hier finden Sie die unterschiedlichen Produkte und Anträge nach Bezugsgruppe unterteilt. Haben Sie den entsprechenden Online-Antrag vollständig ausgefüllt und die Antragsunterlagen ausgedruckt, so begeben Sie sich mit dem ausgedruckten Antrag und einem aktuellen Ausweisdokument zu einem Notar Ihrer Wahl. In Gegenwart des Notars unterzeichnen Sie den Antrag. Sofern Sie Ihren Antrag bereits zuvor unterzeichnet haben, können Sie Ihre Unterschrift auf dem Antrag auch in Gegenwart des Notars anerkennen. Der Notar beglaubigt Ihre Unterschrift unter dem Antrag. Mit Ihrer Unterschrift auf dem Antrag willigen Sie in die Anfertigung einer Ablichtung Ihres vorgelegten Ausweisdokuments ein. Die Notarin oder der Notar senden dann für Sie sämtliche Unterlagen an die Zertifizierungsstelle der Bundesnotarkammer. Sofern dem Antrag die Bestätigung einer Berufsträgereigenschaft beizufügen ist, übergeben Sie das mit dem Antrag ausgedruckte Bestätigungsformular an die bestätigende Stelle, welche die Bestätigung unmittelbar an die Zertifizierungsstelle sendet. Die Notareigenschaft wird automatisch über einen Abgleich mit dem Notarverzeichnis bestätigt.

Für Justizangehörige kann das beschriebene Verfahren auch durch den Präsidenten oder Direktor eines deutschen Gerichts durchgeführt werden. Für Rechtsanwälte steht die Möglichkeit offen, sich durch die für sie zuständige Rechtsanwaltskammer identifizieren zu lassen. Gegebenenfalls stellt die Zertifizierungsstelle der Bundesnotarkammer andere Identifizierungsmöglichkeiten zur Verfügung, die Sie während der Antragstellung auswählen

können. Soweit das Identifikationsverfahren mit der Unterschriftsbeglaubigung beim Erstantrag einer natürlichen Person durchgeführt wurde, ist es regelmäßig bei der Beantragung von weiteren qualifizierten Zertifikaten entbehrlich, die Unterschrift nochmals zu beglaubigen. Folgezertifikatsanträge können darum privatschriftlich oder mittels Login mit einer bereits vorhandenen Chipkarte gestellt werden. Ihr Antrag kann von der Bundesnotarkammer nur bearbeitet werden, wenn er den hier dargestellten Anforderungen entspricht. Anschließend wird Ihnen Ihre Chipkarte bzw. Ihr Folgezertifikat zugestellt.

16. Was sind die gesetzlichen Hintergründe der elektronischen Signatur?

Die gesetzliche Grundlage für elektronische Signaturen bildet die 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 199/93/EG (eIDAS-Verordnung) sowie das zum Zwecke des effektiven Vollzugs der eIDAS-Verordnung in Deutschland erlassene Vertrauensdienstegesetz.

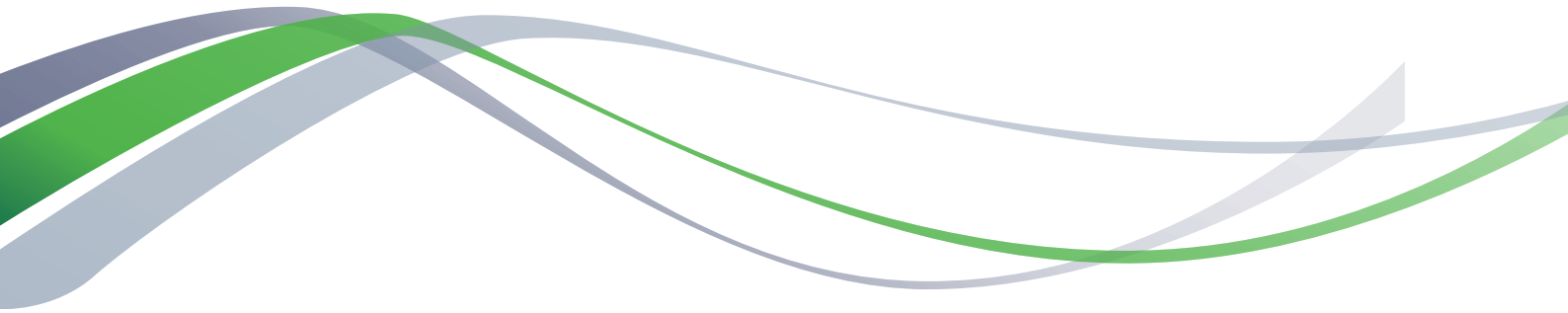
Zu den Rechtswirkungen einer elektronischen Signatur vgl. Frage 3.

17. Wo erhalte ich weitere Informationen zu technischen oder rechtlichen Fragen?

Speziell zu den technischen und rechtlichen Hintergründen elektronischer Signaturen finden sich Informationen auf der Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Bundesnetzagentur unter:

https://www.bsi.bund.de/

http://www.bundesnetzagentur.de.



Herausgeber:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

Stand: August 2021

https://zertifizierungsstelle.bnotk.de