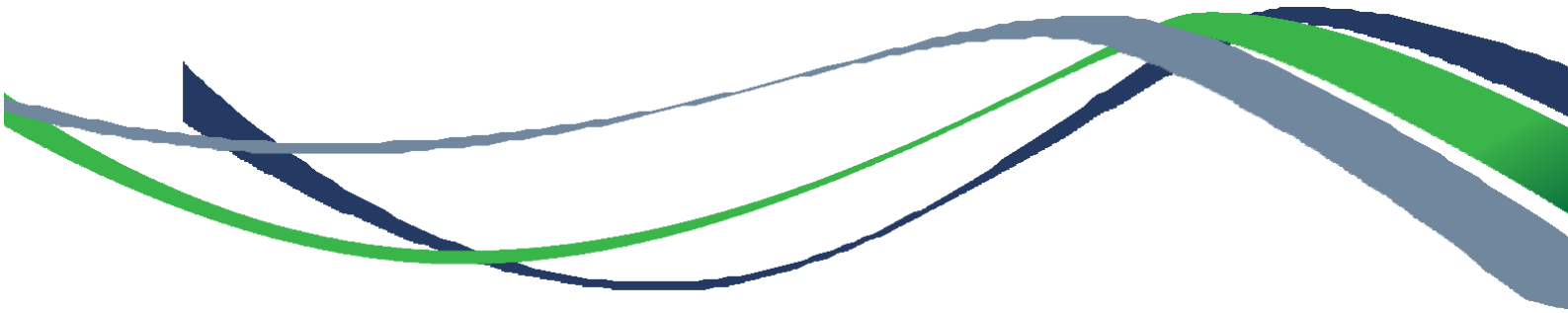
Elektronische Siegel



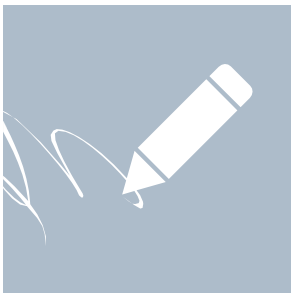
Was Sie vor dem Start wissen müssen

Sehr geehrter Anwender,
sehr geehrte Anwenderin,

mit Ihrer Entscheidung ein elektronisches Siegel bei der Bundesnotarkammer zu beantragen, haben Sie eine zukunftsweisende Entscheidung getroffen. Damit Sie von Beginn an die Vorteile Ihres elektronischen Siegels optimal nutzen können, finden Sie in dieser Broschüre alle relevanten Informationen. Des Weiteren informieren wir Sie darüber, was Sie als Anwender oder Anwenderin eines Siegelzertifikats zu beachten haben.
Bitte nehmen Sie sich daher die Zeit, die Broschüre aufmerksam durchzulesen.

Inhaltsverzeichnis

1. Was ist ein elektronisches Siegel? 4
2. Wofür kann man ein elektronisches Siegel verwenden? 4
3. Welche Rechtswirkung hat ein elektronisches Siegel? 6
4. Für wen ist ein elektronisches Siegel geeignet? 6
5. Wie erfolgt ein Siegelvorgang? 7
6. Der Siegelvorgang aus technischer Sicht 8
7. Wie kann man ein elektronisches Siegel überprüfen? 9
8. Die Siegelprüfung aus technischer Sicht 10
9. Was ist bei der Nutzung eines elektronischen Siegels zu beachten? 11
10. Wie kann ich das Siegelzertifikat widerrufen/ sperren lassen? 14
11. Wo erhalte ich weitere Informationen zu technischen oder rechtlichen Fragen? 15
12. Was geschieht mit meinen persönlichen Daten? 16



1. Was ist ein elektronisches Siegel?

Ein elektronisches Siegel ist vergleichbar mit einem digitalen Stempel einer Behörde oder eines Unternehmens.

Wie bei einer elektronischen Signatur soll auch das elektronische Siegel die Urheberschaft (Authentizität) von Dokumenten nachweisen, sowie deren Unversehrtheit (Integrität) sicherstellen. Technisch sind elektronische Signaturen und elektronische Siegel vergleichbar.

Während eine elektronische Signatur den Unterzeichner als natürliche Person identifiziert, sind elektronische Siegel ausschließlich juristischen Personen (Organisationen) zugeordnet.

Inhaber eines elektronischen Siegels können etwa Kanzleien, Gerichte, Behörden oder sonstige Organisationen sein.

2. Wofür kann man ein elektronisches Siegel verwenden?

Die technologische Entwicklung verändert die Art und Weise, wie wir kommunizieren.

Amtliche Dokumente oder Geschäftskorrespondenzen werden zunehmend elektronisch erstellt sowie digital übermittelt und gespeichert. Der sichere Nachweis von Herkunft und Echtheit ist bei vielen digitalen Dokumenten genauso unverzichtbar wie beim analogen Schriftstück.

Elektronisch gesiegelte Dokumente können einer Organisation eindeutig zugeordnet werden und dienen damit als Herkunftsnachweis.

Ein Dokument, das mit einem digitalen Siegel versehen ist, ist zudem praktisch fälschungssicher, da jeder Manipulationsversuch protokolliert wird.

Im Gegensatz zu verschlüsselten Dokumenten bleibt der Inhalt der gesiegelten Datei jedoch lesbar.

Die Anbringung eines elektronischen Siegels eignet sich überall dort, wo eine persönliche Unterschrift nicht notwendig, aber der Nachweis der Authentizität gewünscht ist, etwa bei elektronischen Rechnungen oder amtlichen Bescheiden.

Darüber hinaus können elektronische Siegel eingesetzt werden, um den Beweiswert von Dokumenten für die Langzeitzeitarchivierung zu sichern.

3. Welche Rechtswirkung hat ein elektronisches Siegel?

Elektronische Siegel haben eine besondere Beweiswirkung. Nach Art. 35 Abs. 2 eIDAS-VO gilt für qualifizierte Siegel die Vermutung des Ursprungs und der Unversehrtheit der mit dem qualifizierten Siegel verbundenen Daten.

Dokumente, die mit elektronsichen Siegeln verbunden sind, können damit ohne Einschränkung z.B. als Beweismittel in Gerichtsprozessen eingebracht werden.

Im Gegensatz zu einer qualifizierten elektronischen Signatur kann ein elektronisches Siegel jedoch nicht die gesetzliche Schriftform (gemäß § 126 BGB) erfüllen. Da elektronische Siegel nur Unternehmen und nicht einzelnen natürlichen Personen zugeordnet werden, können sie nicht die gleiche Rechtswirkung besitzen, wie die eigenhändige Unterschrift.

4. Für wen ist ein elektronisches Siegel geeignet?

Ein elektronisches Siegel kann für Organisationen (z.B. Kanzleien Gerichte oder Behörden) in Betracht kommen, die ihre elektronischen Dokumente sicher archivieren oder vertrauenswürdig mit anderen Kommunikationspartnern austauschen wollen. Wenn Organisationen ein Dokument mit ihrem elektronsichen Siegel versehen, identifizieren sie sich eindeutig als Absender und schützen die darin enthaltenden Informationen gleichzeitig vor Manipulation.

5. Wie erfolgt ein Siegelvorgang?

Das konkrete Vorgehen bei der Siegelung eines Dokuments ist von der verwendeten Signatur- bzw. Siegelsoftware abhängig. Die grundlegenden technischen Schritte bei der Erstellung eines elektronischen Siegels sind jedoch stets gleich.

Nach der Auswahl des Authentisierungstokens (Softwarezertifikat) und der erfolgreichen Eingabe einer zuvor selbstgewählten PIN wird der Siegelvorgang manuell gestartet. Das Signaturprogramm berechnet daraufhin eine krypotografische Kurzform der zu siegelnden Datei, den sogenannten „Hash-Wert".

Der Hash-Wert ist keine inhaltliche Zusammenfassung der Datei, sondern eine individuelle Zeichenkette, die durch eine mathematische Funktion erzeugt wird und einem technischen Fingerabdruck ähnelt.

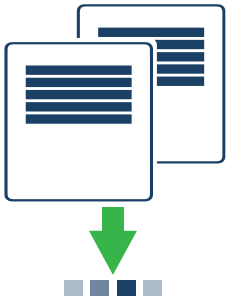
Jede signierte oder gesiegelte Datei hat ihren individuellen Hash-Wert. Dabei führt jede noch so geringe Veränderung in der Datei (und sei es nur ein zusätzliches Leerzeichen zwischen zwei Worten) dazu, dass ein neuer, veränderter Hash-Wert erzeugt wird.

Der Hash-Wert wird anschließend elektronisch an den Zertifikatsspeicher im Rechenzentrum der Bundesnotarkammer übermittelt, wo sich das qualifizierte Siegelzertifikat der Organisation befindet.

Dort wird der Hash-Wert mit Hilfe des geheimen Schlüssels des Siegelzertifikats kodiert und in dieser Form wieder an das Signaturprogramm zurückgesendet. Der nun verschlüsselte Hash-Wert wird als elektronisches Siegel an das Dokument angehängt.

6. Der Siegelvorgang aus technischer Sicht

Textdokument (z. B. elektronische Rechnung)



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

„Fingerabdruck" ("Hash"-Wert)

ABC123

Der „Fingerabdruck" wird mit dem geheimen Schlüssel des qualifizierten Zertifikats verschlüsselt.

Der verschlüsselte Fingerabdruck ist die elektronische Signatur.

3%6dg#

7. Wie kann man ein elektronisches Siegel überprüfen?

Der Empfänger eines Dokuments kann die Gültigkeit des elektronischen Siegels mithilfe einer Signatursoftware überprüfen, wobei der öffentliche Schlüssel der Organisation abgefragt wird. Dieser öffentliche Schlüssel ist in der Zertifikatsdatenbank der Bundesnotarkammer (auch "Verzeichnisdienst" genannt) gespeichert. Damit kann jeder Empfänger zweifelsfrei feststellen, ob das Siegelzertifikat von einem authorisierten Vertrauensdiensteanbieter stammt und die Gültigkeit des Siegels verifizieren. Ein gültiges elektronisches Siegel stellt sicher, dass das gesiegelte Dokument authentisch ist und unverändert beim Empfänger ankommt.

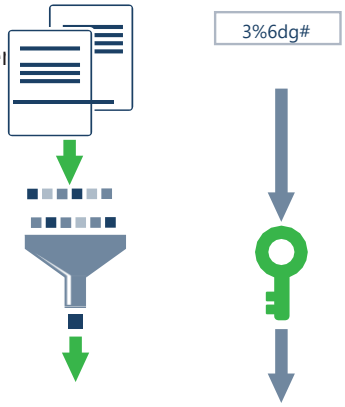
8. Die Siegelprüfung aus technischer Sicht

Der Empfänger erhält das Dokument nebst elektronischem Siegel.

Zwei Fragen sind zu prüfen:

1. Von wem stammt das Dokument?
2. Ist der Inhalt des Dokuments unverändert?

Die Software ermittelt mit der Hash-Funktion den „Fingerabdruck" des übermittelten Dokuments.



Mit dem öffentlichen Schlüssel kann das übermittelte elektronische Siegel entschlüsselt und verifiziert werden.

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

Über den Verzeichnisdienst der Zertifizierungsstelle, kann online abgerufen werden, ob der Absender der Nachricht dort mit den übersendeten Daten (Zertifikatsnummer, öffentlicher Schlüssel) gespeichert ist.

Die Informationen werden im Verzeichnisdienst überprüft. Die Gültigkeit des verwendeten Zertifikates wird geprüft und das Prüfergebnis bereitgestellt.

9. Was ist bei der Nutzung eines elektronischen Siegels zu beachten?

Im Umgang mit einem elektronischen Siegel müssen bestimmte Regeln beachtet werden, damit die Sicherheit der Zertifikate nicht beeinträchtigt wird.

- Die Verwendung des elektronischen Siegels ist nur dem Siegelinhaber sowie siegelberechtigten Personen (z.B. autorisierte Mitarbeitende) und ausschließlich zu beruflichen Zwecken gestattet.
- Voraussetzung für einen elektronischen Siegelvorgang ist der Besitz eines zuvor beantragten Authentisierungszertifikats (Softwarezertifikat). Das Softwarezertifikat ist notwendig, damit siegelberechtigte Personen sich gegenüber der Bundesnotarkammer authentisieren können, um den Siegelvorgang remote (per Fernsiegel) auszulösen. Der Einsatz eines elektronischen Siegels ist erst nach der Beantragung und der initialen Anmeldung mit einem Software-Authentisierungszertifikat möglich.
- Die Verantwortung zum Schutz der Software-Authentisierungszertifikate obliegt ausschließlich dem Inhaber bzw. dem vertretungsberechtigten Antragsteller des Siegelzertifikats. Authentisierungszertifikate sind lediglich zum Auslösen von elektronischen Siegeln einzusetzen und vor dem Zugriff durch unbefugte Dritte zu schützen.
- Ein elektronischer Siegelvorgang ist nur möglich, wenn dieser durch die Eingabe der PIN aktiviert wird. Personen, die im Besitz der PIN und des Software-Authentisierungszertifikats sind, können sodann qualifiziert elektronisch siegeln. Die PIN ist unbedingt geheim zu halten. Sollten Unbefugte Kenntnis von der PIN erhalten oder die sichere Verwendung der PIN nicht mehr gewährleistet sein, muss die PIN unverzüglich geändert werden.
- Bitte wählen Sie eine sichere PIN, damit diese nicht leicht von Unbefugten herausgefunden werden kann. Zahlen aus Ihrem persönlichen Umfeld (Geburtsdaten, Telefonnummern und Ähnliches) sollten nicht als PIN verwendet werden.
- Stellen Sie bitte sicher, dass Sie ausschließlich geprüfte Softwareprogramme zum Auslösen des Siegelvorgangs

verwenden.

- Beachten Sie die Sicherheitshinweise und verwenden Sie alle Geräte und Programme nur gemäß deren Spezifikation und Dokumentation.

- Sorgen Sie für eine vertrauenswürdige Sicherheitsadministration Ihrer Geräte und IT-Plattform. Achten Sie insbesondere darauf, dass sich auf den technischen Endgeräten, mit denen Sie Ihre elektronischen Siegel erzeugen, keine Viren oder andere schädliche Programme befinden.
- Überprüfen Sie vor jedem Siegelvorgang den Inhalt der Daten, die Sie siegeln möchten.

Siegelinhaber und Siegelberechtigte haben außerdem folgende Hinweise zu beachten:

- Das elektronische Siegel darf erst dann im Rechtsverkehr eingesetzt werden, wenn die im Siegelzertifikat enthaltenen Daten auf Richtigkeit überprüft wurden. Mit dem Einsatz im Rechtsverkehr gilt das Siegelzertifikat als angenommen.
- Das elektronische Siegel darf nicht weiter genutzt werden, wenn sich Änderungen an den Zertifikatsdaten (z.B. Änderung des Organisationsnamen) ergeben haben.
- Das Passwort für die Softwarezertifikate, welche das Authentisieren gegenüber der Bundesnotarkammer ermöglichen, ist geheim zu halten und nur an autorisierte Mitarbeitende der Organisation, jedoch nicht an unbefugte Dritte weiterzugeben.
- Der Bundesnotarkammer sind offenkundige Mängel oder Schäden am System oder Verfahren unverzüglich anzuzeigen (Störungsmeldung).
- Das elektronische Siegel darf nicht weiter genutzt werden, wenn bekannt ist, dass das Siegelzertifikat widerrufen/gesperrt wurde, das Wurzelzertifikat kompromittiert ist oder das Enddatum der Zertifikatsgültigkeit verstrichen ist.

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

10. Wie kann ich das Siegelzertifikat widerrufen/ sperren lassen?

Qualifizierte Siegelzertifikate können bereits vor dem Ende ihres Gültigkeitszeitraumes (7 Jahre) widerrufen bzw. gesperrt werden.

Die Sperrung kann auf Verlangen des Zertifikatinhabers (der Organisation) bzw. dem vertretungsberechtigten Antragsteller, als Sperrberechtigten verlangt werden.

Ein Widerrufs- bzw. Sperrverlangen kann der Bundesnotarkammer auf den folgenden Wegen übermittelt werden:

- telefonisch unter den Rufnummern:

  (0800) 3550 400 bzw. (0800) 3550 100;

Sperrberechtigte, die das Siegelzertifikat telefonisch sperren lassen wollen, müssen sich

a) durch Nennung des vereinbarten Widerrufkennworts sowie weiterer persönliche Angaben authentifizieren.

b) Nach der korrekten Angabe von Widerrufkennwort und persönlichen Daten wird zudem ein Einmallink zur Bestätigung des Sperrverlangens an die bei der Bunesnotarkammer hinterlegte E-Mail-Adresse geschickt.

- schriftlich;

mit eigenhändiger Unterschrift an folgende Anschrift:

Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln,

mit eigenhändiger Unterschrift oder qualifiziert signiert via E-Mail an die Zertifizierungsstelle der Bundesnotarkammer (zs@bnotk.de)

Ein schriftliches Sperrverlangen muss von der sperrberechtigten Person entweder eigenhändig unterschrieben oder qualifiziert elektronisch signiert sein. Das zu sperrende Siegelzertifikat muss durch Angaben zu Zertifikat und Zertifikatsinhaber eindeutig bestimmbar sein.

Nutzen Sie dafür bitte unser Sperrformular unter https://zertifizierungsstelle.bnotk.de/hilfe/downloads

Darüber hinaus muss der Bundesnotarkammer eine rechtsgültige Vertretungsmacht der juristischen Person vorgelegt werden. Dieser Nachweis kann in Form eines amtlichen Handelsregisterauszugs (nicht älter als 4 Wochen) oder einer gültigen

Vertretungsvollmacht erbracht werden.

Bitte beachten Sie, dass eine Sperrung des Zertifikats nicht rückgängig gemacht werden kann.

Unsere telefonische Sperrhotline ist rund um die Uhr an sieben Tagen die Woche über erreichbar. Die Sperrung des Siegelzertifikats erfolgt unmittelbar nach Prüfung, spätestens jedoch innerhalb von 24 Stunden.

Der Sperrung des 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 Zertifikats anzeigt.

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

Weitere Informationen, speziell zu den technischen und rechtlichen Hintergründen elektronischer Siegel erhalten Sie in folgenden Dokumenten:

- **Zertifikatsrichtlinie / Certificate Policy (CP)**

  Das CP stellt die Sicherheitsleitlinien für die Anforderungen und Vorgaben für die von der ZS betriebenen Public Key Infrastructure („PKI“) dar.

- **Zertifizierungskonzept / Certificate Practice Statement (CPS)**

  Das CPS stellt die Anforderungen der ZS an das Verfahren bei der Ausgabe, der Verwaltung, dem Widerruf sowie der Erneuerung, der von ihr ausgegebenen qualifizierten Zertifikate dar.

- **PKI Disclosure Statement für qualifizierte Zertifikate (PDS)**

  Das PDS fasst die jeweiligen Kernpunkte der CP/CPS zusammen und dient als Übersicht für die Offenlegungspflichten der ZS sowie die Pflichten der Zertifikatsinhaber.

12. Was geschieht mit meinen persönlichen Daten?

Die Bundesnotarkammer hält sich bei der Verarbeitung Ihrer personenbezogenen Daten streng an die gesetzlichen Bestimmungen der Europäischen Datenschutz-Grundverordnung 2016/679 (nachfolgend „DS-GVO“) und des Bundesdatenschutzgesetzes (nachfolgend „BDSG“). Ihre personenbezogenen Daten werden deshalb nur insoweit verarbeitet, wie dies gesetzlich erlaubt ist. Dies gilt auch für die Weitergabe Ihrer personenbezogenen Daten.

Die Bundesnotarkammer erhebt und verarbeitet personenbezogene Daten, soweit dies für die Erbringung, einschließlich der Prüfung und Sicherstellung der rechtlichen Gültigkeit, des jeweiligen Vertrauensdiensts, erforderlich ist. Diese Daten werden gem. Art. 24 Abs. 2 eIDAS-VO; §16 Abs. 4 VDG für die gesamte Dauer des Betriebes des VDA Bundesnotarkammer und über den Zeitraum ihrer Gültigkeit hinaus aufbewahrt. Die Bundesnotarkammer ergreift sämtliche erforderlichen Maßnahmen, um die personenbezogenen Daten der Anwender vor dem Zugriff Unbefugter zu schützen.

Kontakt zum Datenschutzteam der BNotK können Sie wie folgt aufnehmen:

Datenschutzbeauftragte

c/o Bundesnotarkammer

Mohrenstraße 34, 10117 Berlin

Telefon: +49 30 – 38 38 66 0

Telefax: +49 30 – 38 38 66 66

E-Mail: datenschutz@bnotk.de

Herausgeber:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln
Stand: Juli 2024