BUNDESDRUCKEREI

TEILNEHMERUNTERRICHTUNG GEMÄß SigG §6

Teilnehmerunterrichtung gemäß SigG §6– Dieses Dokument unterrichtet den Anwender einer elektronischen Signatur über die rechtlichen Folgen. Es gibt Hinweise zur Handhabung und stellt erste Schritte zur Problemlösung sowie Kontaktdaten zum Support bereit.

Version:	V1.13_PIN 3.0
Verantwortlich:	D-TRUST GmbH
Stand:	11.08.2016
Status:	freigegeben
Klassifizierung:	- öffentlich -

IMPRESSUM

Warenzeichen
Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

H**inweise**
Die D-TRUST GmbH haftet nicht für direkte oder indirekte Schäden, die sich aus der Verwendung dieses Dokuments ergeben oder damit in Beziehung stehen.

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin
Tel.: +49 (0) 30 25 98 - 0

INHALT

1 Diese Unterrichtungsunterlagen

Wir möchten, dass Sie über Ihre elektronische Signatur Bescheid wissen. Darauf legt auch das deutsche Signaturgesetz (SigG) Wert. Es verlangt, dass Sie eine Unterrichtung über den Gebrauch der elektronischen Signatur erhalten und dass Sie die Kenntnisnahme dieser Unterrichtung bestätigen[1].

Sie halten diese Unterrichtung in Gestalt dieses Textes in Händen. Bitte lesen Sie diese Unterrichtung sorgfältig.

2 Rechtsbelehrung

2.1 Wirkung der elektronischen Signatur im Rechtsverkehr

Mit der elektronischen Signaturkarte der D-Trust GmbH können Sie eine „qualifizierte elektronische Signatur“ erzeugen[2]. Das bedeutet: Wenn Sie mit Ihrer Signaturkarte ein elektronisches Dokument „elektronisch signieren“, so hat dies im Rechtsverkehr dieselbe Wirkung, als hätten Sie das gleichlautende Dokument mit Ihrer handschriftlichen Unterschrift versehen. Denn die „qualifizierte elektronische Signatur“ Ihrer Signaturkarte ist Ihrer handschriftlichen Unterschrift im Rechtsverkehr gleichgestellt. Eine Ausnahme von dieser Gleichstellung tritt nur dann ein, wenn ein Gesetz ausdrücklich etwas anderes bestimmt. Sie würden demzufolge vor Gericht im Zweifelsfall nicht abstreiten können, dass Sie eine elektronische Signatur geleistet haben. Ob Sie sie geleistet haben oder nicht, ist zweifelsfrei und rechtskräftig nachweisbar. Ebenso ist rechtskräftig nachprüfbar, ob das Dokument nach dem persönlichen Signieren noch verändert worden ist oder nicht.

2.2 Zur Rechtskraft der elektronischen Unterschrift

Jede Willenserklärung, die den üblichen gesetzlichen Voraussetzungen genügt (z.B. Geschäftsfähigkeit) und keiner besonderen gesetzlichen Formvorschrift unterliegt, ist rechtlich gültig. Im Rahmen der freien Beweiswürdigung ist ihr Niederschlag, z. B. als E-Mail, vor Gericht verwertbar.

---

[1] In Paragraph 6 des Signaturgesetzes ist die **Unterrichtungspflicht** formuliert:

(1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach Abs.1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und zu deren zuverlässiger Prüfung beizutragen. Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

(2) Der Zertifizierungsdiensteanbieter hat den Antragsteller darüber zu unterrichten, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschrift, wenn durch Gesetz nicht ein anderes bestimmt ist.

(3) Zur Unterrichtung nach Absatz 1 und 2 ist dem Antragsteller eine Belehrung in Textform zu übermitteln, deren Kenntnisnahme dieser als Voraussetzung für die Ausstellung eines qualifizierten Zertifikats in Textform zu bestätigen hat. Soweit ein Antragsteller bereits zu einem früheren Zeitpunkt nach den Absätzen 1 und 2 unterrichtet worden ist, kann eine erneute Unterrichtung unterbleiben.

[2] Vereinfacht ist in diesem Dokument auch von einer „digitalen Signatur“ oder „elektronischen Signatur“ die Rede; gemeint ist damit immer „qualifizierte elektronische Signatur“.

Die mit einer „qualifizierten elektronischen Signatur“ nach dem geltenden deutschen Signaturgesetz versehene Willenserklärung genügt darüber hinaus unter bestimmten Bedingungen auch der Formvorschrift „gesetzliche Schriftform“ und hat vor Gericht den Status eines „Anscheinsbeweises“:

- Gleichstellung: Nach §§126ff BGB ist die gesetzliche „qualifizierte elektronische Signatur“ der handschriftlichen Unterschrift der gesetzlichen Schriftform des Privatrechts gleichgestellt, wenn das signierte Dokument um den Namen des Unterzeichnenden ergänzt („elektronische Form“) und diese elektronische Form vom Gesetz nicht explizit ausgeschlossen wird. Ein solcher Ausschluss betrifft derzeit (Sept. 2001) die Kündigung und Änderung von Arbeitsverhältnissen (§623 BGB), die Erteilung von Arbeitszeugnissen (§630 BGB) sowie Leibrentenversprechen (§761 BGB), Bürgschaftserklärungen (§766 BGB), Versprechen (§780) und Anerkennungserklärungen (§781 BGB).
- §371a ZPO Beweiskraft elektronischer Dokumente

  Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

Das heißt: Wer die Möglichkeit hat, Ihre Signaturkarte zu benutzen, d.h. die Karte und die PIN besitz, kann rechtskräftig für Sie agieren, da er in Besitz Ihrer „digitalen Unterschrift“ ist. Jede mit Ihrem digitalen Signaturschlüssel erzeugte elektronische Signatur wird grundsätzlich Ihnen zugeordnet, falls

- Ihr Zertifikat zum Zeitpunkt der Erzeugung gültig war und
- nicht irgendwelche andere Fakten die Vermutung widerlegen, dass die elektronische Signatur von Ihnen willentlich erzeugt wurde.

3 Gültigkeit und Freischaltung von Zertifikaten

Die Zertifikate auf Ihrer qualifizierten Signaturkarte werden vom Zertifizierungsdiensteanbieter D-TRUST erst als „gültig“ für die Online-Prüfung (OCSP = online certificate status protocol) freigeschaltet, wenn Sie als Zertifikatsinhaber bestätigt haben, dass Sie Ihre Signaturkarte und den dazugehörigen PIN-Brief erhalten haben. Solange das Zertifikat noch nicht freigeschaltet ist, wird bei der Online-Prüfung der Status „Zertifikat unbekannt“ vom Zertifizierungsdiensteanbieter D-TRUST gemeldet.

Die Empfangsbestätigung für Karte und PIN-Brief kann schriftlich in Papierform oder elektronisch mittels SMS-TAN-Verfahren (Short-Message-Service – Transaktionsnummer) erfolgen.

Bei der schriftlichen Empfangsbestätigung senden Sie die unterschriebene Empfangsbestätigung für Karte und PIN-Brief an den Zertifizierungsdiensteanbieter D-TRUST. Ein Formular für die Empfangsbestätigung liegt dem PIN-Brief bei. Ihre Zertifikate werden nach Eingang und Prüfung der Empfangsbestätigung beim Zertifizierungsdiensteanbieter D-TRUST als „gültig“ für die Online-Prüfung freigeschaltet.

Bei der elektronischen Empfangsbestätigung können Sie, sobald Sie die Karte und den PIN-Brief erhalten haben, die Freischaltung Ihrer Zertifikate über das Kundenportal https://my.d-trust.net/freischalten elektronisch beantragen.

Dabei fordern Sie eine SMS-TAN an, die an Ihre Mobilfunknummer gesendet wird. Mit der SMS-TAN bestätigen Sie den Antrag zur Freischaltung Ihrer Zertifikate. War der elektronische Antrag erfolgreich, werden Ihre Zertifikate als „gültig“ für die Online-Prüfung freigeschaltet.

Sie erhalten in beiden Fällen eine E-Mail, wenn Ihre Zertifikate erfolgreich freigeschaltet wurden.

> **Hinweis zum SMS-TAN-Verfahren:**
>
> **Wenn Sie das SMS-TAN-Verfahren nutzen möchten, geben Sie bitte bei der Beantragung der Signaturkarte oder über das Kundenportal Ihre Mobilfunknummer an.**
>
> **Kundenportal:** https://my.d-trust.net/sms-tan

Bitte beachten Sie, dass zur Angabe oder Änderung der Mobilfunknummer über das Kundenportal ein speziell dafür erzeugtes Passwort (Registrierungsgeheimnis) verwendet werden muss. Dieses Passwort sendet Ihnen der Zertifizierungsdiensteanbieter D-TRUST auf Anfrage per Post an Ihre Meldeadresse.

> **Hinweis zum SMS-TAN-Verfahren:**
>
> **Das SMS-TAN-Verfahren wird nicht für alle Kunden mit externer Übergabestelle angeboten.**

4 Besonderheiten bei der Mehrfachsignaturkarte

Nach § 17 Abs. 2 SigG muss insbesondere bei der automatischen Erzeugung von Signaturen (Massensignaturen) sichergestellt sein, dass Signaturen nur zu dem voreingestell-

ten Zweck (z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können. Um die mit einer Mehrfachsignaturkarte erzeugten Signaturen in einem rechtsgültigen Rahmen vorzunehmen, sollte eine entsprechend geprüfte und zugelassene Anwendung eingesetzt werden. Des Weiteren ist der Anwender (Nutzer der Signaturkarte) dafür verantwortlich, dass die entsprechende Soft- und Hardware vor missbräuchlichem Zugriff geschützt, betrieben wird. Beachten Sie die Informationen im Dokument Einsatzbedingungen der Massensignaturkarte, welches Sie gemeinsam mit dem Antrag erhalten haben.

Zum Initialisieren der Signaturkarte muss der D-TRUST Card Assistant verwendet werden. Der D-TRUST Card Assistant besteht aus einer einzigen ausführbaren Datei. Mit dem D-TRUST Card Assistant können auch später die PINs jederzeit geändert werden.

5 Regeln für den Umgang mit der elektronischen Signatur

Es ist außerordentlich wichtig, dass Sie Ihre Signaturkarte und Ihre PIN mit größter Sorgfalt vor unbefugtem Zugriff schützen. Denn jeder, dem es möglich ist, Ihre Signaturkarte zu benutzen, kann rechtskräftig für Sie agieren. Ihre Signaturkarte enthält nicht nur Ihren digitalen Ausweis, sondern zugleich auch Ihre elektronische Unterschrift!

Wir haben einige Regeln für den sicheren Umgang mit der Signaturkarte zusammengestellt:

5.1.1 Die PIN

Bei den PINs handelt es sich um:

- die PIN1 (Card-PIN) für Authentifizierung und Verschlüsselung
- sowie die PIN2 (Signatur-PIN) für die Signatur. Die PIN2 ist im Auslieferungszustand durch eine Transport-PIN geschützt. Die Transport-PIN ist ein Sicherheitsmerkmal der Karte, welches Ihnen ermöglicht festzustellen, dass Ihr persönlicher Signaturschlüssel noch nie – und damit auch noch nie missbräuchlich - benutzt wurde. Vor der ersten Benutzung des Signaturschlüssels werden Sie dazu aufgefordert die PIN2 (siehe PIN-Brief, Signatur-PIN, 5 Stellen, nur Ziffern) zu ändern in **mindestens 6 Ziffern, empfohlen mindestens 8 Stellen, nur Ziffern!**
- Erst nach dieser Änderung ist es möglich, den Signaturschlüssel zu nutzen und damit eine Signatur auszuführen. Werden Sie bei der ersten Benutzung Ihrer Signaturkarte nicht zur Änderung der PIN2 aufgefordert oder wird die Ihnen mitgeteilte PIN2 nicht akzeptiert oder Ihre Transport-PIN mehr als 5 stellig ist, ist Ihre Signaturkarte möglicherweise nicht mehr unversehrt! Es besteht die Möglichkeit, dass je-

mand Ihre Signaturkarte benutzt hat, bevor sie Ihre Karte erhalten haben. PIN1 (Card-PIN) ist von dieser Regelung nicht betroffen.

Unser Supportcenter unterstützt Sie gern bei der Handhabung der PINs (Kontakt siehe letzte Seite).

5.1.2 Die PUK

Die Signaturkarten von D-TRUST, werden mit zwei so genannten PUKs ausgeliefert. Dabei handelt es sich um spezielle PINs, mit deren Hilfe Sie den Fehlbedienungszähler von PIN1 (Card-PIN) und PIN2 (Signatur-PIN) zurücksetzen können. Das bedeutet: Wurde eine der beiden PINs der Signaturkarte aufgrund einer dreimaligen Fehleingabe der entsprechenden PIN gesperrt (Fehlermeldung Karte: „Karte geblockt“), haben Sie durch die Eingabe der entsprechenden PUK die Möglichkeit, die Karte wieder zu entsperren. Eine Änderung der bestehenden PINs durch die Eingabe der PUK ist nicht möglich. Die Anzahl an Entsperrvorgängen durch die PUK ist auf 10 Versuche limitiert.

Kann die Karte nicht erfolgreich entsperrt werden, kann nur – kostenpflichtig – eine Austauschkarte beantragt werden.

Unser Supportcenter unterstützt Sie gern bei der Handhabung der PINs und PUKs (Kontakt siehe letzte Seite).

5.1.3 Persönlicher Gewahrsam

- Behalten Sie Ihre Signaturkarte stets in Ihrem persönlichen Gewahrsam!
- Mit Hilfe der PIN weisen Sie sich als rechtmäßiger Benutzer der Chipkarte aus. Halten Sie deshalb Ihre PINs unter allen Umständen geheim! Lassen Sie sich bei der Eingabe der PINs nicht beobachten. Falls Sie den Eindruck oder den Verdacht haben, dass die PIN bekannt ist, ändern Sie die PIN umgehend!
- Meiden Sie leicht zu erratende PINs (Geburtsdaten, Telefonnummern) und verwenden Sie nicht dieselbe PIN für Ihre Signaturkate, Ihren PC-Zugang, Ihr Online-Banking oder Ihre EC-Karte. Sie kämen damit möglichen Angreifern sehr entgegen.
- Benutzen Sie nicht die gleiche Ziffernfolge für die PIN2 (Signatur-PIN) und PIN1 (Card-PIN). Verwenden Sie unterschiedliche PINs. Besonders wichtig ist dies, wenn Sie die Signaturkarte auch in ungesicherten Umgebungen einsetzen.

5.1.4 Schutz der technischen Komponenten zur Signaturprüfung und -erstellung

- Für die Erzeugung von elektronischen Signaturen müssen „sichere Signaturerstellungseinheiten“ eingesetzt werden. Die Signaturkarte der D-Trust GmbH ist eine solche geprüfte und bestätigte sichere Signaturerstellungseinheit.

- Stellen Sie sicher, dass Sie stets sichere Anwendungsprogramme verwenden, denn diese sind geprüft und bestätigt und lassen Fälschungen der Signaturen und Verfälschungen von Dokumenten erkennen. Die aktuelle Version dieser Auflistung finden Sie im Internet auf den Seiten der Bundesnetzagentur (BNetzA) (http://www.bundesnetzagentur.de).
- Lassen Sie die Softwareprogramme Ihrer Signaturanwendungskomponenten unverändert und führen Sie nur Updates vom Hersteller der Signatursoftware aus: Nur so bleiben sie signaturgesetzkonform.
- Schützen Sie Ihren Computer vor unbefugtem Zugriff, z. B. durch einen Bootschutz. Achten Sie auf einen wirksamen Virenschutz, und vergewissern Sie sich vor dem Signieren, dass Ihr Gerät virenfrei ist. Wenn Veränderungen an der Signiersoftware durch Viren entstehen, so entspricht die Software nicht mehr den Anforderungen für qualifizierte Signaturen.
- Kartenleser mit integrierter Tastatur erreichen ein hohes Sicherheitsniveau und schützen Sie gegen Schadsoftware (Keylogger[3]).
- Im Bedarfsfall können Sie sich vergewissern, die richtige und unbeeinflusste Software des D-TRUST Card Assistant erhalten zu haben. Der Hashwert des D-TRUST Card Assistant wird im Downloadbereich angezeigt. Über ein Tool zum Erzeugen von Hashwerten, welches von der BNetzA[4] angeboten wird, können Sie sich davon überzeugen, dass der auf den D-TRUST Seiten angezeigte Hashwert des D-TRUST Card Assistant, mit dem von Ihnen erzeugten Hashwert der herunter geladenen Applikation des D-TRUST Card Assistant übereinstimmt. Bei der Einrichtung dieses Tools unterstützt Sie unser Support im Bedarfsfall gern.

5.1.5 Notwendigkeit zur Signaturerneuerung

Wenn ein Dokument über einen längeren Zeitraum eine elektronische Signatur trägt, kann die Nachprüfbarkeit der Signatur durch Ablauf der Gültigkeit oder Sperrung des Signaturzertifikats unsicher werden. Deshalb müssen solche Daten rechtzeitig unter Verwendung der jeweilig modernsten Signaturtechnologie erneut elektronisch signiert werden. Diese neue elektronische Signatur bezieht dabei die vorangegangene Signatur und den aktuellen Zeitstempel ein.

[3] Keylogger zeichnen die Eingabe über die Tastatur auf.
[4] www.bundesnetzagentur.de

6 Signaturerzeugung (Signaturbildung) und Signaturprüfung

6.1 Signaturerzeugung

Überprüfen Sie vor der Signaturbildung den Inhalt des digitalen Dokuments mit Hilfe der Darstellungskomponente, die bei der Signaturbildung automatisch geöffnet wird. Diese Darstellungskomponente muss Bestandteil einer geprüften und bestätigten Software zur digitalen Signatur sein. Anderenfalls ist nicht gewährleistet, dass Sie wirklich den maßgeblichen – nämlich den signierten – Wortlaut erhalten. Wenn Sie den Inhalt bestätigen und signieren wollen, müssen Sie die PIN2 (Signatur-PIN) Ihrer Signaturkarte eingeben. Damit ist die Signierung abgeschlossen.

Bei nicht geprüfter Signaturanwendungssoftware besteht das Risko, dass z.B. verborgene Texte in das Dokument eingefügt werden, ohne dass Sie es merken.

6.2 Signaturprüfung

Zur Überprüfung der elektronischen Signatur benötigt Ihre Signaturprüfsoftware den Signaturprüfschlüssel des Absenders. Dieser Signaturprüfschlüssel befindet sich im Zertifikat des Absenders, das mit der signierten Nachricht mitgeschickt wird.

Selbsttätig überprüft die Signatursoftware die Gültigkeit und die Herkunft des Zertifikates sowie die Unversehrtheit der signierten Daten und gibt das Ergebnis der Prüfung in einer Meldung aus. Der rechtlich maßgebliche Inhalt des Dokumentes wird dabei wieder in einer Darstellungsweise angezeigt, die Bestandteil Ihrer Signaturanwendungssoftware ist und gegen unbemerkte Manipulation gesichert ist. Diese Prüfung kann lokal ohne Internetanschluss durchgeführt werden.

Wollen Sie sich vergewissern, dass das Zertifikat noch gültig und nicht gesperrt ist, so können Sie mit einer bestätigten Signaturanwendungssoftware auch eine Online-Prüfung des Zertifikats beim Zertifizie-rungsdiensteanbieter vornehmen. Dazu führen Sie entweder einen Abgleich der Sperrlisten (CRL) oder eine OCSP – Abfrage durch, bei der angezeigt wird, ob das Zertifikat zum aktuellen Zeitpunkt gültig, gesperrt oder unbekannt ist (siehe auch SigV §15 Absatz 2 Punkt 2). Die Adresse der gültigen Sperrliste oder des OCSP-Pfades können Sie dem jeweiligen Zertifikat entnehmen. Wir empfehlen, die OCSP Methode bevorzugt zu verwenden.

Die Sicherheit Ihrer Signaturanwendungssoftware ist nur gewährleistet, wenn Sie Ihren Computer und das Betriebssystem gegen Bedrohungen absichern. Dazu verwenden Sie insbesondere Virenschutzprogramme in der jeweils aktuellsten Version.

7 Sperrung von Zertifikaten

7.1.1 Sperrgründe

Lassen Sie Ihre Signaturkarte sperren,

- wenn Sie Ihre Karte verloren haben oder wenn Sie den Verdacht haben, dass Ihre Karte von Dritten manipuliert worden sein könnte.
- wenn Angaben im Zertifikat ungültig werden, z. B. in Folge einer Namensänderung oder dem Ausscheiden aus der im Zertifikat angegebenen Organisation, sollten Sie ebenfalls eine Sperrung veranlassen.
- wenn Sie Ihre Signaturkarte nicht mehr benötigen (auch nicht zum Entschlüsseln von Dokumenten). Sie können die Signaturkarte unbrauchbar machen, indem Sie die Zertifikate durch mehrfach falsche PIN-Eingabe (siehe Kapitel 5) unbrauchbar machen oder den Chip auf der Karte mechanisch zerstören.

7.1.2 Sperrgründe des Zertifizierungsdiensteanbieters

Wenn der Zertifikatinhaber seinen vertraglichen Pflichten nicht nachkommt, kann der Zertifizierungsdiensteanbieter die Karte sperren.

Weiterhin kann der Zertifizierungsdiensteanbieter Ihre Signaturkarte sperren, wenn die Signaturfunktion aus technischen Gründen nicht mehr als sicher betrachtet werden kann.

7.1.3 Sperrverfahren

Sie haben drei Möglichkeiten, Ihr Zertifikat sperren zu lassen:

- Entweder Sie rufen die Hotline unseres Sperrdienstes an: 030 / 25 93 91 – 600. Der telefonische Sperrdienst ist, wie es das Signaturgesetz verlangt, rund um die Uhr besetzt.
- Sie richten einen schriftlichen Sperrauftrag an unseren Sperrdienst. Senden Sie diesen an die folgenden Adresse: Bundesdruckerei GmbH c/o D-TRUST GmbH, Kommandantenstraße 15, 10969 Berlin.
- Oder Sie beantragen die Sperrung elektronisch mit SMS-TAN-Verfahren über das Kundenportal: https://my.d-trust.net/sperren

Wenn Sie die Sperrung telefonisch über die Hotline beantragen, dann weisen Sie sich als sperrberechtigt aus, indem Sie das Sperrpasswort nennen, das Sie im Rahmen der Antragstellung gewählt haben. Wird das Sperrpasswort korrekt genannt, wird die Sperrung unverzüglich durchgeführt.

Wenn Sie die Sperrung schriftlich vornehmen, wird Ihre Sperrberechtigung anhand Ihrer persönlichen Angaben und Ihrer handschriftlichen Unterschrift überprüft. Als Unterschriftenprobe dient dazu die Unterschrift, die Sie im Rahmen der Antragstellung geleistet haben. Die Sperrung wird an dem Tag durchgeführt, an dem das Schreiben beim Sperrdienst der D-Trust GmbH eingetroffen ist. Sie können in dem Schreiben auch ein in der Zukunft liegendes Datum nennen, zu dem die Sperrung vorgenommen werden soll. Eine rückwirkende Sperrung ist dagegen nicht möglich. Eine vorübergehende Sperrung ist vom Signaturgesetz ausgeschlossen, da eine einmal vorgenommene Sperrung nicht rückgängig gemacht werden kann.

Bei der Sperrung mit SMS-TAN fordern Sie über das Kundenportal eine SMS-TAN an, die an Ihre Mobilfunknummer gesendet wird. Mit der SMS-TAN bestätigen Sie den Antrag zur Sperrung. War der elektronische Antrag erfolgreich, werden Ihre Zertifikate als „gesperrt“ veröffentlicht.

Hinweis zum SMS-TAN-Verfahren:

Für die Sperrung mit SMS-TAN-Verfahren, muss zuvor Ihre Mobilfunknummer beim Zertifizierungsdiensteanbieter D-TRUST hinterlegt werden. Sie können Ihre Mobilefunknummer gleich bei der Beantragung der Signaturkarte oder nachträglich über das Kundenportal angeben.

Kundenportal: https://my.d-trust.net/sms-tan

Hierüber ist auch eine Änderung der Mobilfunknummer möglich. Bitte beachten Sie unbedingt, dass zur Angabe oder Änderung der Mobilfunknummer über das Kundenportal ein speziell dafür erzeugtes Passwort (Registrierungsgeheimnis) verwendet werden muss. Dieses Passwort sendet Ihnen der Zertifizierungsdiensteanbieter D-TRUST auf Anfrage per Post an Ihre Meldeadresse.

Wenn in Ihrem Zertifikat weitere Angaben aufgenommen werden, durch die dritte Personen involviert sind, so sind auch diese berechtigt, Ihr Zertifikat sperren zu lassen. Angenommen, in Ihrem Zertifikat ist angegeben, dass Sie die Vertretungsvollmacht für Ihren Lebenspartner besitzen, dann ist Ihr Lebenspartner gemäß Signaturgesetz berechtigt, Ihr Zertifikat sperren zu lassen.

Folgende Angaben müssen für eine Sperrung angegeben werden:

Telefonischer Sperrauftrag	Schriftlicher Sperrauftrag	Elektronischer Sperrauftrag
▸ Name des Anrufers ▸ Name des Zertifikatinhabers, falls nicht Anrufer selbst ▸ wenn möglich Antrags-/Karten-ID ▸ Sperrpasswort	▸ Name des Absenders ▸ Name des Zertifikatinhabers, falls nicht Absender selbst ▸ wenn möglich Antrags-/Karten-ID ▸ wenn möglich Sperrpasswort ▸ Unterschrift des Absenders ▸ gewünschter Sperrzeitpunkt	▸ Nachname des Zertifikatsinhabers ▸ Antrags-/Karten-ID ▸ SMS-TAN

8 Möglichkeiten zu Beschränkungen des qualifizierten Zertifikats

Das qualifizierte Signaturzertifikat kann monetäre Beschränkungen, Beschränkungen nach Art und Umfang sowie Zusatzinfomationen beinhalten. Wenn in Ihrem Zertifikat Beschränkungen nach Art oder Umfang enthalten sind und für die Verwendung eines von Ihnen signierten Dokumentes diese Beschränkungen (beispielsweise „monetäre Beschränkungen“, d.h. finanzielle Obergrenzen) von Bedeutung sind, dann müssen Sie Ihr Zertifikat dem Dokument hinzufügen und es in die elektronische Signatur einschließen.

8.1.1 Monetäre Beschränkung

Sie können im Zertifikat festhalten, dass die Signatur nur für Verträge gültig ist, deren Gegenwert unterhalb eines gewissen Betrages liegt (monetäre Beschränkung).

8.1.2 Beschränkungen nach Art und Umfang

Freier Text, der zur Beschränkung des Zweckes der Signatur aufgenommen werden kann.

Beispiel: Dieses Zertifikat gilt nur zur Signatur von elektronisch versandten Rechnungen der XY GmbH.

8.1.3 Zusatzinformationen

Freier Text bis zu 2048 Zeichen, z. B. akademischer Titel (Diplom-Ingenieur, Diplom-Volkswirt).

9 Datenschutz

D-Trust unterliegt wie alle Zertifizierungsdiensteanbieter den gesetzlichen Datenschutzbestimmungen. Die Daten eines Zertifikats können im Verzeichnisdienst nur dann von jedermann abgerufen werden, wenn der Zertifikatsinhaber dies bei der An-

tragstellung ausdrücklich gewünscht hat. Anderenfalls ist nur der Status des Zertifikats nachprüfbar: „gültig“, „unbekannt“ oder „ungültig“ („gesperrt“).

D-Trust erhebt keine Daten, die nicht für die Zertifizierungstätigkeit notwendig sind. Die erhobenen Daten werden vor dem Zugriff Unbefugter geschützt. Die dazu erforderlichen Maßnahmen ergreift der Zertifizierungsdiensteanbieter. Eine Weitergabe der persönlichen Daten erfolgt nur auf gerichtliche Anweisung. Die zur Verfügung gestellten Daten nutzt die D-Trust GmbH nur innerhalb ihres Zertifizierungsbetriebes. Eine weitergehende kommerzielle Nutzung findet nicht statt.

Das Signaturgesetz (§10, Absatz 2) schreibt vor, dass dem Zertifikatsinhaber „auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren“ ist.

10 Die freiwillige Akkreditierung des Zertifizierungsdiensteanbieters

Über die strengen Anforderungen hinaus, die eine Zertifizierungsstelle nach dem Signaturgesetz erfüllen muss, kann eine Zertifizierungsstelle ihre technischen Komponenten und ihre Abläufe von einer zugelassenen Stelle prüfen lassen. Wenn eine solche Prüfung erfolgreich durchgeführt wurde, kann die Bundesnetzagentur den Zertifizierungsdiensteanbieter akkreditieren. Der D-Trust GmbH wurde die Akkreditierungsurkunde im März 2002 ausgehändigt. Weiterhin bietet die D-Trust GmbH sowohl qualifizierte Zertifikate mit als auch ohne Anbieterakkreditierung an. Der Schlüssel, mit dem der Zertifizierungsdiensteanbieter D-Trust GmbH etwa in seinem akkreditierten Betrieb Zertifikate seiner Kunden signiert, ist von der Bundesnetzagentur zertifiziert und damit Bestandteil des Zertifikats, das die Bundesnetzagentur der D-Trust GmbH ausgestellt hat. So wie Sie im Verzeichnisdienst der D-Trust GmbH eine Anfrage nach Zertifikaten starten können, die diese ausgestellt hat, so können Sie im Verzeichnisdienst der Bundesnetzagentur eine Anfrage zu Zertifikaten stellen, die die Bundesnetzagentur akkreditierten Zertifizierungsdiensteanbietern wie der D-Trust GmbH ausgestellt hat. Sind Sie im Besitz eines Zertifikats mit Anbieterakkreditierung, lässt sich Ihr Zertifikat wie jedes qualifizierte Zertifikat in der ersten Stufe durch den Verzeichnisdienst des Zertifizierungsdiensteanbieters, z. B. D-Trust, verifizieren, in einer zweiten Stufe kann das Zertifikat des Zertifizierungsdiensteanbieters jedoch zusätzlich durch den Verzeichnisdienst der Bundesnetzagentur überprüft werden. Dadurch wird das Vertrauen in Ihr Zertifikat zusätzlich gestärkt.

D-Trust führt die ausgestellten qualifizierten Zertifikate in einem Verzeichnis ab dem Zeitpunkt ihrer Freischaltung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre (30 Jahre für ein Zertifikat aus der Vertrauenskette der BNetzA) ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifi-

kats endet. Im Falle der Einstellung des Betriebs ist gesetzlich gesichert, dass Dokumentation und Zertifikate von einem Dritten übernommen werden.

11 Beschwerde- und Schlichtungsverfahren

Sollten Sie Probleme oder Fragen haben, die Sie nicht einvernehmlich mit unserem Support klären konnten, haben Sie die Möglichkeit die Bundesnetzagentur als Ansprechpartner für Beschwerde- und Schlichtungsverfahren sowie zu Einzelheiten der Inanspruchnahme solcher Verfahren zu befragen.

12 Hinweise zu Postident-Basic- und Postident-Special-Verfahren

Informationen zu den Verfahren Postident Basic und Postident Special finden Sie auf den Webseiten der D-Trust GmbH unter https://www.d-trust.net/internet/files/Postident_info.pdf.

13 Hinweise zum Notarident-Verfahren

Suchen Sie bitte mit Ihrem noch nicht unterschriebenen Antragsformular einen Notar auf, weisen sich mit Ihrem Personalausweis oder Reisepass aus und unterschreiben Sie das Antragsformular in seiner Gegenwart. Lassen Sie sich vom Notar beglaubigen, dass Sie persönlich das Antragsformular unterschrieben haben (BNotO §20 (1)). Die Beglaubigung senden Sie dann zusammen mit den restlichen Antragsunterlagen an die untenstehende Adresse der D-Trust GmbH. Die Kosten für das Verfahren sind in der Kostenordnung (KostO) festgelegt und von Ihnen selbst zu tragen. Eine Kostenübernahme durch die D-Trust GmbH ist nicht möglich.

14 Kontakte

Wichtige Adressen	
Ihr Zertifizierungsdiensteanbieter: D-Trust GmbH Kommandantenstraße 15 10969 Berlin Tel.: + 49 (0) 30 / 25 93 91 – 0 Fax: + 49 (0) 30 / 25 93 91 –22 info@D-TRUST.net www.D-TRUST.net	**Ihr Vertriebskontakt:** Bundesdruckerei GmbH Kommandantenstraße 18 10969 Berlin Tel.: + 49 (0) 30 / 25 98 - 0 info@bdr.de support@bdr.de www.bundesdruckerei.de
Kundenportal für SMS-TAN: https://my.d-trust.net/sms-tan	
Sperrhotline: Tel.: + 49 (0) 30 / 25 93 91 – 600	