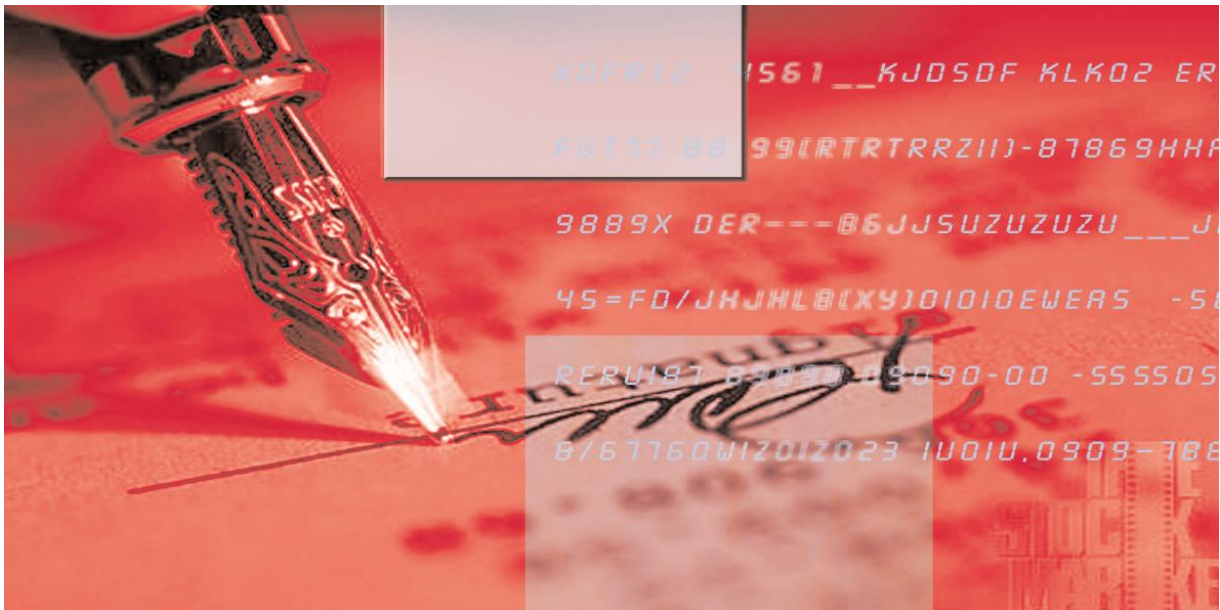




Unterrichtungsunterlagen nach § 6 Signaturgesetz



Wichtige Informationen zum Einsatz der qualifizierten elektronischen Signatur nach dem Signaturgesetz

Inhaltsverzeichnis

1	<i>EINLEITUNG</i>	<i>III</i>
2	<i>ARTEN ELEKTRONISCHER SIGNATUREN</i>	<i>III</i>
3	<i>FUNKTIONSWEISE EINER ELEKTRONISCHEN SIGNATUR</i>	<i>III</i>
4	<i>RECHTLICHE BEDEUTUNG DER ELEKTRONISCHEN SIGNATUR</i>	<i>III</i>
5	<i>SICHERHEITSVORKEHRUNGEN FÜR DEN EINSATZ IHRER SIGNATURKARTE</i>	<i>IV</i>
5.1	Eingesetzte Anwendungsumgebung	<i>IV</i>
5.2	Einmalpasswort, PIN-Handling und Kartenverwendung	<i>V</i>
5.3	Besondere Sicherheitsvorkehrungen beim Einsatz von Massensignaturkarten	<i>VI</i>
6	<i>PRÜFUNG UND ARCHIVIERUNG VON SIGNIERTEN DOKUMENTEN</i>	<i>VI</i>
6.1	Signaturprüfung	<i>VI</i>
6.2	Archivierung	<i>VII</i>
7	<i>SPERRUNG VON ZERTIFIKATEN</i>	<i>VII</i>
8	<i>BESCHRÄNKUNG DER NUTZUNG DES SIGNATURSCHLÜSSELS</i>	<i>VIII</i>
	<i>DURCH DERARTIGE BESCHRÄNKUNGEN WIRD DIE EINSATZFÄHIGKEIT DES ZERTIFIKATS BEGRENZT. ACHTEN SIE STETS DARAUFG, DASS DAS DIE BESCHRÄNKUNGEN ENTHALTENE ZERTIFIKAT DEN ZU SIGNIERENDEN DATEN BEIGEFÜGT UND IN DIE ELEKTRONISCHE SIGNATUR EINGESCHLOSSEN IST.</i>	<i>VIII</i>
9	<i>AUFNAHME EINES PSEUDONYMS AN STELLE DES NAMENS IN DAS ZERTIFIKAT</i>	<i>VIII</i>
10	<i>MÖGLICHKEIT ZUR FREIWILLIGEN ANBIETER-AKKREDITIERUNG</i>	<i>IX</i>
11	<i>ANSPRECHPARTNER BEI FRAGEN</i>	<i>X</i>
12	<i>WEITERFÜHRENDE INFORMATIONEN</i>	<i>X</i>

1 Einleitung

Mit der Entscheidung zum Bezug qualifizierter Signaturleistungen von S-TRUST eröffnen Sie sich neue Möglichkeiten für die elektronische Abwicklung von Rechtsgeschäften z.B. im Internet.

Dieses Dokument informiert Sie entsprechend den gesetzlichen Anforderungen nach § 6 Signaturgesetz und § 6 Signaturverordnung über alle wichtigen Belange bezüglich einer qualifizierten elektronischen Signatur, wie z.B. die Funktionsweise und rechtliche Bedeutung, und gibt Ihnen wichtige Tipps für deren Verwendung.

2 Arten elektronischer Signaturen

Das Signaturgesetz unterscheidet folgende Arten elektronischer Signaturen:

- „elektronische Signaturen“ (§ 2 Nr. 1 SigG)
- „fortgeschrittene elektronische Signaturen“ (§ 2 Nr. 2 SigG)
- „qualifizierte elektronische Signaturen“ (§ 2 Nr. 3 SigG)
- „qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung“ (§ 2 Nr. 3, 15 Abs. 1 Satz 4 SigG)

Besondere gesetzliche Regelungen bestehen nur für die „qualifizierten elektronischen Signaturen“ und die „qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung“. Nur diese können die gesetzliche Schriftform ersetzen (vgl. Nr. 4).

3 Funktionsweise einer elektronischen Signatur

Mittels mathematischer Methoden und des darauf aufsetzenden Public-Key-Verfahrens können digitale Dokumente elektronisch unterzeichnet, verschlüsselt und überprüft werden. Technisch basieren elektronische Signaturen auf zwei Schlüsseln: einem privaten Schlüssel (Signaturschlüssel) und einem (eindeutig) dazugehörigen öffentlichen Schlüssel (Signaturprüfchlüssel). Mit dem öffentlichen Schlüssel können elektronische Signaturen überprüft werden, die mit dem privaten Schlüssel erzeugt wurden. Dieses asymmetrische kryptografische Verfahren erlaubt es, den öffentlichen Schlüssel für jedermann zugänglich zu machen, ohne anderen Personen das Signieren mit dem privaten Schlüssel zu ermöglichen. Ein elektronisches Zertifikat bestätigt dabei die Zuordnung des öffentlichen Schlüssels zu einer bestimmten Person. Dadurch kann der Inhaber des privaten Schlüssels, mit dem die Signatur erzeugt wurde, eindeutig identifiziert werden. Gleichzeitig ist es möglich, die Integrität (Vollständigkeit und Unverändertheit) der signierten Information zu überprüfen.

4 Rechtliche Bedeutung der elektronischen Signatur

Mit der Verabschiedung des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) hat der Gesetzgeber die nötigen Rahmenbedingungen geschaffen, die elektronische Unterschrift (Signatur) der eigenhändigen Unterschrift in ihrer rechtlichen Bedeutung gleichzustellen.

Nach § 126 Abs. 3 BGB kann die gesetzliche Schriftform (eigenhändige Namensunterschrift) durch die elektronische Form ersetzt werden, wenn sich aus dem jeweiligen Gesetz nichts anderes ergibt.

Es bestehen jedoch einige Ausnahmen. Nicht in elektronischer Form möglich sind z.B. Verbraucherdarlehensverträge (§ 492 Abs. 1 Satz 2 BGB), die Kündigung von Arbeitsverhältnissen (§ 623 BGB), die Erteilung eines Arbeitszeugnisses (§ 630 Satz 3 BGB), eine Bürgschaftserklärung (§ 766 Satz 2 BGB), ein Schuldversprechen (§ 780 BGB) sowie ein Schuldanerkennnis (§ 781 BGB). Ist eine notarielle Beglaubigung oder Beurkundung erforderlich, genügt die elektronische Form ebenso nicht (z.B. Grundstücksgeschäfte).

5 Sicherheitsvorkehrungen für den Einsatz Ihrer Signaturkarte

Qualifizierte Signaturanwendungen verfügen über einen hohen Sicherheitsstandard. Damit diese Sicherheit nicht beeinträchtigt wird, müssen bestimmte Regeln beachtet werden. Denn wer im Besitz der Signaturkarte und der PIN ist, kann vortäuschen, die angegebene Person zu sein.

5.1 Eingesetzte Anwendungsumgebung

Zu Ihrer Sicherheit und Ihrem eigenen Schutz empfehlen wir, Ihre Signaturkarte nur auf Systemen zu verwenden, deren Zuverlässigkeit und Vertrauenswürdigkeit Ihnen bekannt ist.

Schützen Sie Ihren PC vor unbefugtem Zugriff:

- Vergewissern Sie sich, dass sich keine Viren auf Ihrem PC befinden, ehe Sie qualifizierte elektronische Signaturen erzeugen.
- Verwenden Sie regelmäßig aktualisierte Firewall- und Virenschutzsoftware.
- Installieren Sie regelmäßig Updates und Sicherheitspatches für Ihr jeweiliges Betriebssystem und Ihren Internetbrowser.
- Weitere Schutzempfehlungen finden Sie auf den Internetseiten <http://www.bsi.de/> des Bundesamtes für Sicherheit in der Informationstechnologie unter <http://www.bsi.de>

Ferner empfehlen wir die ausschließliche Verwendung von signaturgesetzkonformen Signaturanwendungskomponenten unter Beachtung der zugehörigen Einsatzbedingungen. Signaturanwendungskomponenten sind Geräte und Programme, die von einer anerkannten Prüf- und Bestätigungsstelle evaluiert und bestätigt und somit als den gesetzlichen Anforderungen entsprechend eingestuft wurden. Dies gilt insbesondere für den Chipkartenleser. Eine aktuelle Geräte- und Programmliste finden Sie auf den Internet-Seiten der Bundesnetzagentur unter <http://www.bundesnetzagentur.de>.

Integritätsprüfung von Signaturanwendungssoftware: Jede Software ist korrumpierbar. Wir empfehlen daher dringend, Signaturanwendungssoftware nach deren Installation auf ihre Integrität zu prüfen. Sollten Sie auf einer CD- oder DVD-ROM eine Signaturanwendungssoftware erhalten, ist ein ggf. vorhandenes Verpackungssiegel auf Unversehrtheit zu prüfen. Ist das Siegel gebrochen, dürfen Sie die Software nicht verwenden.

Sollte die CD- oder DVD-ROM über kein Siegel verfügen oder Sie die Software downloaden oder in sonstiger Weise erhalten, ist die Signaturanwendungssoftware nach deren Installation sowie in regelmäßigen Abständen online auf ihre Integrität zu prüfen. Die Anbieter der jeweiligen Signaturanwendungssoftware halten hierzu über das Internet Prüfprogramme zum Abruf bereit, über die Sie die Prüfung online durchführen können.

5.2 Einmalpasswort, PIN-Handling und Kartenverwendung

Ihr persönliches Einmalpasswort dient beim Vorgang des Zertifikatsdownloads der Authentifizierung Ihrer Person. Das Passwort ist daher nur für Ihre eigene Verwendung bestimmt und muss geheim gehalten werden.

Auf der Signaturkarte („sichere Signaturerstellungseinheit“, vgl. Definition § 2 Nr. 10 SigG) befinden sich die persönlichen Schlüssel zur Erzeugung elektronischer Signaturen, d.h. Ihrer elektronischen Unterschrift. Ihre Karte ist daher von Ihnen persönlich diebstahlsicher zu verwahren.

Sollten Sie Ihre Karte verlieren oder diese Ihnen abhanden kommen, ist umgehend das jeweilige Zertifikat zu sperren. Siehe dazu Kap. 7 „Sperrung von Zertifikaten“.

Ihre Karte wird mit einer 5-stelligen Transport-PIN für die Signaturfunktion ausgeliefert, die beim ersten Zugriff auf den Signaturschlüssel abgefragt wird. Hierbei ist zu prüfen, ob Ihre Karte mit dieser 5-stelligen Transport-PIN geschützt ist, da nur dann sichergestellt werden kann, dass mit dem Signaturschlüssel noch keine Signaturen erzeugt wurden. Sie müssen nach Eingabe Ihrer Transport-PIN selbstständig zwei PINs für die Karte vergeben:

1. Signatur-PIN für Ihren Signaturschlüssel zur Erzeugung einer qualifizierten elektronische Signatur
2. CSA-PIN für Ihren Verschlüsselungs-/Authentisierungsschlüssel

Achten Sie bei der Wahl Ihrer Signatur-PIN und Ihrer CSA-PIN darauf, dass diese rein zufällige Zahlenkombinationen darstellen, die nicht in Verbindung mit Ihrem persönlichen Umfeld (Geburtsdaten oder Telefonnummern etc.) stehen und dadurch leicht erraten werden könnten. Vermeiden Sie es ferner, denselben Wert für beide Geheimnisse zu verwenden, da auch dadurch die Gefahr eines Missbrauchs vergrößert wird. Die Mindestlänge der Signatur-PIN und der CSA-PIN beträgt 6 Stellen. Eine Rückkehr zu einer Transport-PIN ist nicht möglich.

Halten Sie Ihre Signatur-PIN und Ihre CSA-PIN streng geheim. Besteht der Verdacht, dass sie erraten oder ausgespäht wurden, ändern Sie diese umgehend. Überprüfen Sie, ob die Karte mit Ihren persönlichen Schlüsseln sich ununterbrochen in Ihrem Besitz befunden hat und befindet. In Zweifelsfällen sperren Sie bitte Ihre Zertifikate (siehe hierzu Kap. 7 „Sperrung von Zertifikaten“).

Überprüfen Sie vor jedem Signieren den Inhalt der Daten, die signiert werden sollen. Verwenden Sie hierzu Software, die sicherstellt, dass sämtliche Daten, die signiert werden sollen, vollständig angezeigt werden.

Die Nutzungsmöglichkeit des Signaturschlüssels wird gesperrt, wenn die Signatur-PIN dreimal hintereinander falsch eingegeben wird. Die Möglichkeit zur Nutzung ist dann endgültig gesperrt. Eine Entsperrung ist nicht möglich. Die Karte kann für die Erstellung von qualifizierten elektronischen Signaturen nicht mehr verwendet werden.

Beschädigungen der Signaturkarte oder ein Funktionsversagen der Karte können Hinweise auf eine Verletzung der Geheimhaltung von Schlüssel- oder Passwortdateien sein. In diesen Fällen ist unverzüglich mit dem zuständigen Zertifizierungsdiensteanbieter Kontakt aufzunehmen.

5.3 Besondere Sicherheitsvorkehrungen beim Einsatz von Massensignaturkarten

Massensignaturkarten können bei einmaliger Eingabe der zugehörigen Identifikationsdaten (PIN) eine Vielzahl elektronischer Signaturen erzeugen. Bei Verwendung von Massensignaturkarten besteht insbesondere die Gefahr, dass Dokumente versehentlich signiert werden. Es sind daher besondere Schutzmaßnahmen und besonders hohe Anforderungen an die Sicherheit und Integrität der Einsatzumgebung (Hard- und Software) zu beachten (siehe hierzu auch 5.1).

Wie viel und welche Dokumente signiert werden, wird ausschließlich durch die Signaturanwendungskomponente (Software) gesteuert. Dafür ist eine besondere, für Massensignaturverfahren geeignete und von einer nach dem Signaturgesetz anerkannten Prüf- und Bestätigungsstelle evaluierte und bestätigte Signaturanwendungskomponente einzusetzen. Zu Ihrer Sicherheit empfehlen wir Ihnen, vor Einsatz von Massensignaturkarten sich mit den Anforderungen an die Einsatzumgebung sowie der Funktionsweise der jeweiligen Signaturanwendungskomponente sorgfältig vertraut zu machen.

Vor jeder Eingabe der Identifikationsdaten (PIN) zur Erzeugung einer elektronischen Signatur sind die zu signierenden Dokumente auszuwählen und sorgfältig zu prüfen, damit keine Dokumente unbeabsichtigt signiert werden.

Eine mit einer Massensignaturkarte erzeugte Signatur ist von einer Signatur, die mittels einer sicheren Signaturerstellungseinheit, bei der zur Erzeugung von jeweils lediglich einer einzelnen Signatur die Eingabe Ihrer Identifikationsdaten erforderlich ist, nicht zu unterscheiden.

Angesichts der erheblich größeren Missbrauchsmöglichkeiten bei Massensignaturkarten sollten diese besonders sorgfältig und sicher verwahrt und vor unberechtigtem Zugriff (physisch) geschützt eingesetzt werden. Dies gilt auch für die Identifikationsdaten.

6 Prüfung und Archivierung von signierten Dokumenten

6.1 Signaturprüfung

Zur Überprüfung signierter Daten benötigen Sie als Empfänger neben einer geeigneten Signaturprüfsoftware den öffentlichen Signaturprüf Schlüssel des Signaturschlüsselinhabers. Der Signaturprüf Schlüssel ist im Zertifikat des Signaturschlüsselinhabers enthalten, das in der Regel dem signierten Dokument beigelegt ist.

Prüfen Sie jedes empfangene, signierte Dokument auf

1. Gültigkeit der Unterschrift (mathematische Signaturprüfung – damit können auch Veränderungen an den übermittelten Daten festgestellt werden)
2. Gültigkeit des dazugehörigen Zertifikats (nicht gesperrt oder abgelaufen)

Die Überprüfung der Gültigkeit des dazugehörigen Zertifikats sollte online im Verzeichnisdienst des Zertifizierungsdiensteanbieters durchgeführt werden. S-TRUST empfiehlt eine Verifikation der Gültigkeit des verwendeten Zertifikats sowohl auf den Zeitpunkt der Erstellung der Signatur als auch auf den Empfangszeitpunkt der signierten Daten. Nähere Informationen zum Verzeichnisdienst von S-TRUST finden Sie auf <https://www.s-trust.de>.

Prüfen Sie ferner, ob das Zertifikat Beschränkungen (vgl. unter Nr. 8) oder sonstige Attribute enthält, die im Zusammenhang mit den signierten Daten von Bedeutung sein könnten.

6.2 Archivierung

Elektronische Signaturen basieren auf mathematischen Verfahren, die mit der steigenden Leistungsfähigkeit von Computersystemen mit der Zeit an Sicherheit verlieren. Die mathematischen Verfahren werden daher regelmäßig überprüft und soweit nötig den veränderten Gegebenheiten angepasst. Die Bundesnetzagentur teilt die Anforderungen an die mathematischen Verfahren sowie den Zeitpunkt mit, bis zu dem diese als geeignet gelten. S-TRUST überprüft wie jeder andere qualifizierte Zertifizierungsdiensteanbieter die verwendeten mathematischen Verfahren regelmäßig und passt sie ggf. den neuen Anforderungen an. Ein von S-TRUST ausgestelltes qualifiziertes Zertifikat ist nie länger gültig, als die dafür verwendeten mathematischen Verfahren nach Angaben der Bundesnetzagentur als sicher gelten.

Es ist daher erforderlich, Daten, die qualifiziert elektronisch signiert archiviert werden, vor Ablauf der Gültigkeit der eingesetzten mathematischen Verfahren und damit spätestens vor Ablauf der Gültigkeit der Signatur erneut qualifiziert elektronisch zu signieren. Durch die Neusignatur wird verhindert, dass der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird. Die bereits bestehende elektronische Signatur ist dabei in die erneute Signatur einzuschließen.

7 Sperrung von Zertifikaten

Sie können Ihr Zertifikat vor Ablauf der Gültigkeitsdauer sperren. Sperren Sie Ihr Zertifikat unverzüglich, wenn

- Sie Ihre sichere Signaturerstellungseinheit (Signaturkarte) verloren haben oder Ihnen diese abhanden gekommen ist,
- der Verdacht besteht, dass Ihre sichere Signaturerstellungseinheit manipuliert wurde oder ein Verdacht auf einen sonstigen Missbrauch vorliegt.

Nur durch eine Sperrung lässt sich in solchen Fällen ein (weiterer) Missbrauch verhindern.

Ihnen stehen folgende Sperrmöglichkeiten (7 Tage/Woche und 24 Stunden/Tag) zur Verfügung:

1. Online unter <https://www.s-trust.de>
2. Telefonisch unter der Sperrhotline +49 1805 936000¹

¹ 14 ct./min aus dem deutschen Festnetz; Mobilfunkhöchstpreis 42 ct./min

Zur Online- oder telefonischen Sperrung eines Zertifikats benötigen Sie folgende Angaben:

- Vor- und Nachname des Zertifikatsinhabers
- E-Mail-Adresse die im Zertifikat verwendet wird
- Dazugehöriges Sperrpasswort

Bei Verlust Ihres Sperrpasswortes kann die Sperrung über die zuständige Registrierungsstelle schriftlich (mit eigenhändiger Unterschrift des Zertifikatsinhabers / Sperrberechtigten; kein Telefax) beauftragt werden. Diese hat sich vor einer Sperrung auf geeignete Weise von der Identität des zur Sperrung Berechtigten zu überzeugen.

Wichtige Hinweise:

- Sollten Angaben für die Vertretungsmacht für Dritte, berufsbezogene oder sonstige Angaben zu Ihrer Person in Ihrem Zertifikat enthalten sein, ist eine Sperrung auch durch den Dritten bzw. die bestätigende Stelle (z.B. Ihre Firma) möglich. Diese erhalten ein vom DSV vorgegebenes, eigenes Sperrpasswort..
- Die Onlinesperrmöglichkeit der Internetschnittstelle von S-TRUST wird für die Dauer von vier Stunden gesperrt, wenn das Sperrpasswort dreimal hintereinander falsch eingegeben wird. In einem solchen Fall können Sie die unverzügliche Sperrung des Zertifikats über die telefonische Sperrhotline oder über die zuständige Registrierungsstelle veranlassen. Die Sperrung eines Zertifikats ist irreversibel. Eine rückwirkende Sperrung sowie eine vorübergehende Sperrung sind ausgeschlossen.
- Befinden sich auf einer sicheren Signaturerstellungseinheit bzw. Signaturkarte mehrere Zertifikate (z.B. Signatur- und Authentifizierungszertifikat) so werden bei Sperrung eines der Zertifikate stets automatisch auch alle weiteren Zertifikate (qualifizierte und sonstige Zertifikate) der jeweiligen sicheren Signaturerstellungseinheit bzw. Signaturkarte gesperrt.

8 Beschränkung der Nutzung des Signaturschlüssels

§ 7 Abs. 1 Nr. 7 Signaturgesetz lässt die Möglichkeit zu, die Nutzung des privaten Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang zu beschränken. Es kann sich um monetäre oder sonstige beliebige Beschränkungen handeln.

Jeder Zertifikatantragsteller hat die Möglichkeit, Nutzungsbeschränkungen in das qualifizierte Personenzertifikat (nicht in das fortgeschrittene Authentifizierungs-/Verschlüsselungszertifikat) aufnehmen zu lassen. Für den Inhalt der Beschränkung ist der Zertifikatsantragsteller allein verantwortlich; eine inhaltliche Prüfung nimmt der DSV nicht vor.

Durch derartige Beschränkungen wird die Einsatzfähigkeit des Zertifikats begrenzt. Achten Sie stets darauf, dass das die Beschränkungen enthaltene Zertifikat den zu signierenden Daten beigefügt und in die elektronische Signatur eingeschlossen ist.

9 Aufnahme eines Pseudonyms an Stelle des Namens in das Zertifikat

Anstelle des bürgerlichen Namens kann in ein Zertifikat ein Pseudonym aufgenommen werden. Pseudonyme sind durch die Endung im Zertifikat ":PN" gekennzeichnet. Der DSV ist nach dem Signaturgesetz dazu verpflichtet, die Daten über die Identität eines Signaturschlüssel- Inhabers - auch bei Verwendung eines Pseudonyms - auf Ersuchen an die

zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist. Der DSV dokumentiert die Auskünfte. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Übermittlung der Daten zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüsselinhabers an der Unterrichtung überwiegt.

Bitte beachten Sie, dass auch Zertifikate bei denen ein Pseudonym beantragt wurde, Beschränkungen oder sonstige Attribute enthalten können

10 Möglichkeit zur freiwilligen Anbieter-Akkreditierung

Das Signaturgesetz bietet Zertifizierungsdiensteanbietern (ZDA) wie S-TRUST die Möglichkeit, sich freiwillig einer aufwendigen Prüfung, z.B. durch TÜV-IT, zu unterziehen. Mit dieser optionalen Prüfung weist der ZDA die Einhaltung zusätzlicher Anforderungen für akkreditierte ZDA nach und erhält nach positivem Prüfergebnis ein Gütezeichen der Bundesnetzagentur. Solche ZDA dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf nachgewiesene Sicherheit berufen.

11 Ansprechpartner bei Fragen

Primärer Ansprechpartner ist Ihre zuständige Registrierungsstelle, die Ihnen in allen Fragen der Abwicklung von Zertifikatsanträgen zur Seite steht.

Bei technischen Fragen zum Download der Zertifikate steht Ihnen die Supporthotline Mo. bis Fr. von 8 bis 20 Uhr unter 0900 1 85 80 00² zur Verfügung.

Allgemeine Fragen und Neuigkeiten zu den Produkten von S-TRUST werden auf <https://www.s-trust.de> unter Kontakt beantwortet.

Eine besondere Schlichtungsstelle hat die Deutscher Sparkassen Verlag GmbH (DSV) für Zertifizierungsleistungen nicht eingerichtet. Sie können sich jedoch jederzeit an den DSV wenden. Die postalische Adresse lautet:

- Vertraulich -
Deutscher Sparkassen Verlag GmbH
Abteilung KDP2
Am Wallgraben 115
70565 Stuttgart

12 Weiterführende Informationen

Folgende Internetseiten stehen Ihnen als Informationsquelle rund um das Thema elektronische Signatur zur Verfügung:

<https://www.s-trust.de>

Produktinformationen zu Signaturkarten sowie Anwendungen. Zertifikatsmanagement inklusive Onlinesperrannahme für S-TRUST Personenzertifikate.

<http://www.bundesnetzagentur.de>

Informationen der zuständigen Behörde über Zertifizierungsdiensteanbieter sowie zugelassene Komponenten für die qualifizierte elektronische Signatur.

<http://www.bsi.de>

Bundesamt für Sicherheit in der Informationstechnologie zu den Themen Internetsicherheit, IT-Grundschutz, Zertifizierung/IT-Sicherheitskriterien und Computerviren.

<http://www.tuevit.de>

Informationen der vom ZDA DSV eingesetzten Prüf- und Bestätigungsstelle.

² 0,99 € pro Minute aus dem deutschen Festnetz.
Bei Anrufen aus Mobilfunknetzen können höhere Kosten anfallen.