

Teilnehmerunterrichtung gemäß SigG §6

Sehr geehrte Kundin, sehr geehrter Kunde,

mit Ihrer Entscheidung, sich durch den Zertifizierungsdiensteanbieter **D-TRUST GMBH** ein Zertifikat ausstellen zu lassen, treffen Sie eine bedeutungsvolle Entscheidung, denn die elektronische (oder auch digitale) Signatur ist für die handschriftliche Unterschrift, was das Telefon für das persönliche Gespräch war: eine revolutionäre Entwicklung innerhalb der Kommunikationstechnologie. Sie machen damit einen großen Schritt in Richtung eSecurity, also zu technischer und rechtlicher Sicherheit in der Welt des digitalen Datenverkehrs. - Was dies im Einzelnen bedeutet, wie Sie die Chancen dieser neuen Technologie nutzen und ihre Risiken beherrschen können, soll diese Broschüre verdeutlichen.

Bitte lesen Sie diese Unterrichtung sorgfältig. Bei der Antragstellung müssen Sie auch die Kenntnisnahme dieser Unterlagen durch Ihre Unterschrift bestätigen!

Ihr D-TRUST-TEAM

Inhalt

I. DAS WICHTIGSTE ZUERST...	2
II. RECHTSBELEHRUNG FÜR ANTRAGSTELLER EINES DIGITALEN SIGNATURZERTIFIKATES	2
III. DIE ELEKTRONISCHE SIGNATUR UND IHRE FUNKTIONSWEISE	3
IV. DIE PIN	5
V. DIE PUK	5
VI. DIE DTRUST SIGNATURKARTE	5
VI. DAS QUALIFIZIERTE ZERTIFIKAT UND SEIN INHALT	6
VII. DER ZERTIFIZIERUNGSDIENSTEBANBIETER D-TRUST UND SEINE AUFGABEN	6
VIII. DIE AUFNAHME DER ZERTIFIZIERUNGSTÄTIGKEIT	8
IX. AUSLAND – EXPORT	9
X. PSEUDONYME UND AUSKUNFTSPFLICHT	9
XI. DATENSCHUTZ	9
XII. TECHNISCHE KOMponentEN	9
XIII. DIE SCHRITTE VON DER ANTRAGSTELLUNG BIS ZUR ZERTIFIZIERUNG	10
XIV. WICHTIGE REGELN FÜR DEN UMGANG MIT DER ELEKTRONISCHEN SIGNATUR	12
XV. GRAFIK ZUM SIGNATURERZEUGUNGS- UND -ÜBERPRÜFUNGSVORGANG	14
XVI. KONTAKTE	15

I. DAS WICHTIGSTE ZUERST...

(1) Wir möchten, dass Sie über Ihre elektronische Signatur Bescheid wissen. Darauf legt auch das deutsche Signaturgesetz Wert. Es verlangt, dass Sie eine Unterrichtung über den Gebrauch der elektronischen Signatur erhalten und dass Sie die Kenntnisnahme dieser Unterrichtung bestätigen¹.

Sie haben diese Unterrichtung in Gestalt dieses Textes in Händen!

Die Wirkung der elektronischen Signatur im Rechtsverkehr steht im Zentrum dieser Belehrung:

Wirkung der elektronischen Signatur im Rechtsverkehr

Mit der elektronischen Signaturkarte der D-TRUST GMBH können Sie eine „qualifizierte elektronische Signatur mit“ 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 also 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 persönlichem Signieren noch verändert worden ist oder nicht.

II. RECHTSBELEHRUNG FÜR ANTRAGSTELLER EINES DIGITALEN SIGNATURZERTIFIKATES

Zur Rechtskraft der elektronischen Unterschrift

Jede Willenserklärung, die den üblichen gesetzlichen Voraussetzungen genügt (Geschäftsfähigkeit etc.) 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.

Die mit einer „qualifizierten elektronischen Signatur“ nach dem geltenden deutschen Signaturgesetz versehene Willenserklärung genügt darüber hinaus unter bestimmten Bedingungen (s.u.) 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).

In Paragraph 6 des Signaturgesetzes ist die **Unterrichtungspflicht** formuliert:

- (1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach § 5 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 schriftliche Belehrung auszuhändigen, deren Kenntnisnahme dieser durch gesonderte Unterschrift 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 dieser Broschüre auch von einer „digitalen Signatur“ oder „elektronischen Signatur“ die Rede; gemeint ist damit immer „qualifizierte elektronische Signatur“.

- §371a ZPO Beweiskraft elektronischer Dokumente
 "(1) 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."

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 voreingestellten 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 missbräuchlichen Zugriff geschützt, betrieben wird.**

III. DIE ELEKTRONISCHE SIGNATUR UND IHRE FUNKTIONSWEISE

Der Nutzen elektronischer Signaturen

Für die Kommunikation im privaten, aber auch im geschäftlichen Bereich gewinnen elektronische Medien zunehmend an Bedeutung: Texte und Dokumente werden immer häufiger elektronisch übermittelt, und der Empfänger kann sie sich auf Wunsch selbst ausdrucken.

Aber kann sich der Empfänger darauf verlassen, dass er den Inhalt des elektronischen Dokuments in unveränderter Form erhalten hat, also genau so, wie der Absender es an ihn abgeschickt hat? Und wie sicher ist die Identität des Absenders?

Traditionellerweise werden diese Funktionen durch die Unterschrift von Hand erfüllt, die eine Willenserklärung des Unterzeichners dokumentiert und seine Identität anhand der Unterschrift nachweist. Die elektronische Signatur spielt diese Rolle der handschriftlichen Unterschrift im elektronischen Verkehr: Anhand der elektronischen Signatur lässt sich überprüfen, ob der Inhalt unverändert geblieben ist, nachdem er signiert wurde; auch die Identität desjenigen, der die Daten signiert hat, ist eindeutig feststellbar. Wegen dieser Qualitätskriterien besitzt die „qualifizierte elektronische Signatur“ Rechtskraft: **Jede mit Ihrem elektronischen Signaturschlüssel erzeugte elektronische Signatur wird grundsätzlich und rechtsverbindlich als eine Willensbekundung Ihrerseits angesehen**, falls Ihr Zertifikat zum Zeitpunkt der Erzeugung gültig war und nicht Fakten die Vermutung widerlegen, dass die elektronische Signatur von Ihnen willentlich erzeugt wurde.

Die Funktionsweise elektronischer Signaturen

Jeder Signaturbesitzer bekommt ein individuelles digitales Schlüsselpaar. Es besteht aus dem

- „geheimen Schlüssel“ („Signaturschlüssel“): Der geheime Schlüssel befindet sich auf der Chipkarte des Users und ist nicht auslesbar. Er wird verwendet für die Signaturerzeugung: Beim Signieren der Nachricht wird eine Art Kopie der Nachricht ³ angefertigt und mit Hilfe des geheimen Schlüssels verschlüsselt. Das Ergebnis dieses Vorganges ist die elektronische Signatur, die zusammen mit dem Originaldokument versandt wird.

³ Es wird ein sogenannter „Hashwert“ des Originaldokumentes gebildet. Merkmale des Hashwertes: Verschiedene Nachrichten haben verschiedene Hashwerte; es ist unmöglich, aus dem Hashwert ein Originaldokument zu rekonstruieren; der Hashwert ist wesentlich kürzer als das Originaldokument.

- „öffentlichen Schlüssel“ („Signaturprüfschlüssel“). Mit dem öffentlichen Schlüssel tritt der User nach außen in Erscheinung. Dieser Schlüssel kommt bei der Signaturprüfung zum Einsatz: Der öffentliche Schlüssel wird mit der signierten Nachricht mitgeschickt. Beim Empfänger wird dann die verschlüsselte Kopie des Dokumentes mit Hilfe des öffentlichen Schlüssels entschlüsselt. Die Unversehrtheit der Nachricht wird überprüft, indem das Originaldokument mit der entschlüsselten Kopie verglichen wird.

Ein solches Verfahren, das auf der Verwendung eines geheim zu haltenden Schlüssels und eines frei verfügbaren Schlüssels beruht, bezeichnet man als *asymmetrisches kryptographisches Verfahren*.

Durch die elektronische Signatur wird Ihr Dokument nicht vor unbefugter Einsicht geschützt: Eine handschriftliche Unterschrift auf einem Papierdokument schützt ja auch nicht vor Einsichtnahme Dritter. Dazu müssen Sie das Dokument zusätzlich verschlüsseln, was häufig in der Anwendungssoftware als zusätzliche Option vorgesehen wird.

Wie wird signiert? ⁴

Nehmen wir an, Sie wollen ein Dokument elektronisch signieren:

- Nachdem Sie die elektronischen Daten erzeugt haben, legen Sie Ihre Signaturkarte in den Kartenleser ein.
- In Ihrem Anwendungsprogramm klicken Sie den Befehl „Dokument signieren“ an.
- Insofern die Signaturanwendungskomponente über eine Darstellungskomponente (secure viewer verfügt, wird Ihnen nun der Inhalt des Dokuments noch einmal angezeigt
- Prüfen Sie JETZT, was Sie auf dem Bildschirm sehen, denn dies ist der maßgebliche Inhalt für die elektronische Signatur!
- Wenn Sie nun den Inhalt bestätigen und signieren wollen, müssen Sie die PIN Ihrer Signaturkarte eingeben. Fertig!

Signaturanwendungssoftware, die nicht geprüft ist, ist nicht konform mit dem Signaturgesetz und kann prinzipiell einen verborgenen Text in das Dokument schmuggeln, durch den Sie zum Kauf des berühmten Staubsaugers verpflichtet werden könnten.

Wie prüft man eine Signatur?

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. Will man sich vergewissern, dass das Zertifikat noch gültig und nicht gesperrt ist, so kann man mit bestätigter Signaturanwendungssoftware auch eine Online-Prüfung des Zertifikats beim Zertifizierungsdiensteanbieter vornehmen, entweder indem ein Abgleich der Sperrlisten (CRL) durchgeführt wird oder eine OCSP - Abfrage (online certificate status protocol), bei der angezeigt wird, ob das Zertifikat gültig, gesperrt oder unbekannt ist (siehe auch V. Verzeichnisdienste).

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

⁴ Im Folgenden finden Sie eine allgemeine Beschreibung, die unabhängig von der Software ist, die Sie einsetzen und deshalb keine Details zur Durchführung enthält. Die Handhabung ist an die jeweilige Software gebunden.

IV. DIE PIN

Mit Hilfe der PIN weisen Sie sich als rechtmäßiger Benutzer der Chipkarte aus. Dies setzt natürlich voraus, dass **nur Sie** Ihre PIN kennen, und sonst **niemand**. Halten Sie deshalb Ihre PIN stets geheim! Die PIN ist gewissermaßen Ihre rechte Hand, mit der Sie eine Unterschrift leisten können und die Sie niemals aus der Hand geben dürfen. Auch keiner der Mitarbeiter der D-TRUST GMBH kennt Ihre PIN. Ihre Signaturkarte und die zugehörige PIN werden Ihnen von D-TRUST auf separatem Wege übermittelt.

Bei den PINs handelt es sich um

- die **PIN1 (Basic)** für Authentifizierung und Verschlüsselung
- sowie die **PIN2 (Specific)** für die Signatur. **Achtung:** Bei der PIN2 handelt es sich um eine **Transport-PIN**. Die Transport-PIN ist ein Sicherheitsmerkmal der Karte, welches Ihnen ermöglicht, die Unversehrtheit der Karte vor Inbetriebnahme zu prüfen. Vor der ersten Benutzung des Signaturschlüssels werden Sie automatisch aufgefordert, die PIN2 (Specific) zu ändern (6 bis 8 Stellen, nur Ziffern!). PIN1 ist von dieser Regelung nicht betroffen. Erst nach dieser Änderung ist es möglich, den Signaturschlüssel zu nutzen und damit eine Signatur auszuführen. Unser Supportcenter unterstützt Sie gern bei der Handhabung der PINs (Kontakt siehe Seite 14).
- Hat man Ihre Signaturkarte benutzt, **bevor** Sie sie erhalten, so werden Sie dies daran erkennen, dass die Ihnen mitgeteilte Transport-PIN zur Erstellung einer Signatur nicht akzeptiert wird oder dass Sie bei der ersten Benutzung nicht zur Änderung der PIN aufgefordert werden.
- In Abhängigkeit von der verwendeten Software werden Sie vor der ersten Benutzung zur Änderung der (Transport-) PIN aufgefordert oder Sie finden ein Dialogfeld, das Ihnen anzeigt, ob Ihre PIN schon geändert (initialisiert) wurde.

V. DIE PUK

Die Signaturkarten von D-TRUST werden mit einer so genannten PUK ausgeliefert. Dabei handelt es sich um eine spezielle PIN. Mit Hilfe dieser PUK wird Ihnen ermöglicht den Fehlbedienungsähler der PIN zurückzusetzen. Das bedeutet:

Wurde die Signaturkarte aufgrund einer dreimaligen Fehleingabe einer der beiden PINs gesperrt (Fehlermeldung Karte: „Karte geblockt“), haben Sie durch die Eingabe der PUK die Möglichkeit, die Karte wieder zu entsperren, indem Sie nach der Eingabe der PUK die korrekte PIN eingeben.

wichtiger Hinweis:

Eine Änderung der bestehenden PINs durch die Eingabe der PUK ist nicht möglich.

Die PUK hat einen Usage Counter, über den die maximale Anzahl an Rücksetzvorgängen (unter Zuhilfenahme eben dieser PUK) limitiert wird. In der gegenwärtigen Version hat der Usage Counter einen Wert von zehn.

Bitte beachten Sie folgende Sicherheitsmaßnahme: Wenn Ihre PUK dreimal hintereinander falsch eingegeben wurde, so wird die Karte gesperrt, weil von einem Missbrauchsversuch ausgegangen wird. Die Karte kann dann nicht wieder aktiviert werden. In diesem Fall kann nur – kostenpflichtig – eine Ersatzkarte beantragt werden.

WICHTIGER HINWEIS: MEHRFACHSIGNATURKARTEN VERFÜGEN **NICHT** ÜBER EINE PUK.

VI. DIE DTRUST SIGNATURKARTE

Auf ihrer D-TRUST Signaturkarte befinden sich ein qualifiziertes Zertifikat, ein oder mehrere weitere Zertifikate und die Zertifikate der jeweiligen CA die die Einzelzertifikate ausgestellt hat.

VI. DAS QUALIFIZIERTE ZERTIFIKAT UND SEIN INHALT

Ein Zertifikat bescheinigt, dass der Inhaber eines bestimmten öffentlichen Schlüssels die Person ist, deren Identität im Zertifikat angegeben ist. Ein Zertifikat übernimmt also die Rolle eines digitalen Ausweises, den der Zertifizierungsdiensteanbieter nach erfolgreicher Identifizierung ausstellt.

Das Zertifikat beinhaltet

- den Namen oder – auf Wunsch - das Pseudonym des Signaturschlüsselinhabers
- den zugeordneten Signaturprüfchlüssel
- die Algorithmen (d. h., das Verschlüsselungsverfahren), mit denen die Signaturschlüssel benutzt werden können
- die Zertifikatsnummer
- den Gültigkeitszeitraum des Zertifikates
- den Namen der Zertifizierungsstelle (D-TRUST) sowie das Land, in dem er zugelassen ist (Deutschland)
- die Bestätigung, dass es sich um ein qualifiziertes Zertifikat mit Anbieterakkreditierung handelt
- ggf. Attribute des Signaturschlüsselinhabers (in codierter Form).
- Beschränkungen
- Sonstige Angaben
- Monetäre Beschränkungen
- Firma / Organisation
- Abteilung / Organisationseinheit

Anhand des Zertifikats kann jeder die Echtheit eines signierten Dokumentes prüfen. Die Echtheit des Zertifikates wird nachprüfbar durch eine elektronische Signatur, die der Zertifizierungsdiensteanbieter selbst über dem Zertifikat anbringt.

Beschränkungen nach Art und Umfang

Sie können die Nutzung Ihres Zertifikates einschränken indem Sie zum Beispiel angeben zu welchem Zweck es verwendet werden darf. Unter Beschränkungen nach Art und Umfang zählen aber auch geographische Beschränkungen etc.

Sonstige Angaben

Wollen Sie festhalten, dass Sie gesetzlicher Vertreter oder Vormund einer Person sind, so können Sie auch dies in Ihr Zertifikat aufnehmen, wenn Sie den Nachweis dazu erbringen. Es ist dann gegebenenfalls die Sperrberechtigung Dritter zu berücksichtigen.

Monetäre Beschränkung

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

O und OU

In diesen Feldern können Sie Namen und Abteilung der Firma aufnehmen für die Sie tätig sind. Bitte beachten Sie das die Aufnahme einer Firmenzugehörigkeit Auswirkungen auf die Sperrberechtigung durch dritte Personen hat. Wurde die Firmenzugehörigkeit im Zertifikat aufgenommen, so ist die Firma berechtigt das Zertifikat ggf. sperren zu lassen.

VII. DER ZERTIFIZIERUNGSDIENSTEANBIETER D-TRUST UND SEINE AUFGABEN

Da die elektronische Signatur die Rolle der persönlichen eigenhändigen Unterschrift übernimmt, werden an die Ausgabestellen der Signaturkarten, die Zertifizierungsdiensteanbieter, höchste Sicherheitsansprüche gestellt:

Identifizierung und Registrierung der Teilnehmer des Systems

Der Zertifizierungsdiensteanbieter muss eine erkennungsdienstliche Identifizierung jeder Person durchführen, die eine elektronische Signatur beantragt. Jeder Antragsteller muss sich deshalb mit

einem gültigen Ausweisdokument legitimieren. Weitere Angaben, die in das Zertifikat aufgenommen werden sollen, müssen zuverlässig nachgewiesen werden.

Erzeugung der Schlüssel

Für jede Person, die ein Zertifikat beantragt, muss ein Schlüsselpaar erzeugt werden, das aus dem geheimen und dem öffentlichen Schlüssel besteht. Jedes Schlüsselpaar darf nur einmal existieren. Außerdem darf der geheime Schlüssel nicht von der Karte auslesbar sein.

Zertifizierung des öffentlichen Schlüssels (des „Signaturprüfschlüssels“)

Die „Kernaufgabe“ der Zertifizierungsstelle ist es, einen öffentlichen Schlüssel (den Signaturprüfschlüssel) nach seiner Erzeugung genau einer Person zuzuordnen, so dass Verwechslungen ausgeschlossen sind. Im Zertifikat beglaubigt der Zertifizierungsdiensteanbieter diese Zuordnung unter Berufung auf sein eigenes Zertifikat.

Bereitstellung der Zertifikate: Verzeichnisdienst

Die öffentlichen Schlüssel eines jeden Schlüsselpaares müssen „frei verfügbar sein“. Der Verzeichnisdienst stellt genau diese Dienstleistung dar. Wenn der Zertifikatsinhaber sich bei der Antragstellung damit einverstanden erklärt hat, dass sein Zertifikat nicht *nur nachprüfbar*, sondern auch online *abrufbar* sein soll, so kann das Zertifikat jederzeit vom Verzeichnisdienst abgerufen werden.

Den Verzeichnisdienst von D-TRUST GMBH erreichen Sie über die Internetadresse <http://www.d-trust.net>, indem Sie dem Stichwort „Zertifikatsabfrage“ folgen. Über den Zertifikatsdownload können Sie sich über Details zu Zertifikaten informieren. Über die Seriennummer des Zertifikats (aus den Eigenschaften) ist eine OCSP-Abfrage des Verzeichnisdienstes möglich. Als Antwort auf eine solche OCSP-Anfrage erhalten Sie die Auskunft, dass das betreffende Zertifikat der Zertifizierungsstelle gültig oder nicht mehr gültig (z. B. gesperrt, abgelaufen) oder unbekannt ist.

Sperrdienst – Sperrung von Zertifikaten

Sie können Ihr Zertifikat (vor Ablauf der Gültigkeitsfrist) sperren lassen. Dies empfehlen wir z. B. dringend für den Fall, dass Sie Ihre Signaturkarte verlieren oder sie Ihnen gestohlen wird. Nur durch die Sperrung lässt sich in solchen Fällen sicher ein Missbrauch verhindern.

Beachten Sie: Wer die Möglichkeit hat, Ihre Signaturkarte zu benutzen – also die Karte und die PIN besitzt -, 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.

Wenn in Ihrem Zertifikat weitere Angaben aufgenommen werden, durch die dritte Personen involviert sind, so sind auch diese berechtigt, Ihr Zertifikat sperren zu lassen.

Sie haben zwei 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: **D-TRUST GMBH, Kommandantenstraße 15, 10969 Berlin**.

Folgende Angaben müssen für eine Sperrung angegeben werden:

Telefonischer Sperrauftrag

- Name des Anrufers
- Name des Zertifikatinhabers, falls nicht Anrufer selbst
- wenn möglich Zertifikat-ID oder Signaturkarten-ID
- Sperrpasswort

Schriftlicher Sperrauftrag

- Name des Absenders
- Name des Zertifikatinhabers, falls nicht Absender selbst
- wenn möglich Zertifikat-ID oder Signaturkarten-ID
- Sperrpasswort (optional)
- Unterschrift des Absenders
- Sperrzeitpunkt

Wenn der Zertifikatsinhaber seinen vertraglichen Pflichten nicht nachkommt, so kann auch der Zertifizierungsdiensteanbieter eine Sperrung des Zertifikats vornehmen.

Sobald Sie Ihre Signaturkarte nicht mehr benötigen, so sollten Sie sie sperren lassen und unbrauchbar machen, indem Sie den Chip – zum Beispiel mit einem Locher - zerstören. Beachten Sie dabei unbedingt, dass Sie alle mit dieser Karte verschlüsselten Daten nur wieder mit genau dieser Karte und den dazugehörigen Schlüsseln und PINs entschlüsseln können; das bedeutet, Karte und PIN entweder aufzubewahren oder die Daten vor der Kartenvernichtung zu entschlüsseln. Sollten Sie die Karte aufbewahren, können Sie durch eine dreimalige Falscheingabe des PINs mit der Bezeichnung „SPECIFIC“ den Signaturschlüssel unbrauchbar machen.

Zeitstempeldienst

Ein Zeitstempel dient dazu, das elektronische Dokument mit aktuellem Datum und Uhrzeit zu versehen. Zur Beglaubigung wird das Ganze – Dokument, Datum und Uhrzeit – elektronisch signiert. Die Uhrzeit, auf die der Zeitstempeldienst zurückgreift, ist eine gesetzlich gültige Zeit. Sie ist unter hohem Sicherheitsaufwand gegen Manipulationen geschützt: All dies gehört zu dem hohen Niveau des Sicherheitsmanagements, das bei der D-TRUST GMBH praktiziert wird, um den Zertifizierungsdienst signaturgesetzeskonform anbieten zu können. Übrigens ist diese Dienstleistung kein Pflichtbestandteil eines signaturgesetzeskonformen Zertifizierungsbetriebes. Wird sie aber angeboten, so unterliegt sie genauso strengen Anforderungen wie der gesamte Zertifizierungsbetrieb.

VIII. DIE AUFNAHME DER ZERTIFIZIERUNGSTÄTIGKEIT

Pflichtvoraussetzungen

Bevor D-TRUST die Zertifizierungstätigkeit aufnehmen konnte, musste das Unternehmen gemäß Signaturgesetz und Signaturverordnung strenge Anforderungen erfüllen. Sie erstrecken sich unter anderem auf das Sicherheitsmanagement innerhalb der Zertifizierungsstelle, auf die von ihr verwendeten technischen Komponenten, auf die Fachkunde und Zuverlässigkeit der Mitarbeiter und auf das gebäudetechnische Sicherheitsniveau, insbesondere die sensiblen Bereiche. Will eine Zertifizierungsstelle den Zertifizierungsdienst aufnehmen, so hat sie dies der Bundesnetzagentur anzuzeigen, die die Sicherheit des Betriebes regelmäßig überprüft.

Die freiwillige Akkreditierung der Zertifizierungsstelle

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 für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) den Zertifizierungsdiensteanbieter akkreditieren. Im Gegensatz zur Anzeige der Betriebsaufnahme ist diese Akkreditierung aber freiwillig. Der D-TRUST GMBH wurde die Akkreditierungsurkunde im März 2002 ausgehändigt.

IX. AUSLAND – EXPORT

Die Anwendungssoftware und die Signaturkontrolle unterliegen aufgrund der darin enthaltenen Verschlüsselungstechnologien der Exportkontrolle. Innerhalb Deutschlands sind Betrieb und Nutzung genehmigungsfrei. Die Ausfuhr ins Ausland, der Betrieb und die Nutzung im Ausland können aber genehmigungspflichtig oder sogar verboten sein. Deshalb erkundigen Sie sich nach den gesetzlichen Bestimmungen des Landes, in welches Sie reisen.

X. PSEUDONYME UND AUSKUNFTSPFLICHT

Anstelle des Namens trägt der Zertifizierungsdiensteanbieter auf Wunsch des Antragstellers ein Pseudonym ins Zertifikat ein. Aus rechtlichen Gründen bestimmt der Zertifizierungsdiensteanbieter, die D-TRUST GMBH, das Pseudonym selbst.

Nach dem Signaturgesetz (§14, Abs. 2) ist der Zertifizierungsdiensteanbieter verpflichtet, die persönlichen Daten zur Identität eines Zertifikatsinhabers mit Pseudonym auf Ersuchen an Behörden weiterzugeben, wenn es

- erforderlich für die Verfolgung von Straftaten oder Ordnungswidrigkeiten,
- erforderlich zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung,
- erforderlich für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden ist, oder
- im Rahmen anhängiger Verfahren von einem Gericht angeordnet wurde.

Die erteilten Auskünfte werden dokumentiert.

Die ersuchende Behörde hat den Zertifikatsinhaber über die Aufdeckung des Pseudonyms zu unterrichten, sobald die Wahrnehmung der gesetzlichen Aufgaben dadurch nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüsselinhabers an der Unterrichtung überwiegt.

XI. DATENSCHUTZ

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

XII. TECHNISCHE KOMPONENTEN

Das Signaturgesetz und die zugehörige Verordnung stellen nicht nur an die D-TRUST GMBH als Zertifizierungsstelle hohe Anforderungen, sondern auch an die technischen Komponenten, die rund um die elektronische Signatur verwendet werden – sowohl innerhalb der Zertifizierungsstelle als auch auf Seiten der Benutzer. Es ist deshalb von größter Bedeutung, dass Sie technische Komponenten einsetzen, deren Sicherheit geprüft und bestätigt ist. Wenn Sie dies nicht tun, so kann dadurch die technische und die rechtliche Sicherheit der elektronischen Signatur beeinträchtigt werden. Darüber hinaus gehen Sie das Risiko ein, dass Ihnen durch Viren oder „trojanische Pferde“ fremde Daten zur elektronischen Signatur untergeschoben werden oder die zum Signieren bestimmten Daten kurz vor dem eigentlichen Signieren verändert wurden, ohne dass Sie es bemerken.

Ein ungewollter Kauf des sprichwörtlichen Staubsaugers wäre ein möglicher Schaden von nur geringem Ausmaß, wenn Sie den Sicherheitsstandard der technischen Komponenten außer Acht lassen. Verwenden Sie nur Anwendungsprogramme, für die der Hersteller in einer Erklärung die Konformität mit dem Signaturgesetz zugesichert hat, oder die geprüft und bestätigt sind. Eine **aktuelle Liste** der technischen Komponenten, die entsprechend den Anforderungen des Signaturgesetzes und der zugehörigen Signaturverordnung bestätigt sind, finden Sie auf den Seiten der Bundesnetzagentur: <http://www.bundesnetzagentur.de>

XIII. DIE SCHRITTE VON DER ANTRAGSTELLUNG BIS ZUR ZERTIFIZIERUNG

1. Antragstellung

Sie wählen eine der beiden Möglichkeiten zur Antragsstellung, die wir Ihnen anbieten:

Option 1: Antragstellung mit Identifizierung mittels PostIdent-Verfahren

Sie drucken auf der entsprechenden Web-Site das von D-TRUST angebotene Antragsformular aus oder D-TRUST versendet die Antragsunterlagen auf Anforderung an Sie. Zusammen mit dem Antragsformular erhalten Sie den PostIdent-Coupon, diese Unterrichtungsbrochure, die Rechtsbelehrung und Hinweise zur Beantragung oder Sie drucken sich diese Unterlagen aus dem Internet aus. Bitte füllen Sie das Antragsformular vollständig aus. Sollten Sie Fragen haben, wenden Sie sich an uns **030 / 25 93 91 - 0**.

Außerdem machen Sie bitte von Ihrem Ausweisdokument eine Ablichtung und bestätigen Sie dies mit einer eigenhändigen Unterschrift über das Passbild der Ausweiskopie. Achten Sie darauf, dass die Unterschrift auf dem Antrag und über dem Foto in der Form (Name mit oder ohne Vornamen) zu leisten ist, in der sie auch im vorzuweisenden Ausweisdokument geleistet wurde (Musterunterschrift). Mit den vollständigen Unterlagen begeben Sie sich bitte zu einer Niederlassung der Deutschen Post AG zur Identifizierung. Das Identifizierungsformular und Ihre Unterlagen werden von der Post an D-TRUST gesandt.

Falls Sie weitere Angaben in Ihr Zertifikat aufnehmen lassen wollen, so fügen Sie der Postsendung auch die Unterlagen bei, mit denen Sie diese Angaben nachweisen wollen. Der Antrag wird bei D-TRUST geprüft. Wenn alle Unterlagen vollständig und richtig sind, kann Ihre Signaturkarte erstellt werden.

Wichtig: Benutzen Sie bitte beim gesamten Identifizierungs-Verfahren immer dasselbe Ausweisdokument. Ein Wechsel führt zur Ungültigkeit des Verfahrens.

Option 2: Antragstellung mit Identifizierung in einer Identifizierungsstelle

Sie gehen zum Zertifizierungsdiensteanbieter **D-TRUST GmbH, Kommandantenstraße 15, 10969 Berlin** oder zu einer der externen Identifizierungsstellen. Die Lage der nächsten Identifizierungsstelle können Sie bei D-TRUST erfragen.

Sie erhalten dort diese Unterrichtungsbrochure, die Sie bitte aufmerksam lesen. Sie werden später mit Ihrer handschriftlichen Unterschrift bestätigen müssen, dass Sie diese Unterrichtung zur Kenntnis genommen haben und dass Sie speziell darüber belehrt worden sind, dass die elektronische Signatur der handschriftlichen Unterschrift im Rechtsverkehr gleichgestellt ist.

Sie füllen das Antragsformular aus und werden anhand Ihres Ausweisdokumentes, das sie mitgebracht haben, identifiziert. Selbstverständlich muss es ein gültiges Ausweisdokument sein. Falls Sie weitere Angaben in Ihr Zertifikat aufnehmen lassen wollen, so legen Sie dort auch die Unterlagen vor, mit denen Sie diese Angaben nachweisen wollen.

Hinweis: Sie können zur Verkürzung der Bearbeitungszeit ausgefüllte Unterlagen zur Identifizierungsstelle mitbringen.

2. Übergabeverfahren Signaturkarte

Wählen Sie eines der beiden Übergabeverfahren aus, das wir Ihnen anbieten:

Option 1: Zustellung per Post

Wenn die Signaturkarte mit der Post zugesandt wird, so erfolgt dies standardmäßig per Einschreiben. Daneben bieten wir Ihnen auch an, die Signaturkarte im PostIdent-Special-Verfahren zu versenden. Bei diesem Verfahren überbringt Ihnen ein Postzusteller die Signaturkarte und führt eine Identifizierung anhand des Ausweisdokumentes durch. Auch hier sollten Sie dasselbe Ausweisdokument vorlegen wie bei der Antragstellung. Erst wenn diese Identifizierung erfolgreich durchgeführt worden ist, händigt der Zusteller Ihnen den Umschlag mit der Signaturkarte persönlich aus.

Option 2: Persönliche Abholung

Dazu kommen Sie zu derselben Stelle, an der Sie den Antrag auf Ihr Personenzertifikat gestellt haben (D-TRUST bzw. entsprechende externe Stelle). Dort weisen Sie sich anhand des Ausweisdokumentes aus, das Sie schon bei der Antragstellung verwendet haben und erhalten die Signaturkarte, wenn Ihre Identifizierung erfolgreich durchgeführt wurde.

3. Übermittlung des PIN-Briefs

Den PIN-Brief erhalten Sie in einem Anschreiben auf dem Postwege. Dieses Anschreiben geht standardmäßig an Ihre Privatadresse. Im Anschreiben wird Ihnen erläutert, wie Sie die PINs beim ersten Gebrauch ändern, denn der Transport-PIN soll nur den Übergabeweg der Signaturkarte schützen.

Den Erhalt der Signatur-Karte und der zugehörigen PIN quittieren Sie mit Ihrer Unterschrift auf dem beigefügten Bestätigungsformular und senden dieses an D-TRUST zurück.

Erst wenn wir diese Rückantwort erhalten und geprüft haben, kann Ihre Signaturkarte durch uns freigeschaltet werden. Das heißt, erst ab diesem Zeitpunkt können Sie Ihre Karte rechtsverbindlich zum Signieren verwenden. Erhält D-TRUST **innerhalb von 2 Wochen** nach Zusendung des PIN-Briefes keine **Empfangsbestätigung des Kunden**, so muss die Karte gesperrt werden. Mit einer gesperrten Karte können keine online-Dienste genutzt werden!

Beachten Sie das die Karte durch die so genannte Transport PIN geschützt ist. In Abhängigkeit von der verwendeten Software werden Sie vor der ersten Benutzung zur Änderung der (Transport-) PIN aufgefordert oder Sie finden ein Dialogfeld, das Ihnen anzeigt, ob Ihre PIN schon geändert (initialisiert) wurde.

4. Freischaltung der Karte

Den Erhalt der Signatur-Karte und der zugehörigen PIN quittieren Sie mit Ihrer Unterschrift entweder auf dem beigefügten Bestätigungsformular und senden dieses an D-TRUST zurück oder bei der persönlichen Abholung bei D-TRUST bzw. entsprechende externe Stelle.

Erst wenn wir diese Bestätigung erhalten und geprüft haben, kann Ihre Signaturkarte durch uns freigeschaltet werden. Das heißt, erst ab diesem Zeitpunkt können Sie Ihre Karte rechtsverbindlich zum Signieren verwenden. Erhält D-TRUST **innerhalb von 2 Wochen** nach Übergabe der Signaturkarte und Zusendung des PIN-Briefes keine **Empfangsbestätigung des Kunden**, so muss die Karte gesperrt werden. Mit einer gesperrten Karte können keine online-Dienste genutzt werden!

Etwa 3 Werktage nach Erhalt der Karte bekommen Sie auf dem Postwege ein Anschreiben, welches Ihre PIN enthält. Dieses Anschreiben geht standardmäßig an Ihre Privatadresse. Im Anschreiben wird Ihnen erläutert, wie Sie die PINs beim ersten Gebrauch ändern, denn die Transport-PIN soll nur den Übergabeweg der Signaturkarte schützen.

Den Erhalt der Signatur-Karte und der zugehörigen PIN quittieren Sie mit Ihrer Unterschrift auf dem beigefügten Bestätigungsformular und senden dieses an D-TRUST zurück.

Erst wenn wir diese Rückantwort erhalten und geprüft haben, kann Ihre Signaturkarte durch uns freigeschaltet werden. Das heißt, erst ab diesem Zeitpunkt können Sie Ihre Karte rechtsverbindlich zum Signieren verwenden. Erhält D-TRUST **innerhalb von 2 Wochen** nach Zusendung des PIN-Briefes keine **Empfangsbestätigung des Kunden**, so muss die Karte gesperrt werden. Mit einer gesperrten Karte können keine online-Dienste genutzt werden!

XIV. WICHTIGE 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. Hüten Sie deshalb Ihre Signaturkarte wie Ihren Augapfel! Sie enthält nicht nur Ihren digitalen Ausweis, sondern zugleich auch Ihre elektronische Unterschrift! Geben Sie deshalb auch Ihre PIN unter keinen Umständen preis!

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

1. Sicherung ihres Personal Computers

- Schützen Sie Ihren Personal Computer vor unbefugtem Zugriff, z. B. durch einen Bootschutz.
- Achten Sie auf einen wirksamen Virenschutz, und vergewissern Sie sich vor dem Signieren, dass Ihr PC virenfrei ist. Wenn Veränderungen an der Signiersoftware durch Viren entstehen, so entspricht die Software nicht mehr den Anforderungen für qualifizierte Signaturen.

2. Persönlicher Gewahrsam

- Behalten Sie Ihre Signaturkarte stets in Ihrem persönlichen Gewahrsam!

3. PIN

- Halten Sie Ihre PINs unter allen Umständen geheim! Lassen Sie sich bei der Eingabe der PINs nicht beobachten. Falls Sie den Eindruck oder nur den Verdacht haben, dass die PIN bekannt geworden ist, ändern Sie die PIN umgehend!
- Meiden Sie leicht zu erratende PINs (Geburtsdaten, Telefonnummern, Namen von Familienmitgliedern) und verwenden Sie nicht dieselbe PIN für Ihre Signaturkarte, Ihren PC-Zugang, Ihr Online-Banking oder Ihre EC-Karte. Sie kämen damit dem Ausspäher sehr entgegen.
- Benutzen Sie nicht die gleiche Ziffernfolge für die PIN1 und PIN2. Verwenden Sie unterschiedliche PINs. Besonders wichtig ist dies, wenn Sie die Signaturkarte auch in ungesicherten Umgebungen einsetzen.

4. Schutz der technischen Komponenten zur Signaturprüfung und Signaturerstellung

- 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. Verwenden Sie nur Anwendungsprogramme, für die der Hersteller in einer Erklärung die Konformität mit dem Signaturgesetz zugesichert hat, oder die geprüft und bestätigt sind und im Internet auf den Seiten der Bundesnetzagentur <http://www.bundesnetzagentur.de> aufgeführt sind.

- Lassen Sie die Softwareprogramme Ihrer Signaturanwendungskomponenten unverändert: Nur so bleiben sie signaturgesetzkonform.

Einschluss von Beschränkungen in die digitale Signatur

- + 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“, also finanzielle Obergrenzen) von Bedeutung sind, dann müssen Sie Ihr Zertifikat dem Dokument hinzufügen und es in die elektronische Signatur einschließen.

Zeitstempel

- + Wenn für die Verwendung der von Ihnen signierten Daten ein Zeitpunkt von Bedeutung ist, so bringen Sie bitte einen Zeitstempel an (vgl. Abschnitt)!

5. Erneute Anbringung einer elektronischen Signatur

- Wenn ein Dokument über einen längeren Zeitraum eine elektronische Signatur trägt, dann 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.

6. Signaturerzeugung (Signaturbildung)

- Überprüfen Sie vor der Signaturbildung den Inhalt des digitalen Dokuments mit Hilfe der Darstellungskomponente, die bei der Signaturbildung automatisch geöffnet wird. Anderenfalls ist nicht gewährleistet, dass Sie wirklich den maßgeblichen – nämlich den signierten – Wortlaut zu Gesicht bekommen.

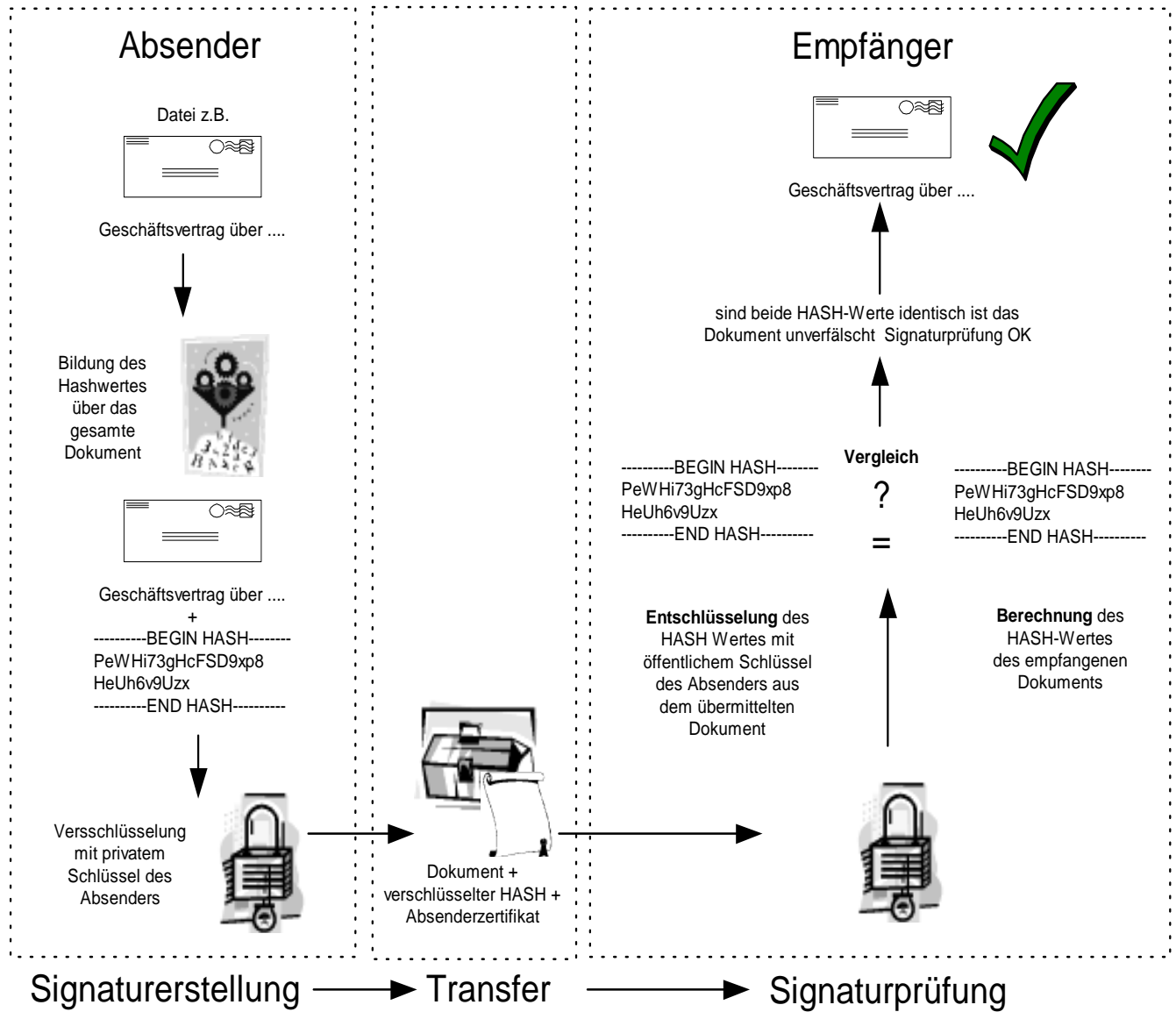
7. Signaturprüfung

- Lesen Sie das signierte Dokument in der Darstellungskomponente (Viewer), der Bestandteil der von Ihnen installierten, geprüften und bestätigten Signaturanwendungssoftware ist. Nur in dieser Darstellung haben Sie die Gewähr, dass Ihnen der vollständige und korrekte Wortlaut des signierten Dokumentes angezeigt wird.

8. Sperrung

- Lassen Sie Ihre Signaturkarte sperren, wenn Sie sie verloren haben oder wenn Sie den Verdacht haben, dass Ihre Karte von Dritten manipuliert worden ist.
- Damit Sie jederzeit eine Sperrung vornehmen lassen können, notieren Sie die Identifizierungsnummer (Seriennummer) Ihrer Signaturkarte, die Zertifikats-ID, die Telefonnummer und Anschrift des Sperrdienstes und bewahren diese Angaben an einem sicheren Ort auf!
- Ihr Sperrpasswort halten Sie auf alle Fälle geheim und merken es sich gut.
- Wenn Sie Ihre Signaturkarte nicht mehr benötigen, müssen Sie sie unbrauchbar machen, indem Sie die Zertifikate durch dreifach falsche PIN-Eingabe sperren oder den Chip auf der Karte mechanisch zerstören (Sie können dazu zum Beispiel mit einem Locher den in der Signaturkarte befindlichen Chip stanzen). Zusätzlich sollten Sie Ihr Zertifikat sperren lassen, falls es nicht schon abgelaufen ist.

XV. GRAFIK ZUM SIGNATURERZEUGUNGS- UND -ÜBERPRÜFUNGSVORGANG



XVI. 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 Support:

D-TRUST GmbH
Tel.: + 49 (0) 30 / 25 93 91 610
Fax: + 49 (0) 30 / 25 93 91 22
support@d-trust.net

Sperrhotline:

Tel.: + 49 (0) 30 / 25 93 91 – 600

Noch Fragen?

**Im Internet finden Sie natürlich viele Informationen
rund um die elektronische Signatur und den Registrierungsbetrieb:**

- ◆ <http://www.iukdg.de>

Diese Seite gehört zum Bundesministerium für Wirtschaft und Technologie (BMWi) und befasst sich mit dem „Informations- und Kommunikationsdienste-Gesetz (IuKDG)“, dessen dritter Artikel das Signaturgesetz in seiner ersten Fassung darstellt. Sie finden dort aber auch die neuere Fassung vom 21. Mai 2001 (eine elektronische Kopie des einschlägigen Bundesgesetzblattes), die Verordnung zum Signaturgesetz etc.

- ◆ <http://www.bundesnetzagentur.de>

Dies ist die Seite der Wurzel-Zertifizierungsstelle, der „Bundesnetzagentur“, die allen Zertifizierungsstellen übergeordnet ist und die Schlüsselzertifikate für sie bereitstellt, falls sie akkreditiert sind. Über diese Seite finden Sie eine Liste mit bestätigten technischen Komponenten, die als signaturgesetzkonforme Signaturerstellungseinheiten geeignet sind.

- ◆ <http://www.bsi.de>

Dies ist die Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dort finden Sie viele Informationen zu rechtlichen und technischen Fragen.