



# Fit für die qualifizierte elektronische Signatur

Unterrichtung zum Signaturgesetz

## Inhalt

1. Das Signaturgesetz	4
2. Qualifizierte elektronische Signatur	5
Wozu benötigen Sie eine qualifizierte elektronische Signatur?	5
Wie funktioniert eine qualifizierte elektronische Signatur?	5
Was muss ich tun, um ein Dokument qualifiziert elektronisch zu signieren?	5
Was muss ich tun, um eine qualifizierte elektronische Signatur zu prüfen?	6
Exkurs: Zeitstempeldienst	6
3. Aufgaben eines freiwillig akkreditierten Zertifizierungsdiensteanbieters	7
Schlüsselgenerierung	7
Zertifizierung des öffentlichen Schlüssels	7
Gültigkeit von Signaturschlüssel, Zertifikaten und qualifizierten elektronischen Signaturen	8
Wirkung einer qualifizierten elektronischen Signatur im Rechtsverkehr	8
Zuordnung der Signatur	8
Attribute	8
Verzeichnisdienst (Bereitstellen der Zertifikate)	9
Sperrdienst	9
Exportbeschränkungen	10
4. Wie erhalte ich meine zertifizierte Kammer-Signaturkarte?	11
Beantragung	11
Identifizierung des Antragstellers und Übergabe des e:secure-Pakets in der Kammer	11
Identifizierung des Antragstellers durch das PostIdent BASIC-Verfahren	11
Übergabe der zertifizierten Signaturkarte	12
5. Sicherer und richtiger Umgang mit der zertifizierten Signaturkarte	13
6. Weitere nützliche Hinweise	14
Wo kann ich weitere Informationen zur qualifizierten elektronischen Signatur erhalten?	14
Beschwerde- und Schlichtungsverfahren	14
Was kann ich tun, damit mein Sperrpasswort sicher ist?	14
Wer kann meine qualifiziert elektronisch signierten Dokumente lesen?	14

## Sehr geehrte Damen und Herren,

mit Ihrer Entscheidung für die zertifizierte Signaturkarte haben Sie die richtige Wahl für die Zukunft getroffen. Bei dem Paket „Kammer e:secure“ handelt es sich um ein dem Signaturgesetz (SigG) und der Signaturverordnung (SigV) entsprechendes Komplettangebot, bestehend aus allen für die Nutzung der qualifizierten elektronischen Signatur notwendigen Hardware-, Software- und Dienstleistungskomponenten. Das Paket umfasst u. a. eine SigG-konforme Signaturkarte (kurz: zertifizierte Signaturkarte), einen Kartenleser und die DATEV-Software GERVA.

Nachdem seit Herbst 2001 das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr“ verabschiedet ist, können Sie mit einer zertifizierten Signaturkarte Erklärungen genauso unterzeichnen, wie mit Ihrer eigenhändigen Unterschrift.

Sie wollen wissen, wozu man qualifizierte elektronische Signaturen benötigt, wie qualifizierte elektronische Signaturen funktionieren und was Sie im Umgang mit Ihrer zertifizierten Signaturkarte beachten müssen? Damit Sie alle Vorteile der qualifizierten elektronischen Signatur nutzen können, finden Sie in der vorliegenden Unterrichtung Informationen rund um die qualifizierte elektronische Signatur und Ihre zertifizierte Signaturkarte.

Diese Unterrichtung muss gemäß § 6 Signaturgesetz und § 6 Signaturverordnung bestimmte, gesetzlich geforderte Inhalte enthalten. Dies bedingt einerseits eine relativ umfangreiche Information für Sie, andererseits werden Sie über alle wichtigen Belange hinsichtlich der qualifizierten elektronischen Signatur ausführlich informiert. Zusätzlich ist es erforderlich, dass Sie durch Ihre Unterschrift bestätigen, die vorliegende Unterrichtung erhalten und zur Kenntnis genommen zu haben, nachdem Ihnen Ihre persönliche zertifizierte Signaturkarte ausgehändigt wurde.

# 1. Das Signaturgesetz

Die erste Fassung des Signaturgesetzes wurde als Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) im August 1997 in Deutschland eingeführt. Dieses SigG wurde entsprechend der am 19. Januar 2000 in Kraft getretenen EU-Richtlinie überarbeitet. Die SigG-Novellierung „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“ ist seit 22. Mai 2001 in Kraft. Das SigG schafft Rahmenbedingungen für qualifizierte elektronische Signaturen, unter denen diese als sicher gelten und Fälschungen qualifizierter elektronischer Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können. Das SigG unterscheidet in Übereinstimmung mit der EU-Signaturrichtlinie folgende Signaturen:

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

Die beiden ersten Arten von Signaturen werden in der EU-Richtlinie und im SigG nur definiert. Nähere rechtliche Anforderungen werden nur an die beiden letzten Signaturen gestellt – und folglich werden nur diese EG-weit der eigenhändigen Unterschrift rechtlich gleichgestellt, wenn durch das Gesetz nichts anderes bestimmt ist (SigG § 6 Abs. 2).

Die „qualifizierte elektronische Signatur“ ist der EU-Mindeststandard für Signaturen, die ein Substitut zur eigenhändigen Unterschrift bildet. Demgegenüber ist bei „qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung“ die Sicherheit durch gesetzlich anerkannte fachkundige Dritte (z. B. TÜVIT) nachgewiesen und eine dauerhafte Überprüfbarkeit (mindestens 30 Jahre) garantiert.

Das Signaturgesetz sieht den Aufbau einer Infrastruktur für qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung vor. Die „Regulierungsbehörde für Telekommunikation und Post“ (Reg TP) ist die oberste Instanz in der Infrastruktur für diese freiwillig akkreditierten Zertifizierungsdiensteanbieter. Sie erteilt den Zertifizierungsdiensteanbietern, wie z. B. DATEV oder der Kammer, die Genehmigung zum Betrieb eines Zertifizierungsdienstes, stellt deren qualifizierte Zertifikate aus und führt diese Zertifikate in einem eigenen Verzeichnis. Mit Hilfe dieses Verzeichnisses kann jedermann überprüfen, ob der öffentliche Schlüssel (Signaturprüfschlüssel) eines akkredi-

tierten Zertifizierungsdiensteanbieters tatsächlich diesem Zertifizierungsdiensteanbieter zugeordnet ist.

Das Signaturgesetz beinhaltet auch Anforderungen an einen freiwillig akkreditierten Zertifizierungsdiensteanbieter hinsichtlich baulicher Maßnahmen eines Trustcenters (hier findet die Zertifikat-Erzeugung in einer sicheren Umgebung statt), eines zu erstellenden Sicherheitskonzepts und der Qualifikation des eingesetzten Personals.

Diese Anforderungen wurden von Ihrer Kammer erfüllt und von einer von der Reg TP anerkannten Bestätigungsstelle geprüft und bestätigt. Somit ist Ihre Kammer ein nach dem Signaturgesetz „freiwillig akkreditierter Zertifizierungsdiensteanbieter“. Ihre Kammer erfüllt damit auch die Maßgaben der EU-Richtlinie.

# 2. Qualifizierte elektronische Signatur

## Wozu benötigen Sie eine qualifizierte elektronische Signatur?

Für unser Geschäfts- und auch Privatleben werden elektronische Medien immer wichtiger. Der Datenaustausch über Netzwerke, wie z. B. über das Internet, nimmt inzwischen eine zentrale Stellung ein. Bei diesem Datenaustausch kommt es immer öfter vor, dass wir mit Personen kommunizieren und geschäftlich verkehren, die wir nicht kennen.

Wir können nicht sicher sein, dass unser Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt. Auch, dass die Daten so ankommen, wie sie abgesendet wurden, ist nicht sichergestellt. Solange wir jedoch kein Vertrauen in unsere Kommunikationspartner haben, werden wir die neuen Medien kaum nutzen.

Auf diese zwei wichtigen Fragen nach der Identität des Kommunikationspartners und der Unversehrtheit der Inhalte bietet die Technik der qualifizierten elektronischen Signatur Antworten. Sie ermöglicht, zweifelsfrei festzustellen, wer der tatsächliche Unterzeichner eines elektronischen Dokumentes ist und ob die übermittelten Daten unterwegs verändert wurden oder nicht. Der Unterzeichner eines Dokumentes ist eindeutig feststellbar. Die Unversehrtheit des Dokumentes kann im Streitfall bewiesen werden.

## Wie funktioniert eine qualifizierte elektronische Signatur?

Die Technik der qualifizierten elektronischen Signatur basiert auf zwei mathematischen Schlüsseln, die zwar verschieden, aber eindeutig einander zugeordnet sind. Diese Schlüssel bezeichnet man als privaten und als öffentlichen Schlüssel. Sie gehören in dem Sinne zusammen, dass Inhalte, die mit dem privaten Schlüssel (Signaturschlüssel) signiert werden, nur mit dem dazugehörigen öffentlichen Schlüssel (Signaturprüfschlüssel) überprüft werden können. Der private Schlüssel (Signaturschlüssel) bleibt immer geheim. Der öffentliche Schlüssel (Signaturprüfschlüssel) darf jedermann bekannt sein.

Ein solches Verfahren, das einen geheimen privaten (Signaturschlüssel) und einen frei verfügbaren öffentlichen Schlüssel (Signaturprüfschlüssel) verwendet, wird als asymmetrisches, kryptographisches Verfahren bezeichnet. Nur ein solches Verfahren ermöglicht es, dass jedermann in den Besitz des öffentlichen Schlüssels (Signaturprüfschlüssel) gelangen kann, um die Identität seines Gegenübers und die Integrität des Kommunikationsinhaltes zweifelsfrei feststellen zu können.

### Beispiel:

Ein elektronisches Vertragsdokument wird mit Hilfe eines Textverarbeitungsprogrammes wie z. B. Microsoft Word erstellt, mit einer qualifizierten elektronischen Signatur

versehen und verschlüsselt und anschließend per E-Mail an den Vertragspartner verschickt. Dieser entschlüsselt das Dokument, versieht es ebenfalls mit einer qualifizierten elektronischen Signatur und schickt es auf dem gleichen Weg wieder verschlüsselt an seinen Vertragspartner zurück. Der elektronisch geschlossene Vertrag ist rechtsgültig (§ 126 a BGB).

## Was muss ich tun, um ein Dokument qualifiziert elektronisch zu signieren?

Wenn Sie ein Dokument qualifiziert elektronisch signieren wollen, gehen Sie wie folgt vor:

1. Melden Sie sich in der Anwendung der DATEV Software GERVA (= Gesicherter Elektronischer Rechtsverkehr mit Attribut) an und geben Sie die PIN für Verschlüsselung und Anwendung im Anmeldedialog ein.
2. Wählen Sie das zu signierende Dokument aus und signieren Sie es mittels der GERVA-Signierbuttons bzw. über die Druckfunktionalität der jeweiligen Anwendung und dem GERVA-Drucker.
3. Das Dokument wird in dem Dialog „Daten qualifiziert signieren und verschlüsseln“ angezeigt. Hier wählen Sie die entsprechenden Optionen aus.

### 3. Aufgaben eines freiwillig akkreditierten Zertifizierungsdiensteanbieters

4. Geben Sie Ihre PIN zur Durchführung der qualifizierten elektronischen Signatur ein.
5. Ihr Dokument wird qualifiziert elektronisch signiert.

#### Was muss ich tun, um eine qualifizierte elektronische Signatur zu prüfen?

Wenn Sie ein qualifiziert elektronisch signiertes Dokument prüfen wollen, gehen Sie wie folgt vor:

1. Öffnen Sie das qualifiziert elektronisch signierte Dokument. Automatisch wird die DATEV-Software GERVA aufgerufen und anschließend das Protokoll der Offline-Verifikation angezeigt.
2. Zusätzlich sollten Sie die „Onlineprüfung“ durchführen, um das Zertifikat des Signierers im Verzeichnisdienst des Trustcenters zu überprüfen.
3. Sie erhalten die Informationen, ob die Signatur zum Prüfzeitpunkt gültig ist.

#### Hinweis:

Zur vollständigen Verifikation nach dem Signaturgesetz (SigG) muss die Gültigkeit des verwendeten qualifizierten Zertifikats online beim Verzeichnisdienst abgefragt werden.

Einzelheiten zum Signier- und Prüfvorgang können Sie dem Installationswegweiser entnehmen.

#### Exkurs: Zeitstempeldienst

Für viele elektronische Dokumente ist es wichtig, die Integrität der Dokumente zu einem vorgegebenen Zeitpunkt rechtsverbindlich feststellen zu können. In diesen Fällen müssen Möglichkeiten zum Rück- oder Vordatieren ausgeschlossen werden. Mit Hilfe des vom Zertifizierungsdiensteanbieter zur Verfügung gestellten „Zeitstempeldienstes“ kann einem Dokument ein Zeitpunkt rechtsverbindlich zugeordnet werden. Dies ist ein optionales Angebot der DATEV. Eine Kostenberechnung ist vorbehalten.

Ein freiwillig akkreditierter Zertifizierungsdiensteanbieter übernimmt viele wichtige Aufgaben, die das Signaturgesetz/die Signaturverordnung vorschreiben.

#### Schlüsselgenerierung

Das zum qualifizierten elektronischen Signieren verwendete Schlüsselpaar, das aus einem privaten (Signatur-schlüssel) und einem öffentlichen Schlüssel (Signaturprüfschlüssel) besteht, muss erzeugt werden. Hier besteht die Anforderung, dass jedes Schlüsselpaar nur einmal auf der Welt existieren darf. Der persönliche Schlüssel muss geheim bleiben – auch der Zertifizierungsdiensteanbieter selbst darf den privaten Schlüssel (Signaturschlüssel) nicht kennen. Das DATEV-Trustcenter erfüllt diese Anforderungen des Signaturgesetzes/der Signaturverordnung. Dies wurde von einer von der Reg TP anerkannten Bestätigungsstelle geprüft und bestätigt. In regelmäßigen Abständen finden Wiederholungsprüfungen statt.

Ein weiteres, wichtiges Sicherheitsmerkmal ist das Speichermedium des Schlüsselpaares. Dieses Speichermedium muss unbedingt sicherstellen, dass der auf ihm gespeicherte private Schlüssel (Signaturschlüssel) nicht ausgelesen werden kann und dieser das Speichermedium niemals verlässt.

Als Speichermedium für das Schlüsselpaar werden spezielle Signaturkarten (sichere Signaturerstellungseinheit) verwendet, die die Anforderungen des SigG und der SigV erfüllen.

#### Zertifizierung des öffentlichen Schlüssels

Was bedeutet „Zertifizierung“? Wörtlich genommen bedeutet Zertifizierung „Bescheinigung“. Zertifizierungsdiensteanbieter wie DATEV oder die Kammer bescheinigen, dass ein öffentlicher Schlüssel (Signaturprüfschlüssel) dem Inhaber des Schlüsselpaares gehört. Um dies bescheinigen zu können, müssen die Zertifizierungsdiensteanbieter die Identität des Karteninhabers zuverlässig feststellen. Dies kann per PostIdent 3-Verfahren der Deutschen Post AG (DPAG) oder durch persönliche Identifizierung durch den Zertifizierungsdiensteanbieter (ZDA) geschehen. Einzelheiten hierzu können Sie aus dem Datenfahrplan entnehmen, der Ihnen zusammen mit dieser Unterrichtung zugegangen ist. Dass der öffentliche Schlüssel (Signaturprüfschlüssel) dem Karteninhaber zugeordnet wurde, bescheinigt – oder zertifiziert – der Zertifizierungsdiensteanbieter durch das sogenannte „Zertifikat“. Ein qualifiziertes Zertifikat enthält folgende Daten:

- Name und Vorname des Zertifikatinhabers
- Ausstellender Zertifizierungsdiensteanbieter
- Seriennummer des Zertifikats
- Gültigkeitsdauer
- Schlüssellänge und -typ
- Signatur- und Hashverfahren<sup>1</sup>
- öffentlicher Schlüssel (Signaturprüfschlüssel) des Zertifikatinhabers
- qualifizierte elektronische Signatur des ausstellenden Zertifizierungsdiensteanbieters.

Damit kann jeder Empfänger zweifelsfrei feststellen, dass das Zertifikat von dem Zertifizierungsdiensteanbieter stammt, und dass dieses nicht manipuliert wurde oder unvollständig ist. Der öffentliche Schlüssel (Signaturprüfschlüssel) eines Zertifizierungsdiensteanbieters wurde wiederum durch die Reg TP zertifiziert und das zugehörige Zertifikat ist in deren Verzeichnisdienst abruf- und prüfbar.

#### Fazit:

Ein Zertifikat ist somit mit einem elektronischen Ausweis des Zertifikatinhabers vergleichbar. Es enthält Informationen zum Zertifikatinhaber sowie zum Zertifikataussteller und dient der Zuordnung eines öffentlichen Schlüssels (Signaturprüfschlüssel) zu einer Person. Die Echtheit des qualifizierten Zertifikats wird durch den Zertifizierungsdiensteanbieter mittels qualifizierter elektronischer Signatur bescheinigt.

<sup>1</sup> Eine Art Einwegverschlüsselung durch Bildung einer Prüfsumme. Der Hashwert ist vergleichbar mit einem Fingerabdruck.

### **Gültigkeit von Signaturschlüssel, Zertifikaten und qualifizierten elektronischen Signaturen**

Wegen der stetig voranschreitenden technischen Entwicklung der elektronischen Geräte und Software werden die Berechnungsroutinen und -parameter zur Erzeugung qualifizierter elektronischer Signaturen nur für einen bestimmten Zeitraum im voraus als geeignet beurteilt. Danach werden sie einer erneuten Prüfung unterzogen und müssen, wenn nötig, den veränderten technischen Gegebenheiten angepasst werden.

Hierzu veröffentlicht die „Regulierungsbehörde für Telekommunikation und Post (Reg TP)“ unter der Internetadresse

[www.regtp.de](http://www.regtp.de)

regelmäßig eine Übersicht der geeigneten mathematischen Verfahren. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) legt den Zeitpunkt fest, bis zu dem die Eigenschaft gilt. Ihr Zertifizierungsdiensteanbieter überprüft regelmäßig seine eingesetzte Routine und Parameter anhand dieser Liste und passt seine Produkte an die Gültigkeitszeiten an. Dabei kann der Gültigkeitszeitraum für ein Zertifikat nie länger sein als die Gültigkeiten darin enthaltener Algorithmen und Parameter. Sie werden von Ihrem Zertifizierungsdiensteanbieter frühzeitig auf geänderte Gültigkeitszeiten hingewiesen.

Daten, die über einen längeren Zeitraum qualifiziert elektronisch signiert zur Verfügung stehen sollen, müssen noch vor dem Ablauf der Gültigkeit der eingesetzten Algorithmen und Parameter, und damit bevor die Signatur ungültig wird, erneut qualifiziert elektronisch signiert werden. Die bestehende Signatur sowie ein aktueller qualifizierter Zeitstempel ist hierbei in die neue Signatur einzubeziehen.

### **Wirkung einer qualifizierten elektronischen Signatur im Rechtsverkehr**

Eine qualifizierte elektronische Signatur hat, nachdem die Vorschriften der privatrechtlichen Gesetze wie zum Beispiel das Bürgerliche Gesetzbuch (BGB) an das neue Signaturgesetz angepasst wurden, im Rechtsverkehr die gleiche Wirkung wie eine eigenhändige Unterschrift, wenn durch das Gesetz nichts anderes bestimmt ist.

### **Zuordnung der Signatur**

Alle mit dem privaten Schlüssel (Signaturschlüssel) erzeugten qualifizierten elektronischen Signaturen können grundsätzlich dem Signaturkarteninhaber zugeordnet werden, soweit

das qualifizierte Zertifikat zum Zeitpunkt der Erzeugung der qualifizierten elektronischen Signatur gültig war und

die Vermutung, dass die qualifizierten elektronischen Signaturen von ihm willentlich erzeugt wurden, nicht durch andere Fakten widerlegt werden.

### **Attribute**

Jeder Inhaber einer zertifizierten Signaturkarte erhält ein qualifiziertes Zertifikat, in dem die Zuordnung seiner Person zu dem im Zertifikat enthaltenen öffentlichen Schlüssel (Signaturprüfchlüssel) bescheinigt wird.

In das Zertifikat können auch sog. Attribute aufgenommen werden. Erlaubt sind auch gesonderte Attribut-Zertifikate, die auf ein gültiges Signaturzertifikat referenzieren. Ein Attribut steht dabei für eine besondere Eigenschaft, Stellung oder Beschränkung der Nutzung des Zertifikats auf bestimmte Anwendungen nach Art oder Umfang. Möchten Sie ihr Attribut verwenden, dann muss dies in die Signatur mit eingebunden werden. Der Empfänger muss bei Prüfung der Signatur Attribute und damit verbundene Einschränkungen beachten.

Bitte beachten Sie, dass bei der Prüfung der qualifizierten Signatur neben der Gültigkeit evtl. auch Einschränkungen angezeigt werden können.

Art und Umfang der Informationen ist von der jeweils verwendeten Signatursoftware abhängig. Beispielsweise könnte die Signatur nur im Zusammenhang eines Kaufs von medizinischen Geräten gültig sein.

Beim Erwerb der zertifizierten Signaturkarte können Sie momentan zwei verschiedene Attribute in einem Attribut-Zertifikat bzw. qualifizierten Zertifikat aufnehmen:

#### **Attribut:**

##### **Berufsrechtliche Zulassung**

Bei einer Signaturkarte von einer Kammer (z. B. Rechtsanwalts-, Steuerberater- oder Wirtschaftsprüferkammer) ist es möglich, die jeweilige Berufsbezeichnung wie z. B. Steuerberater, Rechtsanwalt, Wirtschaftsprüfer im Attributzertifikat zu speichern.

#### **Bitte beachten:**

Wenn eine Berufsbezeichnung in das Attributzertifikat aufgenommen werden soll, müssen Sie das Zertifikat bei Ihrer zuständigen Kammer beantragen.

#### **Attribut:**

##### **Monetäre Beschränkung**

Dieses Attribut wird im qualifizierten Zertifikat aufgenommen. Eine Angabe hier ermöglicht es Ihnen, eine finanzielle Obergrenze beim Einsatz des Zertifikats anzugeben. Dabei beachten Sie bitte folgende Regel: Die Wertangabe ist nur in ganzen 10er, 100er, 1000er usw. Schritten möglich. Die Beschränkung ist also

auf z. B. 10, 20 bis 90, weiter 100, 200 bis 900, weiter 1000, 2000 bis 9000 Euro und höher möglich.

### **Verzeichnisdienst (Bereitstellen der Zertifikate)**

Um eine qualifizierte elektronische Signatur zu überprüfen, muss es möglich sein, jederzeit von einer vertrauenswürdigen Stelle zu erfahren, ob das qualifizierte Zertifikat existiert oder ob es gesperrt ist. Diese Aufgabe übernimmt der Verzeichnisdienst, der von der DATEV erbracht wird. Wenn der Zertifikatinhaber bei Beantragung seiner zertifizierten Signaturkarte angegeben hat, dass sein Zertifikat abrufbar sein soll, erhält der Anfragende die Möglichkeit das Zertifikat herunterzuladen.

### **Wo kann ich Zertifikate online abfragen?**

Der Verzeichnisdienst ist automatisch aus der Anwendungssoftware GERVA anwählbar. Einzelheiten zum Verzeichnisdienst können Sie in dem Installationswegweiser zu GERVA nachlesen.

### **Sperrdienst**

Für den Empfänger einer qualifizierten elektronisch signierten Nachricht ist es sehr wichtig zu wissen, ob ein Zertifikat gültig oder gesperrt ist. Eine Sperrung kann durch den Zertifikatinhaber veranlasst werden, wenn er beispielsweise feststellt, dass seine zertifizierte Signaturkarte gestohlen wurde oder wenn er diese verloren hat. Dann muss er sein Zertifikat unverzüglich sperren, um einem Missbrauch vorzubeugen. Eine Sperrung des Zertifikats kann auch durch die Reg TP oder durch den jeweiligen Zertifizierungsdiensteanbieter erfolgen, z. B. wenn das Zertifikat aufgrund falscher Angaben erzeugt wurde.

### **Telefonische Sperrung**

Diese Möglichkeit der Sperrung existiert an 7 Tagen in der Woche und 24 Stunden an jedem Tag. Eine Sperrung, die beim Zertifizierungsdiensteanbieter eingeht, wird umgehend an den zugehörigen Verzeichnisdienst weitergegeben und dort unverzüglich vermerkt.

Zum telefonischen Sperren benötigen Sie Ihr Sperrpasswort, das Sie im Rahmen des Bestellvorgangs angeben haben. Eine Sperrung kann telefonisch unter nachstehenden kostenfreien Service-Rufnummern erfolgen:

**0800 77377227 national**

**+800 77377227 international**

## 4. Wie erhalte ich meine zertifizierte Kammer-Signaturkarte?

Insbesondere in Deutschland sind die meisten Telefone mit einer Tastatur ausgestattet, bei denen auf den einzelnen Zifferntasten zusätzlich zu der Zahl auch die Buchstaben des Alphabets aufgedruckt sind.

Die kostenfreie Service-Rufnummer hat den Vorteil, dass sich diese Sperrnummer auch als „Begriff“ darstellen lässt und so leicht zu merken ist.

Wenn Sie sich den Begriff „**Sperrcard**“ gemerkt haben, drücken Sie nach Eingabe der „0800“ die Tasten, die den Buchstaben des Begriffs entsprechen. So drücken Sie für den Buchstaben „S“ die „7“, für „P“ die „7“, für „E“ die „3“ usw.

Bei der nationalen Rufnummer können Sie nun entweder die 8-stellige Rufnummer anwählen oder die Buchstabenfolge:

**0800 SPERRCARD**

Bei der internationalen Rufnummer steht das „+“ für einen Platzhalter, der länderspezifisch zu ersetzen ist. In Deutschland steht der Platzhalter (Auslandsvorwahl) für die „00“. So können Sie nun entweder die 8-stellige Rufnummer anwählen oder die Buchstabenfolge:

**00800 SPERRCARD**

Wollen Sie aus einem anderen Land eine telefonische Sperrung vornehmen, beachten Sie bitte die entsprechenden Auslandsvorwahlen. So ist beispielsweise die Auslandsvorwahl aus Österreich, Belgien, Dänemark, Frankreich, Großbritannien, Irland, Italien, Luxemburg, Neuseeland ebenfalls die „00“, dagegen ist die Auslandsvorwahl aus den USA die „011“.

### Schriftliche Sperrung

Neben der telefonischen Sperrung gibt es auch die Möglichkeit der schriftlichen Sperrung. Auch bei einer schriftlichen Sperrung sollten Sie das Sperrpasswort angeben. Haben Sie Ihr Sperrpasswort vergessen, dann können Sie eine Sperrung nur schriftlich (mit „Briefpost“ kein Fax, kein E-Mail) veranlassen.

Ihre schriftliche Sperrung senden Sie an Ihren jeweiligen Kammer Zertifizierungsdiensteanbieter:

c/o DATEV eG  
Abteilung Sicherheit  
Sperrdienst  
90329 Nürnberg

### Exportbeschränkungen

Die Ihnen überlassene Anwendungssoftware, zusammen mit der zertifizierten Signaturkarte unterliegen aufgrund der enthaltenen Verschlüsselungskomponenten der Exportkontrolle. Betrieb und Nutzung sind innerhalb Deutschlands genehmigungsfrei. Eine Ausfuhr (und gegebenenfalls Einfuhr und Betrieb in einem Zielland) richtet sich nach dem Recht des jeweiligen Ziellandes und kann genehmigungspflichtig sein. Auch die nur vorübergehende Mitnahme, z. B. auf einem Laptop, kann einer Genehmigungspflicht unterliegen. Ein Verstoß gegen geltende Vorschriften ist strafbar. Vor einem Export sind daher die gesetzlichen Anforderungen des Ziellandes zu prüfen.

### Beantragung

Sie können die Antragsunterlagen bei der Kammer schriftlich, telefonisch oder elektronisch anfordern sowie im Internet herunterladen.

Die zertifizierte Signaturkarte ist Bestandteil des Kammer e:secure-Pakets, das zusätzlich die Software GERVA, den Kartenleser und den PIN-Brief – Teil 1 enthält.

Die Kammer schickt Ihnen als Antragsteller (AS) eine Bestellmappe. Diese beinhaltet das Antragsformular, den Datenfahrplan und die Unterrichtung.

Sie füllen den Antrag aus und unterschreiben ihn. Beachten Sie bitte, dass die E-Mail-Adresse bei der elektronischen Signatur von großer Bedeutung ist. Die Signaturanwendungs-Software bietet mit der Angabe der E-Mail-Adresse eine komfortable Benutzerführung. Es ist daher sinnvoll, dass die E-Mail-Adresse angegeben wird, mit der der Karteninhaber am häufigsten arbeitet. Wichtig ist, dass auf dem Antragsformular nichts durchgestrichen oder ausgebessert wird. Zusätzlich kopieren Sie Ihr gültiges Ausweisdokument (Vorder- und Rückseite), also entweder Ihren gültigen Personalausweis oder Reisepass und unterschreiben die Kopien. Bei der Kopie mit der Abbildung des Passfotos unterschreiben Sie bitte quer über das Foto. Wenn Sie Ihren Reisepass verwenden, dann müssen Sie eine Meldebestätigung, die nicht älter als

drei Monate sein darf, beifügen. Den unterschriebenen Originalantrag und die Kopien des Ausweisdokumentes schicken Sie an die Kammer. Falls Sie die Identifizierung und die Auslieferung durch die Deutsche Post AG (DPAG) durchführen lassen wollen, dann senden Sie die Unterlagen an die DATEV. Die Mitarbeiter der DATEV veranlassen das notwendige PostIdent-Verfahren. Bitte denken Sie daran, dass jede Unterschrift, im Zusammenhang mit der zertifizierten Signaturkarte immer so geleistet werden muss, wie im abgelichteten Ausweisdokument.

### Identifizierung des Antragstellers und Übergabe des e:secure-Pakets in der Kammer

Nach der Prüfung des Antragsatzes wird die Signaturkarte produziert und der PIN-Brief Teil 1 (Übersetzungstabelle) gedruckt. Diese Unterlagen werden an die Kammer geliefert.

Sie werden informiert, dass Ihre zertifizierte Signaturkarte in der Kammer bereit liegt und ein Abholtermin wird vereinbart.

Sie werden in der Kammer durch zwei Mitarbeiter identifiziert.

Sie geben Ihr Sperrpasswort in der Kammer direkt am PC ein. Die zertifizierte Signaturkarte wird Ihnen übergeben. Sie bestätigen, dass Sie die zertifizierte Signaturkarte erhalten haben und die Unterrichtung, die Sie in

der Bestellmappe bekommen haben, zur Kenntnis genommen haben.

Danach wird der PIN-Brief Teil 2 (6-stellige Buchstabenkombination) gedruckt und per Einwurf-Einschreiben an Sie als Antragsteller gesandt.

Sie ermitteln Ihre PIN für die qualifizierte elektronische Signatur und senden die Empfangsbestätigung im ebenfalls beiliegenden Antwortkuvert an die DATEV zurück.

Nach Überprüfung der Unterschrift im Posteingang der DATEV wird das Zertifikat in den Verzeichnisdienst eingestellt. Hierüber erhalten Sie sowie Ihre Berufskammer ein Bestätigungsschreiben.

Die Originalunterlagen werden 35 Jahre lang archiviert.

### Identifizierung des Antragstellers durch das PostIdent BASIC-Verfahren

Sie erhalten ein Anschreiben und den PostIdent BASIC-Coupon.

Bitte unterschreiben Sie das Anschreiben. Sie bestätigen dadurch die Richtigkeit Ihrer personenbezogenen Daten. Die Bestätigung ist für die Weiterbearbeitung des Antragsformulars zwingend notwendig. Mit dem unterschriebenen Anschreiben, dem PostIdent BASIC-Coupon sowie Ihrem Ausweisdokument gehen Sie zu einer Postagentur oder einer Postfiliale.

## 5. Sicherer und richtiger Umgang mit der zertifizierten Signaturkarte

Dort lassen Sie sich identifizieren. Das PostIdent BASIC-Formular und das unterschriebene Anschreiben wird durch die Post im posteigenen Postsachekouvert an die DATEV geschickt.

Im Posteingang der DATEV werden die Unterlagen auf Vollständigkeit und Korrektheit überprüft.

### Übergabe des e:secure-Pakets durch die Deutsche Post AG

Nach der Prüfung des Antragsatzes wird die Signaturkarte produziert und der PIN-Brief Teil 1 (Übersetzungstabelle) gedruckt. Die zertifizierte Signaturkarte wird durch die Deutsche Post AG an den Antragsteller zugestellt.

Sie überzeugen sich davon, dass die zertifizierte Signaturkarte wirklich im Paket enthalten ist. Dann bestätigen Sie per Unterschrift, dass Sie die zertifizierte Signaturkarte erhalten haben. Die Empfangsbestätigung schicken Sie im beiliegenden Antwortkuvert an die DATEV zurück.

Im Posteingang der DATEV werden die Unterlagen wieder auf Vollständigkeit und Korrektheit überprüft.

Danach wird der PIN-Brief Teil 2 (6-stellige Buchstabenkombination) gedruckt und per Einwurf-Einschreiben an Sie gesandt.

Sie ermitteln Ihre PIN für die qualifizierte elektronische Signatur.

Nach Überprüfung der Unterschrift im Posteingang der DATEV wird das Zertifikat in den Verzeichnisdienst eingestellt. Hierüber erhalten Sie sowie Ihre Berufskammer ein Bestätigungsschreiben.

Die Originalunterlagen werden 35 Jahre lang archiviert.

1. Wer in Besitz von einer zertifizierten Signaturkarte und PIN ist, kann vortäuschen die auf der zertifizierten Signaturkarte angegebene Person zu sein. Beachten Sie deshalb folgende Hinweise:

Schützen Sie Ihren PC vor unbefugtem Zugriff (z. B. Bootschutz).

Nehmen Sie keine Veränderungen an der mitgelieferten DATEV-Software vor. Denn nur im Auslieferungszustand ist die mitgelieferte DATEV Software GERVA signaturgesetzkonform. Den Originalzustand der DATEV Software GERVA können Sie mit Hilfe eines Prüfprogramms zur Programmintegrität sicherstellen.

Bevor Sie den PC zur Erstellung einer qualifizierten elektronischen Signatur nutzen, vergewissern Sie sich, dass sich keine Viren auf dem PC befinden. Verwenden Sie hierzu ein Virensuchprogramm. Bei Veränderungen, die z. B. durch Viren verursacht wurden, erlischt diese Gesetzeskonformität.

Die zertifizierte Signaturkarte soll ständig in persönlichem Gewahrsam aufbewahrt werden.

Die PIN sowohl zur Anwendung von GERVA, zur Verschlüsselung als auch zur qualifizierten elektronischen Signatur ist von Ihnen unter allen Umständen geheim zu halten. Lassen Sie sich bei der Eingabe der PIN nicht über die Schulter sehen. Haben Sie den Verdacht, dass dies geschehen ist, so ändern Sie Ihre PIN umgehend.

Achten Sie darauf, dass Ihre PIN nicht erraten werden kann. Geburtsdaten, Telefonnummern und Ähnliches sind ungeeignet und sollten nicht als PIN verwendet werden. Beachten Sie die Hinweise für die Wahl eines Passwortes.

Zur PIN-Eingabe bei der qualifizierten elektronischen Signatur haben Sie nur drei Versuche. Danach ist die zertifizierte Signaturkarte unbrauchbar.

Vermeiden Sie, dieselbe PIN für unterschiedliche Authentisierungsvorgänge wie z. B. Online-Banking oder PC-Zugang zu verwenden.

2. Überprüfen Sie vor dem qualifizierten elektronischen Signieren den Inhalt der Daten, die qualifiziert elektronisch signiert werden sollen, über die Darstellungskomponente, die bei der Signaturbildung automatisch geöffnet wird.

3. Für die sichere Erzeugung qualifizierter elektronischer Signaturen nach dem Signaturgesetz ist die Verwendung einer „sicheren Signaturerstellungseinheit“ notwendig. Auf der Signaturerstellungseinheit befindet sich der private (geheime) Schlüssel, der nicht auslesbar ist sowie die Software, mit der die qualifizierte elektronische Signatur erzeugt wird.

Einen weiteren Sicherheitsanker bildet die bestätigte „Signaturanwendungskomponente“. Gemäß Signaturgesetz ist bei Erzeugung einer qualifizierten elektronischen Signatur sicher-

gestellt, dass die auf dem Bildschirm angezeigten Daten auf ihrem Weg zur Signaturerstellungseinheit nicht verändert werden und eine qualifizierte elektronische Signatur nur durch den rechtmäßigen Nutzer vollzogen werden kann. Bei Prüfung der Signatur wird sichergestellt, dass der Prüfvorgang korrekt abläuft und das Prüfergebnis korrekt angezeigt wird.

Die im e:secure-Paket enthaltenen Komponenten Anwendungssoftware, zertifizierte Signaturkarte und Kartenleser erfüllen diese Anforderungen.

4. Lassen Sie Ihre zertifizierte Signaturkarte sperren, wenn:

Sie Ihre zertifizierte Signaturkarte verloren haben

Sie den Verdacht haben, dass Ihre zertifizierte Signaturkarte von Dritten manipuliert wurde.

5. Bewahren Sie Signaturkarten-Identifikationsnummer, Telefonnummer und Anschrift des Sperrdienstes schnell zugänglich auf.

6. Merken Sie sich Ihr Sperrpasswort gut und halten Sie es geheim.

7. Wenn Sie Ihre zertifizierte Signaturkarte nicht mehr benötigen, müssen Sie diese unbrauchbar machen, z. B. durch mechanisches Zerstören des Chips auf der Karte oder durch Lochen mit einem handelsüblichen Locher. Zusätzlich ist das Zertifikat (falls noch nicht abgelaufen) zu sperren.

## 6. Weitere nützliche Hinweise

### Wo kann ich weitere Informationen zur qualifizierten elektronischen Signatur erhalten?

Unter den Adressen

[www.datev.de/eseecure](http://www.datev.de/eseecure)

bzw.

[www.zda.datev.de](http://www.zda.datev.de)

haben Sie Zugriff auf die Homepage des Zertifizierungsdiensteanbieters DATEV.

Hier können Sie folgende Informationen einsehen bzw. abrufen:

allgemeine Informationen zum Zertifizierungsdiensteanbieter wie z. B. die Unterrichtung

Teilnehmerzertifikate

Übersicht der akkreditierten Zertifizierungsdiensteanbieter Kammern

Weiter erhalten Sie auch unter der Homepage-Adresse Ihrer zuständigen Kammer Informationen zur elektronischen Signatur.

### Beschwerde- und Schlichtungsverfahren

Bei Anfragen (z. B. zur Identifizierung), Problemen (z. B. Ausbleiben der Signaturkarte) oder bei Beschwerden (z. B. das Zertifikat enthält falsche Angaben) können Sie sich an nachstehende Hotline-Nummer wenden:

01805 975266

Für den Fall, dass Ihr Anliegen dort nicht zufriedenstellend gelöst werden kann, steht Ihnen zusätzlich Ihre zuständige Berufskammer zur Verfügung.

### Was kann ich tun, damit mein Sperrpasswort sicher ist?

Ein sicheres Sperrpasswort besteht aus einer Kombination von Buchstaben und Zahlen. Das Sperrpasswort sollte mindestens 6 Zeichen, möglichst aber 8 oder mehr Zeichen haben. Ein sicheres Sperrpasswort hat keinen persönlichen (z. B. Vor- und Nachnamen, Kfz-Kennzeichen usw.) oder fachlichen Bezug und es ist nicht in (auch fremdsprachlichen) Wörterbüchern enthalten.

Die Grundlage für die Wahl eines sicheren Sperrpasswortes könnte ein leicht merkbarer Satz sein wie beispielsweise „Auf dem Kanal fahren 2 Schiffe“. Nimmt man nun die Anfangsbuchstaben jedes Wortes und die im Satz enthaltene Zahl, so ergibt sich daraus das Passwort „AdKf2S“.

Dieses Passwort stellt nach heutigen Erkenntnissen ein recht sicheres Passwort dar.

Dieses Beispiel könnte auch in der Weise verändert werden, dass Sie nicht die Anfangsbuchstaben des Satzes, sondern die letzten Buchstaben von jedem Wort verwenden. Damit würde sich als Passwort „fmln2e“ ergeben.

**Bitte verwenden Sie dieses Beispiel nicht bei der Vergabe Ihres eigenen Passwortes.**

### Wer kann meine qualifiziert elektronisch signierten Dokumente lesen?

Beachten Sie, dass ein qualifiziert elektronisch signiertes Dokument weiterhin im Klartext gelesen werden kann. Um für Unberechtigte die Nicht-Lesbarkeit sicherzustellen, können Sie das Dokument verschlüsseln. Ihre zertifizierte Signaturkarte enthält hierfür die notwendigen Schlüsselpaare.

Einzelheiten hierzu können Sie dem Installationswegweiser GERVA entnehmen.