die handschriftliche Unterschrift sind im Rechtsverkehr gleichgestellt. Ausnahmen gibt es nur, wenn ein Gesetz ausdrücklich etwas anderes bestimmt.

Aus diesem Grund ist eine zuverlässige Identifizierung des Antragstellers zwingende Voraussetzung. Weitere Angaben, die in das Zertifikat aufgenommen werden sollen, müssen ebenso zuverlässig nachgewiesen werden.

Neben der elektronischen Signatur als Analogie zur handschriftlichen Unterschrift sieht die eIDAS-Verordnung auch für Siegel ein „elektrisches“ Analogon vor. Die entsprechenden Zertifikate (Siegelzertifikate) werden anstelle einer natürlichen auf eine juristische Person ausgestellt. Hierfür ist eine zuverlässige Identifizierung dieser juristischen Person sowie eines Vertretungsberechtigten erforderlich.

In der europäischen eIDAS-Verordnung ist die Rechtswirkung für elektronische Siegel geregelt. So darf einem elektronischen Siegel die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt. Für ein qualifiziertes elektronisches Siegel gilt jedoch die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

In der eIDAS-Verordnung ist ferner auch die Rechtswirkung von elektronischen Zeitstempeln geregelt, wonach einem elektronischen Zeitstempel die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil er in elektronischer Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Zeitstempel erfüllt. Jedoch gilt auch hier für qualifizierte elektronische Zeitstempel die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten.

Siehe auch §13, Absatz (1) 3 des Vertrauensdienstegesetzes (VDG).

2 Sicherheitsmaßnahmen

Jede mit Ihrem Signaturschlüssel erzeugte elektronische Signatur wird grundsätzlich Ihnen zugeordnet, wenn Ihr Zertifikat zum Zeitpunkt der Erzeugung gültig war und keine Fakten die Vermutung widerlegen, dass die qualifizierte elektronische Signatur von Ihnen willentlich erzeugt wurde. Daher ist es wichtig, dass sichergestellt wird, dass tatsächlich nur Sie mit Ihrer Karte signieren. Hierzu sind die Hinweise der folgenden Abschnitte zu beachten. Siehe auch §13, Absatz (1) 1 und 2 des VDG.

2.1 Aufbewahrung der Signaturkarte

Die elektronische Signaturkarte sollte ständig in Ihrem persönlichen Gewahrsam gehalten werden. Stellen Sie sicher, dass unbefugte Dritte keinen Zugang erhalten.

2.2 Anwendung der Signaturkarte

Obwohl in der eIDAS-Verordnung keine dedizierten Anforderungen an Kartenleser oder andere Signaturanwendungskomponenten gestellt werden, empfehlen wir - soweit möglich und verfügbar - die im Folgenden aufgeführten Hinweise zu berücksichtigen.

- Benutzen Sie Ihre elektronische Signaturkarte soweit möglich nur mit Geräten und Anwendungen, deren Sicherheit und Zuverlässigkeit von einer anerkannten Prüf- und Bestätigungsstelle bescheinigt wurde (siehe Kap. 2.3) oder die über eine entsprechende Sicherheitszertifizierung (z.B. nach CommonCriteria „CC“ oder des BSI) verfügen.
- Betreiben Sie die Geräte und Anwendungen der elektronischen Signaturkarte nur gemäß den entsprechenden Spezifikationen.
- Achten Sie darauf, dass sich auf dem zur Signatur verwendeten PC keine Viren, Trojanische Pferde oder Würmer befinden. Sorgen Sie dafür, dass der PC vor unbefugter Manipulation geschützt ist.
- Überprüfen Sie den Inhalt der Daten vor der Erstellung der qualifizierten elektronischen Signatur in einer sicheren Darstellungskomponente, die die zu signierenden Daten anzeigt. Signieren Sie keine Dokumente, die „aktive Inhalte“ wie Makros, automatische Feldfunktionen und Ähnliches enthalten, da der Empfänger sonst gegebenenfalls keine erfolgreiche Signaturprüfung durchführen kann.

- Kontrollieren Sie die Signatur der zu sendenden Daten zunächst selbst, bevor Sie die Nachricht absenden.

2.3 Einsatz zertifizierter Produkte

Aufgrund der Bedeutung für die Sicherheit bei der Anwendung von elektronischen Signaturen ist es wichtig, ausschließlich sichere Produkte, wie Chipkartenleser und Anwendungssoftware einzusetzen. Viele Hersteller lassen daher ihre produkte von einer unabhängigen Prüfstelle zertifizieren und/oder geben Hinweise zur Sicherheit Ihrer Produkte mittels einer Herstellererklärung. Wir empfehlen, ausschließlich solche Komponenten einzusetzen.

Hinweise auf solche Produkte sowie die veröffentlichten Herstellererklärungen und Zertifizierungen finden Sie auf den Webseiten der Bundesnetzagentur unter http://www.bundesnetzagentur.de (Sachgebiet „Qualifizierte elektronische Signatur“) bzw. in den Veröffentlichungen der jeweiligen Hersteller.

2.3.1 Einsatzbedingungen

Sowohl bei den Herstellererklärungen als auch bei den Bestätigungen sind Hinweise auf die Einsatzbedingungen der jeweiligen Produkte angegeben, die die Voraussetzungen für den sicheren Betrieb beschreiben. Bitte beachten Sie, dass die Sicherheit beim Einsatz der Produkte nur gewährleistet ist, wenn die dort beschriebenen Voraussetzungen eingehalten werden. Da diese in der Regel Anforderungen an die tatsächliche technische Einsatzumgebung, wie z.B. Ihren PC in Form der unterstützten Betriebssysteme, und Nutzungshinweise an Sie als Nutzer des jeweiligen Produktes angeben, ist es wichtig, dass Sie sich vor dem Einsatz des jeweiligen Produktes über dessen Einsatzbedingungen informieren und deren Einhaltung sicherstellen.

2.4 Geheimhaltung der persönlichen Identifikationsnummern (PIN)

Die Signaturkarte ist mit einer oder mehreren persönlichen Identifikationsnummern (PINs) geschützt, durch deren Eingabe verschiedene Anwendungen aktiviert werden. Optional kann die Signaturkarte auch mit einem persönlichen Freischalt-Code (PUK) versehen sein, mit dem eine durch mehrfache Falscheingabe gesperrte PIN wieder entsperrt werden kann. Diese Funktion steht nicht für PINs zur Aktivierung der Signaturfunktion Ihrer qualifizierten Signaturkarte zur Verfügung. Die nachfolgenden Hinweise gelten ohne besondere Erwähnung auch für PUKs.

Mit Hilfe der PINs weisen Sie sich als rechtmäßiger Benutzer der elektronischen Signaturkarte aus. Dies setzt natürlich voraus, dass nur Sie Ihre PINs kennen. Die PINs sind daher von Ihnen unter allen Umständen geheim zu halten und in regelmäßigen Abständen zu ändern. Vermeiden Sie, dass jemand Kenntnis von Ihren PINs erlangt und notieren Sie sie auf keinen Fall auf der Karte.

Insbesondere bei der Eingabe von PINs ist darauf zu achten, dass diese nicht von Dritten beobachtet werden kann. Sollten Sie die Vermutung haben, dass Dritte Kenntnis von einer Ihrer PINs erlangt haben, ändern Sie diese unverzüglich.

Achten Sie bei der Auswahl einer PIN darauf, dass diese nicht zu erraten ist. Verwenden Sie insbesondere keine trivialen Zahlenkombinationen (111111, 123456, etc.) oder Daten aus Ihrem persönlichen Umfeld (Geburtsdaten, Telefonnummern, etc.) Vermeiden Sie auch die Verwendung derselben PIN für unterschiedliche Authentisierungsvorgänge wie z.B. Online-Banking oder PC-Zugang.

Bitte wählen Sie die PIN zur qualifizierten Signatur stets unabhängig von PINs für andere Anwendungen der Signaturkarte, beispielsweise Verschlüsselung, um einer Verwechslung bei rechtlich unterschiedlich bewerteten Vorgängen vorzubeugen.

Vermeiden Sie Fehleingaben von PINs, da die Signaturkarte nach dreimaliger Falscheingabe einer PIN automatisch gesperrt wird und nicht mehr entsperrt werden kann.

2.5 Erneuerung von 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 Bundesnetzagentur unter der Internet-Adresse www.bundesnetzagentur.de regelmäßig eine Übersicht mathematischer Verfahren, die nach Angaben des BSI (Bundesamt für Sicherheit in der Informationstechnik) unter der Berücksichtigung internationaler Standards und der Beteiligung von Experten aus Wissenschaft und Wirtschaft als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Ihr Vertrauensdiensteanbieter überprüft regelmäßig seine eingesetzten Algorithmen, Schlüssellängen und Parameter u.a. anhand dieser

Liste und passt seine Produkte an die Gültigkeitszeiten an. Bei Bedarf werden Sie von Ihrem Vertrauensdiensteanbieter 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. Dies muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

0211-77008-456

infoline@dgnservice.de

4.1 Beschwerde und Schlichtungsmöglichkeiten

Im Falle von Beschwerden und Reklamationen können Sie sich an das Kundencenter der DGN wenden:

0211-77008-456

reklamation@dgnservice.de

5 Datenschutz

5.1 Datenschutzbestimmungen

Vertrauensdiensteanbieter unterliegen den gesetzlichen Datenschutzbestimmungen. Die DGN erhebt keine Daten, die nicht für die Zertifizierungstätigkeit und den Betrieb der Vertrauensdienste notwendig sind. Die erhobenen Daten werden vor dem Zugriff von Unbefugten geschützt. Die dazu erforderlichen Maßnahmen ergreift die DGN.

Die zur Verfügung gestellten Daten nutzt die DGN nur innerhalb ihres Zertifizierungsbetriebes. Eine weitergehende kommerzielle Nutzung findet nicht statt.

5.2 Weitergabe von Daten und Einsicht durch zuständige Stellen

Eine Weitergabe und Einsicht der persönlichen Daten erfolgt nach Vorgabe des Vertrauensdienstegesetz (VDG):

VDG §8 Abs. 2:

„Der Vertrauensdiensteanbieter darf personenbezogene Daten einer Person, die Vertrauensdienste nutzt, den zuständigen Stellen übermitteln,

1. soweit die zuständigen Stellen die Übermittlung nach Maßgabe der hierfür geltenden Bestimmungen verlangen, da die Übermittlung erforderlich ist

a) für die Verfplgung von Straftaten oder Ordnungswidrigkeiten,

b) zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder

c) für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden, oder

2. soweit Gerichte die Übermittlung im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.

5.3 Persönliche Einsicht

Zusätzlich wird Ihnen das Recht eingeräumt, Einblick in die über Sie gespeicherten Daten zu gewähren:

DSGVO Art. 15 Abs.1 a-g:

„Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogenen Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) *die Verarbeitungszwecke;*

b) *die Kategorien personenbezogener Daten, die verarbeitet werden:*

c) *die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;*

d) *falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;*

e) *das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;*

f) *das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;*

g) *wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;.“*

6 Weitere Informationsquellen zur elektronischen Signatur

Die Veröffentlichung dieses Dokuments sowie CPS erfolgt auf den jeweiligen Seiten zur Antragstellung und unter
http://www.dgnservice.de/trustcenter/public/dgnservice/index.html.

Im Internet finden Sie weitere Informationen rund um die elektronische Signatur und andere Vertrauensdienste u.a. an diesen Stellen:

- http://www.bundesnetzagentur.de
  (Sachgebiet „Qualifizierte elektronische Signatur“)

  Dies ist die Seite der Bundesnetzagentur, die als zuständige Aufsichtsstelle für die Vertrauensdienste elektronische Signatur, elektronische Siegel, elektronische Zeitstempel und Dienste für die Zustellung elektronischer Einschreiben im Sinne der eIDAS-Verordnung für Deutschland benannt wurde. Der Bundesnetzagentur obliegt die Pflege und Bereitstellung der deutschen Vertrauensliste nach eIDAS durch die Vertrauensdiensteanbieter.

  Über die Seite der Bundesnetzagentur finden Sie u.a. auch eine Auflistung bestätigter Produkte und hinterlegter Herstellererklärungen (siehe Kap. 2.3).

- http://www.bsi.de

  Dies ist die Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI), welches als zuständige Aufsichtsstelle für Vertrauensdienste im Bereich der Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung in Deutschland benannt wurde. Dort finden Sie viele Informationen zu rechtlichen und technischen Fragen.

7 Glossar

eIDAS	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol: technisches Protokoll zur Prüfung der Gültigkeit von Zertifikaten
QSEE	Qualifizierte elektronische Signaturerstellungseinheit (in der Regel eine Smartcard bzw. Signaturkarte)
VDA	Vertrauensdiensteanbieter