Die qualifizierte elektronische Signatur

Informationen zu qualifizierten elektronischen Signaturen und qualifizierten Zertifikaten des Vertrauensdiensteanbieters
medisign GmbH

Sehr geehrte Kundin, sehr geehrter Kunde,

mit dem gesteigerten Aufkommen der elektronischen Medien wächst auch der Anteil der elektronischen Kommunikation. Die Kommunikation per E-Mail beispielsweise ist heute so normal geworden wie das Telefonat. Das Bedürfnis nach Sicherheit und Vertrauen spielt hier sowohl im privaten als auch im geschäftlichen Umfeld eine immer größere Rolle. Wie können Sie nun aber sicherstellen, dass Sie mit demjenigen kommunizieren, für den sich Ihr Gegenüber ausgibt? Im Gegensatz zur Face-to-Face Kommunikation sind hier zusätzliche Instrumente erforderlich, um eine Vertrauensbasis zu schaffen.

Der Schlüssel zu dieser Vertrauensbasis ist die qualifizierte elektronische Signatur. Dieser Leitfaden soll Ihnen einen Überblick über die Funktionen der qualifizierten elektronischen Signatur und deren Vorteile bieten. Im Folgenden erfahren Sie, wozu man qualifizierte elektronische Signaturen benötigt, wie qualifizierte elektronische Signaturen funktionieren und was im Umgang mit Ihrer Signaturkarte zu beachten ist.

Sie werden über alle wichtigen Belange hinsichtlich der qualifizierten elektronischen Signatur informiert. Es ist daher sinnvoll und erforderlich, dass Sie die vorliegende Unterrichtung sorgfältig lesen und zur Kenntnis nehmen. Weitere Informationen zur Nutzung und möglichen Nutzungsbeschränkungen zu den von Ihnen genutzten Zertifikaten sowie dem Betrieb des Vertrauensdiensteanbieters finden Sie in den AGB sowie im Certification Practice Statement (CPS). Siehe hierzu auch Kapitel 6.

Inhaltsverzeichnis

1 Elektronische Signatur

1.1 Zweck elektronischer Signaturen

Die qualifizierte elektronische Signatur nimmt für die elektronische Kommunikation eine zentrale Stellung ein. Hier ist es erforderlich, dass die Kommunikationspartner einander vertrauen und die kommunizierten Inhalte nicht unbemerkt verfälscht werden können. Die elektronische Kommunikation gewinnt sowohl im privaten als auch im beruflichen Leben zunehmend an Bedeutung. Bei diesem Datenaustausch kommt es häufig vor, dass der Kommunikationspartner nicht persönlich bekannt ist. Da z.B. das Kommunikationsmedium E-Mail von sich aus keine Überprüfung der Absenderangaben bietet, kann sich der Empfänger von elektronischen Daten nicht immer darauf verlassen, dass die Identität des Absenders den übermittelten Angaben auch tatsächlich entspricht. Weiterhin besteht die Möglichkeit, dass Dritte die übermittelten Daten manipulieren. Die qualifizierte elektronische Signatur stellt hier eine Technik zur Verfügung, die diese Probleme beseitigt.

Durch die qualifizierte elektronische Signatur kann die Identität des Absenders zweifelsfrei festgestellt werden und es ist nachprüfbar, ob die gesendeten Daten unverfälscht vorliegen.

Sonderformen der elektronischen Signatur stellen elektronische Siegel und Zeitstempel dar (Siehe Kapitel 1.8 Gesetzliche Wirkung). Wie beim elektronischen Siegel wird bei einem Zeitstempel die Technologie der Signatur verwendet. Jedoch wird zusätzlich die gesetzliche Zeit von einer vertrauenswürdigen Quelle in die Signatur einbezogen.

Zeitstempel und Siegel eignen sich ebenso, die Unversehrtheit von Dokumenten und Daten (Informationen) zu überprüfen bzw. nachzuweisen. Siegel können zusätzlich die Herkunft von Informationen und Zeitstempel das Vorhandensein von Informationen zu einem bestimmten Zeitpunkt belegen.

Die Erläuterungen zur Funktionsweise der Signatur gelten in gleicher Weise für elektronische Siegel und Zeitstempel.

1.2 Funktionsweise

Die Technik der qualifizierten elektronischen Signatur beruht auf zwei unterschiedlichen mathematischen Schlüsseln, die einander eindeutig zugeordnet sind, jedoch nicht voneinander abgeleitet werden können. Jeder Teilnehmer erhält ein individuelles Schlüsselpaar. Einen dieser Schlüssel bezeichnet man als privaten oder geheimen Schlüssel, den anderen als öffentlichen Schlüssel.

Der private Schlüssel (Signaturschlüssel) ist auf der Signaturkarte gespeichert und kann nicht ausgelesen werden. Dadurch wird gewährleistet, dass der private Schlüssel geheim bleibt, nicht einmal dem Hersteller der Signaturkarte oder dem Erzeuger des Schlüssels sind dieser private Schlüssel bekannt. Als sicheres Speichermedium werden Chipkarten eingesetzt, deren Sicherheit von unabhängigen Stellen geprüft wurde. Die Signaturkarten werden auch „Sichere Signaturerstellungseinheiten“ (SSEE) oder „Qualifizierte elektronische Signaturerstellungseinheit“ (QSEE) genannt. Die Signatur wird unter Nutzung des privaten Schlüssels direkt auf der Signaturkarte erstellt, so dass auch bei der Herstellung bzw. Personalisierung der private Schlüssel die Signaturkarte nicht verlässt.

Die beiden Schlüssel gehören in dem Sinne zusammen, dass mit dem privaten Schlüssel erzeugte Signaturen von Daten nur mit dem dazugehörigen öffentlichen Schlüssel (Signaturprüfschlüssel) überprüft werden können.

Der Signaturprüfschlüssel darf jedem bekannt gegeben werden. Zu diesem Zweck wird der öffentliche Schlüssel zertifiziert, das heißt er wird Teil eines Zertifikats, in dem Angaben über den Besitzer, in der Regel dessen Name oder ein unverwechselbares Pseudonym, enthalten sind. Dieses Zertifikat wird von einem Vertrauensdiensteanbieter (VDA), wie z.B. medisign, ausgestellt, signiert und auf die Signaturkarte aufgebracht.

Damit ist die Zugehörigkeit des Signaturprüfschlüssels zu dem Besitzer der Signaturkarte nachgewiesen und eine Verifikation der Signatur bestätigt nicht nur, dass die Daten seit der Signaturerstellung nicht verändert wurden, sondern auch, dass sie vom Besitzer der Karte signiert wurden.

1.3 Zertifikate

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

Mit Hilfe eines Zertifikates kann der Empfänger eines elektronisch signierten Dokuments die Identität des Absenders feststellen.

Ein qualifiziertes Zertifikat enthält u. a. folgende Angaben:

- Vornamen und Name des Signaturschlüssel-Inhabers oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym (als solches zu erkennen am angehängten „:PN“)
- den öffentlichen Schlüssel (Signaturprüfschlüssel) des Signaturschlüssel-Inhabers
- die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdienste-anbieters benutzt werden kann
- die Zertifikatsnummer
- das Datum, ab dem das Zertifikat gültig ist
- das Datum, bis zu dem das Zertifikat gültig ist
- Angaben zum Vertrauensdiensteanbieter, der das Zertifikat ausgestellt hat
- die Bestätigung, dass es sich um ein qualifiziertes Zertifikat handelt
- Informationen über den zuständigen Verzeichnisdienst für die Überprüfung der Gültigkeit des Zertifikats
- gfs. weitere optionale Attribute des Signaturschlüssel-Inhabers (s. Abschnitt 1.3.2)

Mit dem zugehörigen Zertifikat kann jeder die Echtheit eines signierten Dokumentes prüfen.

Zur Bestätigung, dass die im Zertifikat enthaltenen Angaben korrekt sind und um eine Manipulation des Zertifikats auszuschließen, wird jedes Zertifikat vom ausstellenden Vertrauensdiensteanbieter signiert.

1.3.1 Attribute

Ein Attribut steht für eine besondere Eigenschaft des Zertifikatsinhabers oder eine Beschränkung der Nutzung des Zertifikates auf bestimmte Anwendungen nach Art und Umfang. Attribute werden auf Antrag des Antragstellers in das Zertifikat aufgenommen.

1.3.2 Arten von Attributen

Vertretungsmacht für eine natürliche Person:

Ist der Antragsteller rechtlich zur Unterschrift für eine weitere Person bevollmächtigt, so kann dies in seinem Zertifikat vermerkt werden.

Voraussetzung hierfür ist die schriftliche Einwilligung der Person, für die eine Bevollmächtigung besteht, sowie deren erfolgreiche Identifizierung bei der Antragstellung.

Mit der Vertretungsvollmacht wird dem Signaturkarteninhaber das Recht eingeräumt, im Namen der vertretenen Person zu signieren. Die zu vertretende Person hat neben dem Antragsteller auch das Recht, das Zertifikat zu sperren (s. Kapitel 1.7 dieser Belehrung).

Berufsbezogene Angaben:

Die bestehenden gesetzlichen Vorgaben ermöglichen u.a. auch die Aufnahme der Berufsbezeichnung in ein Zertifikat. Zur Aufnahme dieses Attributes muss ein Nachweis über die Berufsbezeichnung erbracht werden. Ist der Antragsteller beispielsweise ein Arzt, so muss die zuständige Ärztekammer dies bestätigen. Neben dem Antragssteller hat auch die bestätigende Stelle das Recht, Zertifikate zu sperren, wenn die Bedingungen für die Nutzung der Berufsbezeichnung nicht mehr gegeben sind.

1.3.3 Beschränkungen nach Art und Umfang:

In einem Zertifikat können beliebige Beschränkungen abgebildet werden. Ob eine Beschränkung sinnvoll ist oder nicht, liegt im eigenen Ermessen. Eine Überprüfung von Seiten des Vertrauensdiensteanbieters erfolgt hierbei nicht. Beispielsweise kann eine sogenannte monetäre Beschränkung eingerichtet werden, um die Gültigkeit z.B. für finanzielle Transaktionen zu begrenzen. Gemäß aktueller Rechtsprechung hat die monetäre Beschränkung nur Gültigkeit für unmittelbare Geldgeschäfte (z.B. Überweisungsvorgänge o.ä). Bei Verwendung zur Signatur z.B. von allgemeinen Schriftsätzen dient die Signatur dem Nachweis

der Urheberschaft und die monetäre Beschränkung bleibt unbeachtlich. Sollte das Ziel bestehen, die Beschränkung auch auf allgemeine Erklärungen auszudehnen, um möglicherweise Haftungsrisiken einzugrenzen, so ist nicht das Feld „monetäre“, sondern „allgemeine Beschränkung“ zu verwenden.

1.4 Vorgehen bei der Signatur von Daten

Das konkrete Vorgehen bei der Signatur Ihrer Daten oder E-Mails ist abhängig von der verwendeten Software. Diese wird zusammen mit dem Kartenleser im Sprachgebrauch der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS) als Signaturerstellungseinheit (im Folgenden auch SAK) bezeichnet. Die grundlegenden Schritte bei der Erstellung einer Signatur sind aber immer gleich und können wie folgt beschrieben werden:

1) Starten Sie Ihre Signaturanwendung, nachdem Sie das zu signierende Dokument, z.B. eine E-Mail oder ein PDF-Dokument, erstellt haben. Für die elektronische Signatur muss Ihre Signaturkarte im Kartenlesegerät gesteckt sein.

2) Die Signaturanwendungen zeigen Ihnen nun auf dem Bildschirm noch einmal die zu signierenden Daten zur Überprüfung an. Dies dient zu Ihrer eigenen Sicherheit.

3) Nach Bestätigung des Inhalts durch die Eingabe Ihrer persönlichen Signatur-PIN wird nun eine qualifizierte elektronische Signatur erstellt.

1.5 Vorgehen bei der Signaturprüfung

Zur Überprüfung der elektronischen Signatur benötigt Ihre SAK (genauer: der Teil der Software zur Signaturprüfung - Signaturprüfsoftware) den Signaturprüfschlüssel des Signierenden. Dieser ist im Zertifikat des Signierenden enthalten, das mit dem signierten Dokument übertragen wird und/oder im lokalen Zertifikatsspeicher der Signaturprüfsoftware vorhanden ist. Die Überprüfung signierter Daten erfordert die Onlineüberprüfung der Zertifikatsgültigkeit anhand eines Statusinformationsdienstes. Nur so kann festgestellt werden, ob das Zertifikat zum Zeitpunkt der Signaturerstellung existiert hat sowie gültig und nicht gesperrt war. Eine signaturgesetzkonforme Signaturprüfsoftware als Teil der SAK zeigt die relevanten Inhalte des signierten Dokuments in einer eigenen sicheren Darstellungskomponente (ebenfalls Teil der

SAK) an, unabhängig von der Anwendung, mit der das Dokument erstellt wurde. Ist der Zugriff auf den Statusinformationsdienst nicht möglich, kann nur überprüft werden, ob das signierte Dokument nicht verändert, das Zertifikat nicht manipuliert wurde, das Gültigkeitsende des Zertifikats noch nicht erreicht ist und welcher VDA das Zertifikat ausgestellt hat. Es fehlt in diesem Fall jedoch die Information, ob das Zertifikat zum Zeitpunkt des Signierens gültig und nicht gesperrt war, z.B. weil es dem Zertifikatsinhaber gestohlen wurde.

1.6 Vertrauensdiensteanbieter (VDA)

Signaturprüfungen gemäß eIDAS können darüber hinaus auch mittels eines sogenannten Validierungsdienstes durchgeführt werden. Für Hinweise zu deren Nutzung wenden Sie sich bitte an den jeweiligen Anbieter des Dienstes.

1.6.1 Aufgaben

Neben der zuverlässigen Identifizierung und Registrierung der Antragsteller übernimmt ein Vertrauensdiensteanbieter unter anderem die sichere Erzeugung des Schlüsselpaares auf der Signaturkarte und verbindet den Signaturprüfschlüssel (öffentlicher Schlüssel) mit den persönlichen Daten des zukünftigen Signaturkarteninhabers in einem Zertifikat. Dieses Zertifikat wird vom VDA signiert. Damit dient der VDA als Vertrauensanker für die Korrektheit der Angaben im Zertifikat. Der VDA kann mögliche Nutzungsbeschränkungen über die Schlüsselverwendung in das Zertifikat eintragen. Des Weiteren besteht eine Beschränkung dahingehend, dass mit dem zertifizierten Signaturschlüssel keine weiteren Zertifikate ausgestellt werden können.

Da Zertifikate eine begrenzte Gültigkeitsdauer haben und auch gesperrt werden können, betreibt der VDA einen öffentlich erreichbaren Statusinformationsdienst (Verzeichnisdienst), der elektronisch Auskunft über den jeweiligen Status des Zertifikats gibt (siehe Kap. 1.5).

Der VDA stellt zusätzlich das Zertifikat bei Zustimmung des Inhabers der Öffentlichkeit über einen öffentlichen Verzeichnisdienst, der über das Internet zugänglich ist, zum Abruf bereit.

1.6.2 Qualifikationsstatus des Vertrauensdiensteanbieters

In der eIDAS-Verordnung werden verschiedene Vertrauensdienste definiert, u.a. elektronische Signatur- und Zeitstempeldienste sowie elektronischen Siegel. Weitere Vertrauensdienste, die

von der eIDAS-Verordnung umfasst werden, wie elektronische Einschreiben, Zertifikate für Website-Authentifizierungen und die Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten, werden derzeit von medisign nicht angeboten.

Die oberste Instanz (die sogenannte Root-Instanz) der Infrastruktur für die Vertrauensdienste nach eIDAS bilden eigene Root-Zertifikate, von denen die entsprechenden CA-Zertifikate abgeleitet werden, die die (qualifizierten) Endteilnehmer-Zertifikate oder Siegel erzeugen, und die Zertifikate des Zeitstempeldienstes.

Die Einhaltung der in der eIDAS-Verordnung vorgegebenen (Sicherheits-)Anforderungen wird mittels einer sog. Konformitätsbestätigung von einer anerkannten Konformitätsbewertungs-stelle nachgewiesen. Dazu werden regelmäßig, spätestens alle 2 Jahre, entsprechende Audits durchgeführt und der Konformitätsbewertungsbericht der jeweils zuständigen Behörde, für die hier betrachteten Vertrauensdienste ist das die BNetzA, zugeleitet. Der von der Aufsichtsstelle (BNetzA) u.a. anhand dieses Berichts verliehene Status eines qualifizierten Vertrauensdiensteanbieters nach eIDAS dient somit als Bestätigung, dass der VDA die Anforderungen an qualifizierte Vertrauensdiensteanbieter erfüllt und die zum Betrieb der von ihm angebotenen und in die Vertrauensliste aufgenommenen qualifizierten Vertrauensdienste notwendigen technischen und organisatorischen Sicherheitsmaßnahmen umgesetzt hat.

Die BNetzA ist zudem dafür zuständig, die qualifizierten Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste in eine Vertrauensliste aufzunehmen und diese zu veröffentlichen.

Der Vertrauensdiensteanbieter darf die qualifizierten Vertrauensdienste erst dann erbringen, nachdem diese durch die Bundesnetzagentur in die Vertrauensliste übernommen wurden.

1.7 Sperrung von Zertifikaten

Eine qualifizierte elektronische Signatur ist nur dann gültig, wenn zum Zeitpunkt der Signaturerstellung das Zertifikat zum verwendeten Schlüssel gültig war. Ein Zertifikat ist ungültig, wenn

a) der betreffende Betrachtungszeitpunkt außerhalb des Gültigkeitszeitraums des Zertifikats liegt (vor „gültig ab“ oder nach „gültig bis“) oder

b) das Zertifikat vor dem betreffenden Betrachtungszeitpunkt gesperrt wurde.

Die Sperrung eines Zertifikats kann von folgenden Personen oder Organisationen in Auftrag gegeben werden:

a) Bundesnetzagentur

b) Vertrauensdiensteanbieter

c) Attributbestätigende Stelle (z.B. zuständige Ärztekammer)

d) Dritte Person, soweit das Zertifikat oder Attributzertifikat Angaben über die Vertretungsmacht für diese dritte Person enthält

e) Signaturschlüssel-Inhaber oder Bevollmächtigter

Die Autorisierung zur Sperrung eines Zertifikats wird bei Antragstellung über ein sicheres Verfahren geprüft.

1.8 Gesetzliche Wirkung

Die qualifizierte elektronische Signatur hat im Rechtsverkehr die gleiche Wirkung wie eine handschriftliche Unterschrift. Mit anderen Worten: Die qualifizierte elektronische Signatur und 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 Signaturen und Siegel geregelt. Demnach darf einer elektronischen Signatur bzw. 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 Signaturen bzw. 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 beim jeweiligen Hersteller 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. 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.

2.4.1 Card Access Number (CAN)

Einige Signaturkarten verfügen über eine sogenannte kontaktlose Schnittstelle. Diese ermöglicht die Nutzung der Signaturkarte ohne Einstecken in einen Kartenleser, sondern z.B. einfach durch Auflegen auf ein geeignetes Kartenterminal. Für die Absicherung der Kommunikation zwischen der Signaturkarte und dem Kartenterminal ist die Eingabe der „Card Access Number“ (CAN) erforderlich. Diese ist auf Ihrer Signaturkarte aufgedruckt und sollte –

genau wie die PIN - vor Unberechtigten geheim gehalten werden. Lassen Sie daher keine Ablichtungen Ihrer Signaturkarte zu, auf denen die CAN nicht unkenntlich gemacht ist.

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.

2.6 Verlust oder Missbrauchsverdacht

Um eine missbräuchliche Nutzung Ihrer Signaturkarte zu verhindern, sollten Sie bei der Vermutung, dass Dritte Kenntnis von einer Ihrer PINs erlangt haben, diese unverzüglich ändern.

Wenn Sie Ihre Signaturkarte verloren haben oder sie Ihnen gestohlen wurde, ist der VDA umgehend über diesen Umstand zu informieren. In diesen Fällen wird die Signaturkarte gesperrt (genauer: die enthaltenen Zertifikate), die Verfahren zur Sperrung sind in Kapitel 3 „Verfahren zur Sperrung“ beschrieben.

Beachten Sie hierzu folgende Hinweise:

- Bei Verlust, Entwendung oder dem Verdacht der Manipulation durch Dritte müssen die Zertifikate der Karte umgehend gesperrt werden.
- Bewahren Sie die Telefonnummer und Anschrift des Sperrdienstes immer griffbereit auf.
- Merken Sie sich Ihr Sperrpasswort gut und halten Sie es geheim.

2.7 Einsatz von Multisignatur-Signaturkarten

Bei der Nutzung von sogenannten Multisignatur-Signaturkarten, das sind Signaturkarten, bei der mit der Eingabe einer (Signatur-)PIN die Erzeugung von mehreren Signaturen ohne weitere PIN-Eingabe ermöglicht wird, werden besondere Sicherheitsanforderungen an die Einsatzumgebung gestellt. Da alle durchgeführten Signaturen Ihnen als Signaturschlüssel-Inhaber zugerechnet werden, sind Sie zu Ihrem eigenen Schutz für die Einhaltung der folgenden Maßnahmen verantwortlich.

2.7.1 Physische Absicherung

Schützen Sie Ihre Signaturkarte, insbesondere bei unbeaufsichtigtem Betrieb, vor unbefugtem Zugriff, z.B. durch eine abschließbare Umgebung. Beachten Sie, dass alle durchgeführten Signaturen Ihnen als Signaturschlüssel-Inhaber zugerechnet werden.

2.7.2 Logische Absicherung

Für die Anwendung im eIDAS-Kontext gilt der Einsatz zertifizierter Produkte als Empfehlung, sofern entsprechende Produkte verfügbar sind. Beachten Sie dabei die ordnungsgemäße

Installation der Produkte und die Einhaltung der vorgesehenen Einsatzumgebung gemäß den zugehörigen Handbüchern und Bestätigungen.

Prüfen Sie die Integrität der eingesetzten Produkte und der zugrunde liegenden Plattform.

Schützen Sie die entsprechenden IT-Systeme z.B. durch den Einsatz von aktueller Antivirensoftware vor Schadsoftware wie Viren oder Trojanern.

Sorgen Sie für eine vertrauenswürdige Systemadministration.

Sollte die Signaturkarte in einem IT-Netz und nicht nur auf einem Standalone-System eingesetzt werden, sorgen Sie für eine vertrauenswürdige Netzinfrastruktur und, falls es sich nicht nur um ein lokales Netz handelt, sorgen Sie für eine vertrauenswürdige Anbindung an externe Kommunikationsnetze wie z.B. dem Internet.

Sollten Sie Zweifel an der ausreichenden Sicherheit der von Ihnen genutzten oder vorgesehenen Einsatzumgebung haben, kontaktieren Sie eine anerkannte Prüf- und Bestätigungs- bzw. Konformitätsbewertungsstelle (siehe http://www.bundesnetzagentur.de/).

3 Verfahren zur Sperrung

Die Sperrung von Zertifikaten kann auf verschiedenen Wegen beantragt werden. Empfohlen ist die telefonische Sperrung, da hier zwischen Sperrwunsch und technischer Durchführung die geringste Verzögerung entsteht.

Für eine Sperrung der Signaturkarte sind unabhängig von der Art der Übermittlung des Sperrauftrags folgende Daten nötig:

- Name des Antragstellers
- Name des Zertifikatsinhabers, falls nicht der Inhaber selbst beantragt
- Seriennummern der zu sperrenden Zertifikate
    - falls nicht möglich: ID der Signaturkarte
    - falls nicht möglich: Nummer des Antrags auf Ausstellung der Signaturkarte
- Sperrpasswort bei telefonischer Sperrung, Personalausweis oder Reisepass bei persönlichem Erscheinen und eigenhändige Unterschrift bei schriftlicher Sperrung

3.1 Telefonische Sperrung

Diese Möglichkeit der Sperrung existiert an 7 Tagen in der Woche und 24 Stunden an jedem Tag. Eine Sperrung, die beim Vertrauensdiensteanbieter 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 angegeben haben. Eine Sperrung kann telefonisch unter 0180 5 034430 erfolgen. (Anrufer zahlt 0,14 Euro pro Minute. Preisangaben beziehen sich nur auf Anrufe aus dem deutschen Festnetz. Anrufe vom Mobilfunk (max. € 0,42 pro Minute) und aus dem Ausland können abweichen.)

3.2 Schriftliche Sperrung

Senden Sie den Sperrauftrag mit den folgenden Angaben: Name, Vorname, Titel und Zertifikatsnummer/n an die folgende Adresse:

medisign Trustcenter -
Postfach 102144
40012 Düsseldorf

Wenn Sie die Sperrung schriftlich vornehmen, wird Ihre Sperrberechtigung anhand Ihrer persönlichen Angaben und Ihrer handschriftlichen Unterschrift überprüft. Als Unterschriftenprobe dient dazu die Unterschrift, die Sie im Rahmen der Antragstellung geleistet haben. Die Sperrung wird dann an dem Tage durchgeführt, an dem das Schreiben beim Sperrdienst des Vertrauensdiensteanbieters eingetroffen ist.

3.3 Persönliches Erscheinen

Sie können auch persönlich beim VDA eine Sperrung veranlassen. Die medisign hat ihren Sitz unter der folgenden Anschrift:

medisign GmbH
Richard-Oskar-Mattern-Straße 6
40547 Düsseldorf

Bitte bringen Sie für diesen Vorgang Ihren Personalausweis oder Reisepass zur Identifizierung mit.

4 Hilfe und Kontakt

Bei Anfragen, Problemen oder Beschwerden, die die Signaturkarte oder das Zertifikat bzw. die qualifizierte elektronische Signatur betreffen, können Sie sich an das Kundencenter der medisign GmbH wenden:

0211-77008390

4.1 Beschwerde und Schlichtungsmöglichkeiten

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

0211-77008-390

reklamation@medisign.de

5 Datenschutz

5.1 Datenschutzbestimmungen

Vertrauensdiensteanbieter unterliegen den gesetzlichen Datenschutzbestimmungen. Die medisign 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 medisign.

Die zur Verfügung gestellten Daten nutzt die medisign 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 erfolgen nur nach Vorgabe gesetzlicher Bestimmungen. Das Vertrauensdienstegesetz (VDG) formuliert hierzu folgende Regelungen:

VDG §8 Abs. 2-4:

„(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.

(3) Die Vertrauensdiensteanbieter haben die Übermittlung zu dokumentieren. Die Dokumentation ist zwölf Monate aufzubewahren.

(4) Hat die zuständige Stelle ein Verlangen nach Datenübermittlung nach Absatz 2 Nummer 1 gestellt, so unterrichtet sie die betroffene Person über die erfolgte Übermittlung der Daten. Von der Unterrichtung kann abgesehen werden, solange die Wahrnehmung der gesetzlichen Aufgaben gefährdet würde und solange das Interesse der betroffenen Person an der Unterrichtung nicht überwiegt. Fünf Jahre nach der Übermittlung kann endgültig von der Benachrichtigung abgesehen werden, wenn die Voraussetzungen für die Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.

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 unter http://www.medisign.de.

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