

Qualifiziert signierte und verschlüsselte Gutachten via E-Mail an den elektronischen Gerichtsbriefkasten senden

von Dipl.-Ing. (Assessor) Jochem Kierig und Dipl.-Ing. (FH) Kerstin Klein

Immer mehr Gerichte und Behörden bieten die Möglichkeit, Gutachten in elektronischer Form an den elektronischen Gerichtsbriefkasten zu senden. Welche Voraussetzungen Sie dafür erfüllen müssen und welche Firmen derzeit qualifizierte Signaturen auf dem Markt anbieten, haben wir für Sie recherchiert. In dem folgenden Fachbeitrag stellen wir sie Ihnen vor.

1 Rechtsgrundlage

Mit dem Justizkommunikationsgesetz (JKomG) werden der Zivilprozess und die Fachgerichtsbarkeiten für eine elektronische Aktenbearbeitung geöffnet. Die Verfahrensbeteiligten haben die Möglichkeit, elektronische Kommunikationsformen gleichberechtigt neben der – herkömmlich papiergebundenen – Schriftform oder der mündlichen Form rechtswirksam zu verwenden. Dies bedeutet für Sachverständige, die für Gerichte tätig sind, dass Sie Ihre Gutachten per E-Mail einreichen können, wenn diese nach dem Signaturgesetz (SigG) qualifiziert signiert sind (vgl. Abschnitt 5).

Gemäß § 12 Abs. 2 Satz 2 Muster-Sachverständigenordnung (MSVO) 2001 des DIHK, sind Gutachten im Fall einer elektronischen Übermittlung mit einer qualifizierten Signatur zu versehen. Gemäß den Richtlinien zur MSVO 2001 (11.2) können die Gutachten zusätzlich mit der gescannten Unterschrift und dem gescannten Rundstempel versehen werden.¹⁾

Auch das Bürgerliche Gesetzbuch sieht in § 126 ff. vor, dass die gesetzlich vorgeschriebene handschriftliche Form durch die elektronische Form ersetzt werden kann, wenn der Aussteller der Erklärung seinen Namen hinzufügt und das elektronische Dokument mit einer qualifizierten Signatur nach dem SigG versieht – vorausgesetzt, es geht aus dem Gesetz nichts Gegenteiliges hervor.

2 Das elektronische Gerichts- und Verwaltungspostfach“ (EGVP)

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik, dem Bundesfinanzhof, dem Bundesverwaltungsgericht, dem Land Nordrhein-Westfalen und der Firma Bremen Online Service GmbH & Co.KG (bos) wurde das „Elektronische Gerichts- und Verwaltungspostfach“ (EGVP) entwickelt. EGVP ist eine Software, mit der nach einmaliger Installation die elektronische Kommunikation mit Gerichten und Behörden sicher durchgeführt werden kann. Die Software kann kostenfrei unter www.egvp.bund.de/software heruntergeladen werden.

Die Gestaltung und Handhabung des Programms erinnert stark an gängige E-Mail-Programme. Es gibt jedoch entscheidende Unterschiede in der Zustellungssicherheit der elektronischen Nachrichten.

Eine E-Mail, die mit Programmen wie z.B. Outlook im SMTP-Protokoll versendet wird, ist vergleichbar mit einer offenen Postkarte, die per Post verschickt wird. Deren Inhalt ist von „jedermann“ les- und ggf. sogar manipulierbar, ohne dass es die Kommunikationspartner bemerken. Dahingegen ist der Versand von E-Mails mit dem EGVP im OSCI-Protokoll mit einem Versand eines Einschreibens mit Rückschein vergleichbar. Über jede E-Mail, die im sog. „Gerichtsbriefkasten“ beim Gericht eingeht, wird ein Prüfprotokoll erstellt. Neben der zeitlichen Erfassung des Nachrichteneingangs wird zusätzlich die Signatur²⁾ des Absenders geprüft. Durch das Prüfprotokoll und durch den Versand der Nachrichten im OSCI-Protokoll, bietet das EGVP den Kommunikationspartnern eine wesentlich höhere Sicherheit als die meisten anderen E-Mail-Programme.

Das EGVP ist jedoch ausschließlich für die elektronische Kommunikation mit Gerichten und Behörden vorgesehen und nicht für die Kommunikation zwischen Privatpersonen. [1]

3 Elektronischer Rechtsverkehr auf E-Mail Basis (elba)

Die Verwaltungsgerichtsbarkeiten des Landes Rheinland-Pfalz setzen hingegen den Microsoft BizTalk Server für die Abwicklung des elektronischen Rechtsverkehrs ein. Dieser Server verarbeitet die eingehenden E-Mails automatisch weiter. Er prüft die Gültigkeit der qualifizierten Signatur sowie die verwendeten Dateiformate. Der Absender der elektronischen Dokumente erhält wie beim EGVP automatisiert eine Eingangsbestätigung per E-Mail. Interessante Informationen über den elektronischen Rechtsverkehr auf E-Mail Basis (elba) in Rheinland-Pfalz, findet man in der gleichnamigen Informationsbroschüre, die auf den Seiten der rheinlandpfälzischen Verwaltungsgerichtsbarkeiten als pdf-Dokument heruntergeladen wer-

1) Vgl. diesbezüglich Beitrag in WFA 1/2005, S. 29.

2) Vgl. Abschnitt 4.

den kann (www.justiz.rlp.de/justiz)¹⁾. Die Broschüre beschreibt den genauen Ablauf des elektronischen Rechtsverkehrs mit den Verwaltungsgerichtsbarkeiten in Rheinland-Pfalz. Die Fachgerichtsbarkeiten in Niedersachsen arbeiten ebenfalls mit dem System elba.

4 Empfohlene Datenformate und Datengrößen

Auf der Internetseite des EGVP (www.egvp.bund.de/bearbeitung/index.htm) findet man für die einzelnen Gerichtsbarkeiten, die mit dem EGVP zusammenarbeiten, Informationen zu den akzeptierten Datenformaten und Datengrößen. Gerichte und Staatsanwaltschaften in Frankfurt/Main sowie Kassel stellen beispielsweise u.a. folgende Anforderungen:

„Aus technischen und organisatorischen Gründen dürfen einer Nachricht nicht mehr als zehn Dateien angehängt werden, deren Gesamtvolumen 10 Megabyte (MB) nicht überschreiten darf. [Bei größeren Datenmengen besteht die Möglichkeit, diese in einem komprimierten Format beispielsweise als so genannte Zip-Datei zusammenzufassen.] Bei der Übermittlung soll, sofern bekannt, in dem Betreff der Nachricht das gerichtliche Aktenzeichen angegeben werden; bei verfahrenseinleitenden elektronischen Dokumenten und in Fällen, in denen das gerichtliche Aktenzeichen sonst noch nicht bekannt sein kann, soll die jeweilige Verfahrensart (z.B. Klage, Revisionschrift, Beschwerde) schlagwortartig angegeben werden.

Die elektronische Nachricht soll enthalten:

- a) das gerichtliche Aktenzeichen, bei Neueingängen die schlagwortartige Bezeichnung der Verfahrensart
- b) eine schlagwortartige Bezeichnung des Inhalts und
- c) die Kurzbezeichnung der Hauptbeteiligten.

Zu einem Dokument gehörige Anlagen sollen denselben Dateinamen erhalten wie das Hauptdokument, erweitert um die Bezeichnung „Anlage“ und eine dreistellige fortlaufende Nummer.“ [2]

In Tabelle 1 sind alle vom EGVP anerkannten Dateiformate aufgeführt.

Bis auf eine Abweichung in der zugelassenen Datenmenge decken sich die Anforderungen von elba Rheinland-Pfalz überwiegend mit denen des EGVP. Eine E-Mail an die Verwaltungsgerichtsbarkeiten in Rheinland-Pfalz sollte inkl. Dateianhang eine Datenmenge von 5 MB nicht überschreiten. Bei größeren Dateien über 5 MB besteht die Möglichkeit, diese wie auch beim EGVP, in einem komprimierten Format (beispielsweise als Zip-Datei) zusammenzufassen. Erfahrungen aus der Praxis haben jedoch gezeigt, dass auch E-Mails mit einem Volumen von bis zu 10 MB fehlerfrei übermittelt werden können. [3]

1) Rubrik Gerichte, Bereich Elektronischer Rechtsverkehr, Verwaltungsgericht Koblenz, Informationsbroschüre zum elektr. Rechtsverkehr.

Die Anforderungen von elba Niedersachsen entsprechen weitestgehend denen des EGVP.

Format	Version / Einschränkungen	Erstellung durch Programm (Beispiel)
ASCII (American Standard Code for Information Interchange)	<ul style="list-style-type: none"> Ohne Versionsbeschränkung als reiner Text ohne Formatierungs-codes und ohne Sonderzeichen 	Notepad
Unicode	<ul style="list-style-type: none"> Ohne Versionsbeschränkung als reiner Text ohne Formatierungs-codes 	
RTF (Rich Text Format)	<ul style="list-style-type: none"> soweit mit Microsoft Office darstellbar; Version 1.0 bis 1.6. ohne Erweiterung für Word 2000 	Microsoft Word
Adobe PDF (Portable Document Format)	<ul style="list-style-type: none"> Version 1.0 bis 1.4. (sofern mit Adobe Reader 6.0 lesbar) 	Adobe-Acrobat-Writer; Free-PDF
Microsoft Word	<ul style="list-style-type: none"> keine aktiven Komponenten Word 97, Word 2000 (Version 8 oder 9), Word XP 	Microsoft Word
XML (Extensible Markup Language)	<ul style="list-style-type: none"> Sofern mit Internet Explorer 5.x darstellbar; eine zum Dokument gehörige DTD (Document Type Definition) muss zugeordnet sein 	
TIFF (Tag Image File Format)	<ul style="list-style-type: none"> Version 6 oder niedriger (CCITT/TTS Gruppe 4, sofern Grafik-Daten übermittelt werden, z.B. Fax, eingescannte Unterlagen als Anlagen) 	Adobe Photoshop

Tab. 1: Anerkannte Dateiformate des EGVP [2]

5 Die elektronische Signatur; Unterschiede und Anwendung

Im Sinne des Artikels 2 der Europäischen Richtlinie über elektronische Signaturen und des § 2 des Gesetzes über Rahmenbedingungen für elektronische Signaturen bezeichnet die **elektronische Signatur** Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Die elektronische Signatur besteht aus einer alphanumerischen Kombination²⁾, die anderen elektronischen Daten (bspw. Word-Dokumenten, pdf-Dokumenten etc.) beigefügt wird. Alternativ ist es möglich, die elektronische Signatur mit dem signierten Dokument zu verknüpfen, so dass nur eine und keine zwei Dateien zu verwalten sind³⁾. Zudem dienen Signaturen der

2) Buchstaben- und Zahlenkombination.

3) Bei einem pdf-Dokument ist es möglich, die Signatur unmittelbar im Dokument durchzuführen, so dass keine separate „Signatur-Datei“ entsteht.

Personen-Authentifizierung. Die elektronische Signatur lässt sich in 3 Arten unterscheiden.

Wenn bislang bei der herkömmlichen papiergebundenen Schriftform keine handschriftliche Unterschrift erforderlich war, so ist bei Verwendung der elektronischen Kommunikationsform eine **einfache Signatur**, also z.B. der Namenszusatz oder eine eingescannte Unterschrift ausreichend. Die einfache Signatur ist weder in der zuständigen Europäischen Richtlinie noch in den jeweiligen deutschen Gesetzen und Verordnungen erwähnt.

Die **fortgeschrittene elektronische Signatur** (definiert in Artikel 2 Nr. 2, Europäische Richtlinie 1999/93 EG) ist eine elektronische Signatur, die ausschließlich dem Unterzeichner zugeordnet ist.

Sie ermöglicht die Identifizierung des Unterzeichners (Prüfung erfolgt durch das Internet beim zuständigen Trustcenter¹⁾) und lässt den Empfänger der Nachricht erkennen, ob die Daten manipuliert wurden. Im Gegensatz zu qualifiziert signierten Daten besitzen fortgeschritten signierte Daten keine Rechtssicherheit.

Die **qualifizierte Signatur** wird auf Basis eines qualifizierten Zertifikats²⁾ (§ 2 Signaturgesetz) ausgestellt und muss als solches erkennbar sein. In erster Linie enthält die qualifizierte Signatur Angaben zum Zertifikatshersteller (Trustcenter) und zur unterzeichnenden Person.

Das Zertifikat muss außerdem Signaturprüfdaten enthalten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen. Des Weiteren müssen die Gültigkeitsdauer sowie der Identitätscode des Zertifikats angegeben werden.

Das qualifizierte Zertifikat ist aufgrund der hohen Anforderungen der handschriftlichen Unterzeichnung weitestgehend gesetzlich gleichgestellt (§ 126 ff. BGB). Aus diesem Grund muss ein **Gutachten**, das **in elektronischer Form bei dem Gericht eingereicht** wird, mit einer **qualifizierten Signatur** „unterzeichnet“ werden. Signaturen die durch ein qualifiziertes Zertifikat erstellt wurden, sind vor Gericht als Beweis zugelassen. Zu den Anwendungsbereichen der qualifizierten Signatur gehören z.B.: elektronische Vertragsunterzeichnung, E-Billing (elektronische Rechnungsstellung; Berechtigung zum Vorsteuerabzug entsprechend den Vorgaben des Umsatzsteuergesetzes), e-Vergabe (elektronisch durchgeführte Vergabe aus öffentlicher oder privater Hand) sowie die elektronische Steuererklärung (ELSTER). Zudem können Digitalfotos mit einer elektronischen Signatur kameraintern signiert

werden und sind somit als Beweismittel vor Gericht geeignet. [4]

In besonders empfindlichen Bereichen ist die Verwendung der elektronischen Signatur nicht rechtsgültig. Dazu gehören z.B. die Kündigung von Arbeitsverhältnissen, Zeugnisse, Bürgschaften sowie notarielle Beurkundungen. [5]

6 Beantragung eines Zertifikats

Unter anderem werden Zertifikate für die fortgeschrittene und qualifizierte Signatur von den Trustcentern der Deutschen Post, der Deutschen Sparkassen Verlag GmbH, der Deutschen Telekom sowie D-TRUST angeboten. Die Bestellung der Zertifikate erfolgt meist über das Internet. Nachdem der Interessent auf der Website des Zertifikatdiensteanbieters ein Antragsformular ausgefüllt hat, erhält der Kunde vom Zertifizierungsdiensteanbieter i.d.R. ein Signaturpaket. Dieses Paket enthält einen Registrierungsantrag, eine Karte, die Signatursoftware, eine Einmal-PIN zum Zertifikatsdownload, ggf. ein Formular für das Postident-Verfahren³⁾ und eine Informations-CD-ROM inkl. Bedienungsanleitung.

Die Registrierung bei den oben genannten Anbietern läuft bis auf D-Trust jeweils über das Postident-Verfahren. Antragsteller von D-Trust müssen sich z.B. bei den D-Trust Registrierungsstellen und bei den Registrierungsstellen der IHKs identifizieren lassen.

Kunden, die eine Signaturkarte bei der Deutschen Post, dem Deutschen Sparkassen Verlag oder beispielsweise der Deutschen Telekom beantragen, können den Komfort des Postident-Verfahrens in Anspruch nehmen. Das Postident-Verfahren hat den großen Vorteil, dass sich der Kunde mit geringem Zeitaufwand deutschlandweit flächendeckend bei einer Filiale der Deutschen Post registrieren lassen kann. Der Antragsteller geht mit den unterzeichneten Formularen zu einer Filiale der Deutschen Post, die die Leistungen des Postident-Verfahrens anbietet, und lässt sich in Verbindung mit seinem Personalausweis oder Reisepass identifizieren. Der Postangestellte überprüft die Unterschrift des Antrages mit der Unterschrift im Ausweis und vergleicht den Antragsteller mit dem Foto im Ausweis. Der Zertifizierungsanbieter erhält von der Deutschen Post den unterschriebenen Antrag, eine Ausweiskopie sowie ein Protokoll über die Identifizierung. Nach Erhalt dieser Unterlagen bekommt der Kunde eine E-Mail, die ihn zum Download seines Zertifikats berechtigt, zugeschickt.

1) Trustcenter dienen der Herstellung von Zertifikaten, die auf Chipkarten gespeichert werden. Betreiber von Trustcentern sind bspw. Deutscher Sparkassen Verlag GmbH, T-Systems und die Deutsche Post Com GmbH.

2) Ein Zertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird.

3) Identifizierung der Unterschrift auf dem Registrierungsantrag und Identifizierung der Person anhand eines Personalausweises oder Reisepasses durch einen speziell geschulten Mitarbeiter bei einer Filiale der Deutschen Post. Der Registrierungsantrag wird von der Deutschen Post an den Zertifizierungsdiensteanbieter weitergeleitet. Eine Postdienststelle, die die persönliche Identifikation in Ihrer Nähe anbietet, finden Sie auf der Homepage der Deutschen Post (www.deutschepost.de, Rubrik „Über uns / Deutsche Post Filialen / Filial-Suche“).

7 Chipkarte, Kartenlesegerät und Software

Um eine fortgeschrittene oder qualifizierte Signatur vorzunehmen werden eine Chipkarte, ein Kartenlesegerät sowie eine spezielle Software benötigt. Anbieter qualifizierter Zertifikate bieten in den meisten Fällen ein Komplettpaket in ihrem Programm an. Das Zertifikat des Zertifikatsanbieters sowie ein privater und ein öffentlicher Schlüssel¹⁾ werden auf einer persönlichen **Chipkarte** gespeichert. Die Daten werden in Verbindung mit einem **Kartenlesegerät** an den Computer übermittelt. Das Kartenlesegerät dient der PIN-Eingabe und kann durch einen USB-Anschluss an den Computer angeschlossen werden. Die Kartenlesegeräte werden in 3 Geräteklassen eingeteilt. Bei Geräten der **Klasse 1** erfolgt die Eingabe der PIN über die Tastatur des Computers. Es besteht die Gefahr, dass sog. Trojaner die PIN über die Tastatur auslesen. Das Gerät besitzt kein Display. Diese Geräte sind für eine qualifizierte Signatur und somit auch für den elektronischen Rechtsverkehr nicht geeignet. Kartenlesegeräte der **Klasse 2** enthalten ein eigenes Tastenfeld zur PIN-Eingabe. Dies ermöglicht eine sichere Eingabe. Diese Geräte sind sowohl für eine qualifizierte Signatur wie auch für HBCI (Homebanking Computer Interface) geeignet. Die Anzeige der PIN erfolgt wie bei Geräten der Klasse 1 meist auf dem Computerbildschirm. Dies stellt jedoch keine große Sicherheitsgefährdung dar. Geräte der **Klasse 3** besitzen neben einem eigenen Tastenfeld immer ein eigenes Display. Sie entsprechen den höchsten Sicherheitsanforderungen und sind, neben den Möglichkeiten mit einer qualifizierten Signatur zu unterzeichnen und HBCI zu betreiben, auch für den Einsatz einer Geldkarte geeignet. Kartenlesegeräte der Klasse 3 kosten mit ca. 95,00 € ungefähr 45,00 € mehr als Geräte der Klasse 2.

Die Firma Cherry GmbH bietet als einzige uns bekannte Firma ein Kartenlesegerät der Klasse 2 an, das in eine Computertastatur integriert ist. Die PIN-Eingabe erfolgt



Abb. 1: Klasse-3-Chipkartenleser von REINER SCT

1) Vgl. Abschnitt 9 „Verschlüsselte Dateien“.

hierbei über den Nummern-Block. Da die Tastatur jedoch keine ZKA-SigAPI unterstützt, ist ein Zertifikatsdownload bei S-TRUST nicht möglich. Deshalb wird von dieser Lösung abgeraten.

Die Kartenlesegeräte müssen für den Einsatz von qualifizierten Signaturen dem SigG und der SigV entsprechen. Dies setzt voraus, dass die Geräte von der Bundesnetzagentur anerkannt sind.

Anerkannte Kartenlesegeräte sind auf der Homepage der Bundesnetzagentur zu finden:

(www.bundesnetzagentur.de, Rubrik „Elektronische Signatur / Bestätigte Produkte / Chipkartenleser“). Hersteller anerkannter Geräte sind u. a. ReinerSCT Kartengeräte GmbH & Co. KG, Siemens AG Österreich, Kobil Systems GmbH und Orga Kartensysteme GmbH.

Die **Software** für das Kartenlesegerät sowie eine Software zur Durchführung der Signatur werden vom jeweiligen Anbieter mitgeliefert.

8 Wie signiere ich ein Dokument?

Es gibt zwei Möglichkeiten ein Dokument zu signieren. Beispielhaft wird in den folgenden zwei Abschnitten erklärt wie ein Microsoft Word-Dokument signiert wird.

1. Möglichkeit

Microsoft Word-Dokumente können unter zu Hilfenahme eines sog. Viewers direkt aus Microsoft Word signiert werden. Das Word-Dokument wird als Bild (meist Tiff-Format) angezeigt. Nach Eingabe der persönlichen PIN in das Kartenlesegerät wird eine Signatur für das geöffnete Dokument erstellt. Zusätzlich zu dem Dokument existiert nach dem Signieren eine „Signatur-Datei“. Die „Signatur-Datei“ erhält neben dem Namen des Word-Dokuments eine Zahlenkombination sowie ein „s“ für Signatur. Die Datei enthält alle wichtigen Informationen über die Signatur. Durch einen Doppelklick auf die Signatur-Datei können diese Informationen überprüft werden. Abbildung 2 zeigt wie eine Überprüfung der Signatur aussehen kann.

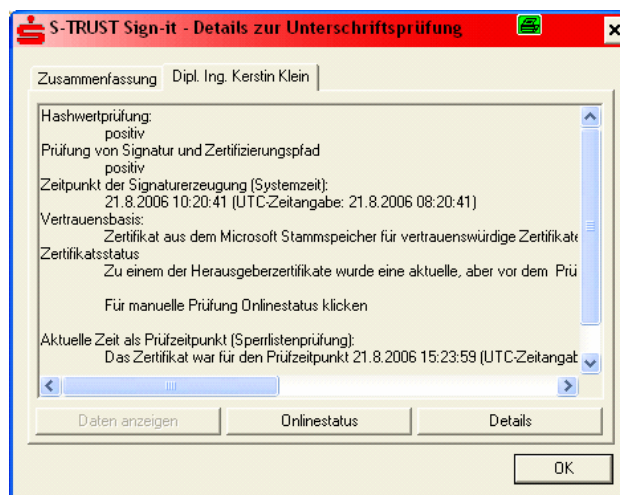


Abb. 2: Beispiel einer Signaturprüfung

2. Möglichkeit

Alternativ kann ein Dokument im „Arbeitsplatz“ oder auf dem Desktop signiert werden. Das zu signierende Dokument wird in einem separaten Verzeichnis gespeichert. Durch Anklicken des Dokuments mit der rechten Maustaste kann man den Befehl „signieren“ auswählen. Nach Eingabe der PIN ist das Dokument signiert. Wie bereits zuvor beschrieben entsteht auch hier bei Microsoft Word-Dokumenten eine separate Datei, die die Signatur nachweist.

Bei Dokumenten im pdf-Format ist es möglich innerhalb des Dokuments zu signieren, so dass keine zweite Signatur-Datei entsteht. Es empfiehlt sich alle Dokumente im pdf-Format abzuspeichern, da somit gewährleistet ist, dass sich bspw. aufgrund unterschiedlicher Microsoft Word-Versionen die textliche Gestaltung des Dokuments nicht mehr verändert. Zudem hat es den Vorteil, dass man keine 2 Dateien (Signatur und signiertes Dokument) verwalten muss.

Beim Signieren einer Datei wird ein sog. Hash-Wert gebildet. Man könnte ihn auch als Doc-ID oder Fingerabdruck bezeichnen, da dieser Wert für jedes Dokument einmalig ist. Wird das Dokument geändert so stimmt der Hashwert des Originaldokuments nicht mehr mit dem des geänderten Dokuments überein und der Kommunikationspartner erkennt, dass das Dokument manipuliert wurde.



Abb. 3: Bildliche Darstellung der Verschlüsselung während einer Signierung [4]

Der Hash-Wert wird derzeit in der Regel mit 1.024 bit (RSA) verschlüsselt¹⁾ (Bei S-TRUST sind es aktuell 1.728 bit). Der private Schlüssel auf der Chipkarte wird durch die Eingabe der PIN freigegeben, d.h. die Karte wird geöffnet. Die Verschlüsselung des Hash-Werts findet auf dem Chip der Karte statt. Die verschlüsselten Daten werden im Anschluss wieder in den Computer zurück geschickt.

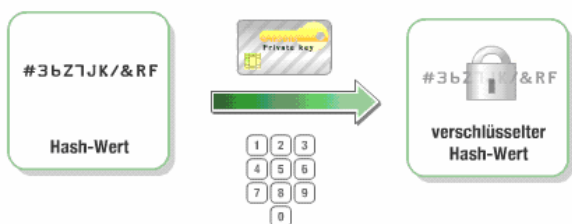


Abb. 4: Bildliche Darstellung der Verschlüsselung des Hash-Werts durch die Eingabe der PIN [4]

1) vgl. Abschnitt 9 „Verschlüsselte Dateien“.

Diese hier kompliziert erscheinenden Vorgänge werden im Hintergrund von der Software automatisiert durchgeführt.

9 Verschlüsselte Dateien

Der Versand einer unverschlüsselten E-Mail ist ähnlich dem einer Postkarte per Post. Theoretisch kann man diese E-Mail bzw. Karte lesen und ggf. deren Inhalt manipulieren. Verschlüsselte E-Mails sind hingegen mit einem verschlossenen Brief vergleichbar. Die Verschlüsselung von Daten ist bisher nicht gesetzlich geregelt. Es ist jedoch im Interesse des Verfassers, seine Nachricht vor den Augen Dritter zu schützen.

Die Verschlüsselung sowie die Signatur, basieren auf einer Public Key Infrastruktur (PKI). Sowohl bei der Signatur als auch bei der Datenverschlüsselung kommt eine **asymmetrische Verschlüsselung** zum Einsatz. Asymmetrisch bedeutet, dass immer zwei verschiedene Schlüssel verwendet werden; der private Schlüssel (private key) und der öffentliche Schlüssel (public key). Die Schlüssel ergänzen sich gegenseitig. Daten, die mit dem öffentlichen Schlüssel „abgeschlossen“ wurden, können nur mit dem privaten wieder „aufgeschlossen“ werden.

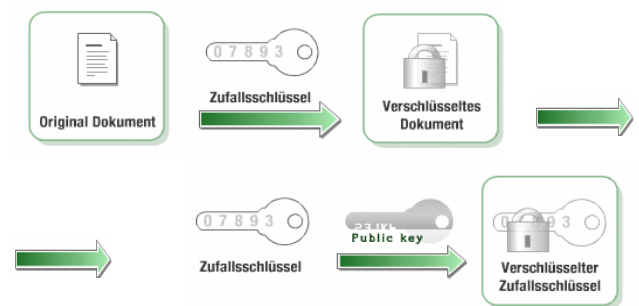


Abb. 5: Bildliche Darstellung der Daten-Verschlüsselung [3]

Zunächst wird das Dokument mit einem Zufallsschlüssel im Triple DES Verfahren verschlüsselt. Das heißt, das Dokument wird dreimal hintereinander mit 192 bit verschlüsselt. Hier kommt bei den meisten Zertifikatsanbietern eine 1.024bit RSA-Verschlüsselung zum Einsatz (dies entspricht 10^{1024} Schlüsseln)²⁾. Die Deutsche Sparkassen Verlag GmbH verschlüsselt bereits mit einer Schlüssellänge von 1.728 bit. Um dem technischen Fortschritt Stand zu halten, werden im nächsten Jahr auch andere Zertifizierungsdiensteanbieter in Deutschland mit 1.728 bit verschlüsseln. Der Zufallsschlüssel wird dann noch einmal mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.

Der öffentliche Schlüssel des Empfängers ist in ein Verschlüsselungszertifikat integriert und kann im Verzeich-

2) Zum Vergleich: Die Anzahl der Atome im Universum beträgt ca. 10^{77} . Mit einer 1024bit-Verschlüsselung lassen sich 10^{1024} Schlüssel generieren.

nisdienst des Trustcenters abgerufen und auf dem Computer gespeichert werden. Es ist auch möglich, den öffentlichen Schlüssel auszulesen und ihn per E-Mail an Kommunikationspartner zu versenden. Alle gespeicherten öffentlichen Schlüssel werden von der „Zertifikats-Software“ beim Verschlüsseln eine Nachricht automatisch angezeigt.

Das verschlüsselte Dokument und der verschlüsselte Zufallsschlüssel werden zusammen archiviert oder per E-Mail an die Kommunikationspartner versandt, mit deren öffentlichem Schlüssel verschlüsselt wurde.

Möchten Sender und Empfänger sicher gehen, dass die Nachricht unverändert zugestellt wird, sollte zusätzlich signiert werden. Denn nur durch eine Signatur ist eine Veränderung der Daten für den Empfänger erkennbar.

Zur Entschlüsselung eines Dokuments benötigt man den privaten Schlüssel. Dieser ist auf der persönlichen Chipkarte gespeichert und kann nur mit entsprechender PIN angewendet werden. Der private Schlüssel ist nicht auslesbar.

Ist der Zufallsschlüssel von der Software entschlüsselt, kann auch das gesamte Dokument entschlüsselt werden.

Durch die Eingabe der PIN bei der Entschlüsselung der Daten ist gewährleistet, dass nur der Karteninhaber Zugriff auf die Daten erhält.

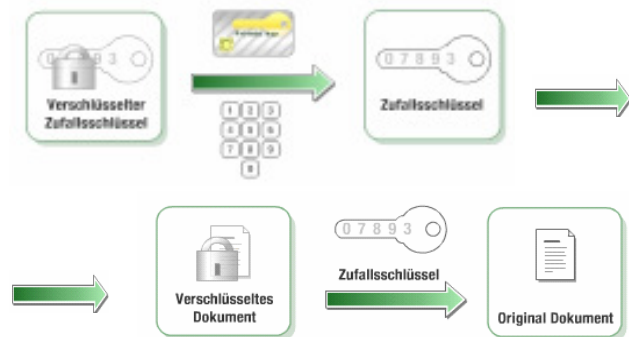


Abb. 6: Bildliche Darstellung der Daten-Entschlüsselung [3]

Die Trustcenter, die den digitalen Ausweis (Zertifikat) erzeugt haben, verfügen nicht über die geheimen Informationen auf der Chipkarte, die für die Entschlüsselung von Daten notwendig sind. Ist die Chipkarte bzw. der dazugehörige PIN nicht mehr verfügbar, weil sie bspw. verloren gegangen sind, können die mit dem öffentlichen Schlüssel verschlossenen Daten nicht mehr geöffnet bzw. hergestellt werden.

10 Trustcenter

Wie bereits erläutert erhält man die Signaturkarte von einem Trustcenter. Die Unterhaltung eines Trustcenters ist aufgrund der hohen Sicherheitsanforderungen und technischen Einrichtungen sehr kostenintensiv. Aus diesem Grund gibt es in Deutschland nur wenige Trustcenter. Zu den Betreibern eines Trustcenters gehören unter anderem

die Deutsche Post Com GmbH, die Deutsche Telekom AG, DATEV, die Deutsche Sparkassen Verlag GmbH, die Zertifizierungsstelle der Bundesnotarkammer, D-Trust u.a. Für uns als Immobilienbewertungssachverständige schränkt sich die Wahl der Trustcenter jedoch ein. Nicht alle Trustcenter stehen für jedermann zur Verfügung. Das Angebot des Trustcenters der Bundesnotarkammer steht beispielsweise ausschließlich Notaren zur Verfügung. Die DATEV stimmt ihre Software auf die Berufsgruppe der Steuerberater ab. Angebote dieses Trustcenters sind ausschließlich über den persönlichen Steuerberater zu beziehen. Für die Immobilienbewertungssachverständigen kommen die **Deutsche Post Com GmbH, die Deutsche Telekom AG, D-Trust¹⁾ sowie die Deutsche Sparkassen Verlag GmbH** in Betracht.

Einige Institutionen bieten ein Paket für die elektronische Signatur an und kaufen die erforderlichen Chipkarten bei den am Markt vertretenen Trustcentern ein. Die Industrie- und Handelskammern bieten beispielsweise Signaturen in Kooperation mit D-Trust an.

Wir haben für Sie die konditionell interessantesten Angebote der Trustcenter miteinander verglichen und in der folgenden Tabelle ausgewertet. Das Angebot der einzelnen Anbieter beinhaltet eine Chipkarte mit 2 Zertifikaten sowie eine Software des jeweiligen Trustcenters zur Anwendung der Zertifikate. Ein Zertifikat dient der qualifizierten Signatur und ein zweites Zertifikat dient der Ver- und Entschlüsselung von Daten. Nach Ablauf der ersten Vertragsdauer ist eine erneute Beantragung notwendig (Signtrust nach einem Jahr, T-Telesec nach drei Jahren und S-TRUST nach vier Jahren).

Die Deutsche Post Com GmbH sowie die Deutsche Telekom AG (vgl. Tab. 2) sind von der Bundesnetzagentur akkreditiert und somit für die Zusammenarbeit mit Gerichten, die bereits den elektronischen Rechtsverkehr unterstützen, anerkannt.

Die Deutsche Sparkassen Verlag GmbH ist noch nicht akkreditiert, hat aber bereits den Betrieb eines Zertifizierungsdienstes bei der Bundesnetzagentur angezeigt (§ 4 Abs. 3 SigG i.V.m. §§ 1, 2 SigV). Das Trustcenter der Deutschen Sparkassen Verlag GmbH wird bereits von allen für die Bewertungssachverständigen relevanten Gerichtsbarkeiten anerkannt.²⁾

Hinweis

Beim Trustcenter der Deutscher Sparkassen Verlag GmbH besteht zudem die Möglichkeit, sich anstelle bei einer Postfiliale direkt bei einem Sparkassen-Institut zu

1) Die Preise von **D-Trust** sind im Vergleich zu den in Tab. 2 aufgeführten Anbietern zu hoch. Aus diesem Grund ist dieser Anbieter für uns nicht empfehlenswert.

2) Quelle: Deutscher Sparkassen Verlag GmbH für Verwaltungsgerichtsbarkeiten und schriftliche Auskunft der Firma BOS Bremen Online Services für EGVP sowie Informationsbroschüre elba für Verwaltungsgerichtsbarkeiten Rheinland-Pfalz.

	T-Telesec Deutsche Telekom AG		Signtrust Deutsche Post Com GmbH		S-TRUST Sign it Deutscher Sparkassen Verlag GmbH	
Chipkarte für 4 Jahre	ca. 164,00 €*	–	ca. 156,00 €*	–	ca. 108,90 €/**	+
Registrierung	deutschlandweit flächendeckend durch die Filialen der Deutschen Post gesichert	+	deutschlandweit flächendeckend durch die Filialen der Deutschen Post gesichert	+	deutschlandweit flächendeckend durch die Filialen der Deutschen Post gesichert	+
Software Installation	Die Software erfordert die Installation des Programms Adobe Reader 6.0. Die Software arbeitet ausschließlich mit dieser Version zusammen. Dies bedeutet, dass aktuellere Versionen dieses Programms deinstalliert werden müssen.	–	Keine Probleme bei der Installation	+	Keine Probleme bei der Installation	+
Anwendung der Software	Verständlich, ermöglicht einen schnellen Einstieg	+	Verständlich, ermöglicht einen schnellen Einstieg	+	Verständlich, ermöglicht einen schnellen Einstieg	+
Für den elektronischen Rechtsverkehr anerkannt	von der Bundesnetzagentur zugelassen	+	von der Bundesnetzagentur zugelassen	+	von den Verwaltungsgerichten zugelassen	+
Ergebnis	Befriedigend	–	Gut	+/-	Sehr gut	+

* Preis pro Chipkarte inkl. qualifiziertem Zertifikat zzgl. MwSt. (Stand Juni 2007).

** Preis für WF-Kunden gem. Rahmenvertrag zwischen dem WertermittlungsForum und S-TRUST.

Tab.2: Vergleich Zertifizierungsdiensteanbieter

registrieren. Alle Sparkassen-Registrierungsstellen können unter www.s-trust.de/registrierungsstellen eingesehen werden.

11 Empfehlung | Partner WertermittlungsForum

Anfang Januar 2007 haben wir für Sie eine Rahmenvereinbarung mit der Deutschen Sparkassen Verlag GmbH abgeschlossen. Wir halten die Deutsche Sparkassen Verlag GmbH für einen zuverlässigen Partner, der gute Qualität zu günstigen Konditionen anbietet. Aufgrund der Rahmenvereinbarungen war es uns möglich, einen **Paketpreis**¹⁾ für Sie – inkl. Postident-Verfahren – von lediglich **108,90 €** zu erzielen (gültig für 4 Jahre). Sie erhalten durch die Rahmenvereinbarungen mit der Deutschen Sparkassen Verlag GmbH einen günstigen Einstiegspreis mit niedrigen Folgekosten.

Das für Sie zusammengestellte Paket enthält eine Chipkarte mit 2 Zertifikaten sowie eine Software des Trustcenters zur Anwendung der Zertifikate. Ein Zertifikat dient der qualifizierten Signatur und ein weiteres Zertifikat dient der Ver- und Entschlüsselung von Daten. Die Sparkassen Verlag GmbH ermöglicht Ihnen durch das Postident-Verfahren eine einfache Registrierung vor Ort. Die Software des Anbieters wurde durch unser Haus intensiv ge-

testet. Wir stellten fest, dass sich die Software problemlos installieren lässt und die Anwendung benutzerfreundlich gestaltet ist. Wir erfuhren bei fachlichen Fragen eine kompetente und sehr engagierte Beratung. Die Kosten des Gesamtpaketes enthalten neben den zuvor genannten Zertifikaten und der Chipkarte auch die Grundgebühr des Zertifikats für eine Laufzeit von 4 Jahren. Nach unseren Recherchen werden die Produkte von S-TRUST bei den Gerichten, die bereits den elektronischen Rechtsverkehr anbieten, anerkannt.

Zusätzlich kann über die Homepage der Deutsche Sparkassen Verlag GmbH (www.sparkassen-shop.de/home/shop/161/) ein von der Bundesnetzagentur anerkanntes Kartenlesegerät der Klasse 2 (ca. 50,- €) oder 3 (ca. 95,- €) mit dazugehöriger Software erworben werden. Das für die Rahmenvereinbarung zusammengestellte Paket enthält keinen Kartenleser, da es jedem Kunden selber überlassen bleiben soll, ob er das Gerät nur für die qualifizierte Signatur benötigt – dann ist ein Gerät der Klasse 2 ausreichend – oder ob er, falls er eine Geldkarte besitzt, ein Gerät der Klasse 3 benötigt. Wie bereits in Abschnitt 7 beschrieben, ist für die Unterzeichnung der Gutachten ein Kartenleser der Klasse 2 ausreichend. Wir empfehlen als Kartenleser der Klasse 2 das Gerät cyberJack pinpad der Firma ReinerSCT und als Kartenleser der Klasse 3 das Gerät cyberJack e-com der Firma ReinerSCT.

1) alle Preise zzgl. 19% Mehrwertsteuer.

Neben vergünstigten Konditionen, die in regelmäßigen Abständen mit den Preisen von Mitbewerbern verglichen werden, hat der **WF-Kunde** den **entscheidenden Vorteil, dass die Schnittstelle in WF-ProSa** (geplant für die Herbst-Version 2007) **auf die Software der Deutschen Sparkassen Verlag GmbH abgestimmt ist. Verwalten Sie alle eingehenden signierten und verschlüsselten Dokumente** mit dem **WF-Dokumentenmanager** sowie die **elektronische Gerichtsakte** zum einzelnen Auftrag **ohne eine zusätzliche Verwaltungssoftware. Sparen Sie als WF-Kunde kostbare Zeit** ein, indem Sie ihr **Gutachten unmittelbar aus dem WF-Dokumentenmanager heraus signieren** und als **Anhang an eine durch den WF-Schriftverkehr automatisch erstellte E-Mail** mit nur wenigen Mausklicks **versenden**. Die Empfangsbestätigung des Gerichts wird in naher Zukunft ebenfalls durch den **WF-Dokumentenmanager** selbstständig verwaltet. Profitieren Sie davon, dass die Adressen der Gerichtspostfächer sowie die **öffentlichen Schlüssel automatisch** und immer zugänglich für Sie **in der WF-Adressverwaltung hinterlegt** werden.

Aufgrund dieses abgestimmten Systems **sparen** Sie nicht nur **Zeit**, sondern haben auch **alles** rund um ihr (Gerichts-) Gutachten an **einer Stelle optimal verwaltet**.

12 Wie kommt das Zertifikat zum Sachverständigen?

Neben weiteren umfassenden Informationen zu dem Thema „Elektronischer Rechtsverkehr“ finden Sie auf unserer Homepage www.wertermittlungsforum.de unter der Rubrik Leistung, elektronischer Rechtsverkehr ein Kontaktformular für die elektronische Signatur.

Sie können das Formular direkt bei uns auf der Homepage ausfüllen und per Email an S-TRUST senden. Es handelt sich hierbei nicht um ein Bestellformular. Es dient lediglich der Mitteilung an S-TRUST, dass Sie an diesem Produkt interessiert sind und Informationsmaterial zu diesem Thema wie auch das Bestellformular zugesendet bekommen.

Sollten Sie sich für die Bestellung einer qualifizierten Signatur entscheiden, müssen Sie lediglich das Antragsformular, das Ihnen von S-TRUST zugeschickt wird, ausfüllen und es mit Ihrem Personalausweis oder Reisepass sowie dessen Kopie bei einer Postfiliale in Ihrer Nähe vorlegen. Dort werden Sie dann, wie bereits in Abschnitt 6 beschrieben, registriert.

Als nächster Schritt muss die Software auf ihrem Computer installiert und das Zertifikat aus dem Internet heruntergeladen werden. Um das Zertifikat auf die Chipkarte heruntergeladen zu können, erhalten Sie von der Deutschen Sparkassen Verlag GmbH eine E-Mail, die ein Passwort sowie weitere Arbeitsanweisungen enthält. Falls Sie neben dem Zertifikat auch ein neues Kartenlesegerät erworben haben, muss die Software des Kartenlesers ebenfalls installiert und das Gerät durch den USB-Anschluss an den Computer angeschlossen werden. Nun steht einer elektronischen Unterschrift nichts mehr entgegen. Der zuvor erläuterte Ablauf von der Registrierung bis zum Zertifikat-Download wird in Abbildung 7 verdeutlicht.

Hinweis:

Interessenten des S-TRUST Signaturpakets erhalten bei Bestellung eine Kurzanleitung. Diese beschreibt auf einfache Art und Weise die einzelnen Prozessschritte bis hin zum Download des qualifizierten Zertifikats auf die Karte.

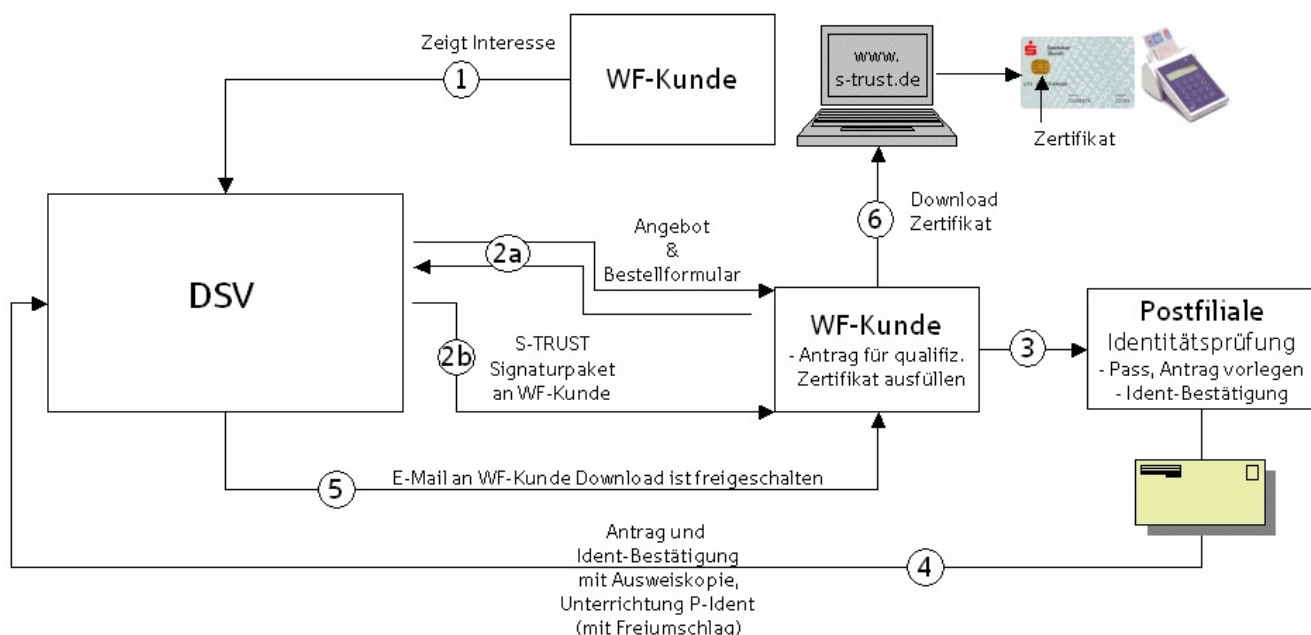


Abb. 7: **Beantragung und Zustellung des qualifizierten Zertifikats [6]**
(DSV = Deutsche Sparkassen Verlag GmbH)

13 Fazit

Bei dem elektronischen Rechtsverkehr wird es sich wie bei der Einführung des Faxgerätes verhalten; zu Beginn bestand Unsicherheit, ob man das Gerät überhaupt benötigt, da man nur jemandem etwas faxen konnte, der ebenfalls über ein Faxgerät verfügte. Heute gehört das Faxgerät zur Standardausstattung jedes Büros und man findet es selbst in vielen privaten Haushalten.

Einen ähnlichen Weg wird die qualifizierte Signatur beschreiten. Immer mehr Gerichtsbarkeiten werden in diesem Jahr dem elektronischen Rechtsverkehr die Türen öffnen¹⁾ und Ihnen dadurch die Möglichkeit geben ihre Unterlagen für ein Gerichtsgutachten in Verbindung mit WF-ProSa an einer Stelle, ohne großen Zeitaufwand digital zu verwalten. Circa 4 % der Teilnehmer unseres 15. Jahreskongresses in Dresden nutzten bereits spontan die Möglichkeit, sich registrieren zu lassen und signieren ihre Gutachten bereits erfolgreich.

Nutzen Sie die elektronische Signatur neben dem Einsatz im elektronischen Rechtsverkehr außerdem für die einfache und rechtssichere Abwicklung sämtlicher Online-Verträge und für Ihre Steuererklärung (ELSTER). Die Unternehmen benötigen keine zusätzliche Software mehr für die Steuererklärung, da die Formulare kostenfrei über das Elsteronline-Portal ausgefüllt werden können. Durch die elektronische Prüfung innerhalb der elektronischen Formulare werden Formfehler vermieden. Für alle Sachverständigen, die auch im Bereich der Bauausführung tätig sind, ist zudem die e-Vergabe eine sinnvolle Einführung. Mit Vergabepattformen aus öffentlicher oder privater Hand kommen Sie an Ausschreibungen, Angebote und Aufträge. Nehmen Sie an der elektronisch durchgeführten Vergabe teil und verzichten Sie auf stressige Anfahrten in letzter Minute vor Fristablauf.

Die Anwendung der qualifizierten Signatur in den zuvor genannten Punkten, verringert nicht nur Ihre Ausgaben (Porto-, Druckerkosten etc.), sondern lässt Sie auch wertvolle Zeit einsparen.

Das Interesse und die Nachfrage an dem elektronischen Rechtsverkehr und somit der qualifizierten Signatur steigt täglich und umso mehr freut es uns, dass wir für Sie ein günstiges Einsteigerpaket mit günstigen Folgekosten schnüren konnten, bevor die Trustcenter auf die wachsende Nachfrage mit einem Preisanstieg reagieren.

14 Literaturverzeichnis

- [1] Kierig J., Zum elektronischen Rechtsverkehr mit Gerichten, *WFA* 1|2005, S. 30 f
- [2] Elektronisches Gerichts- und Verwaltungspostfach (EGVP), 08.09.2006
www.egvp.bund.de/bearbeitung/index.htm
- [3] Projektgruppe Elektronischer Rechtsverkehr, Oberverwaltungsgericht Rheinland-Pfalz, elba (Stand Februar 2006)
- [4] Elektronische Signatur macht Digitalfotos fälschungssicher, *S-Trust Magazin* 1|2007
- [5] OPENLiMiT SignCubes AG: S-TRUST Sign-it Elektronisches Handbuch (Stand der Informationen August 2006)
- [6] Grafik entstand auf der Grundlage von: Bernhard Ratzmann, Deutscher Sparkassen Verlag GmbH, Qualifizierte Signaturen für das WertermittlungsForum

Die Verwendungsmöglichkeiten der qualifizierten Signatur beziehen sich vereinzelt auf die Aussage der Deutschen Sparkassen Verlag GmbH (www.s-trust.de, 26.02.2007)

*Dipl.-Ing. (Assessor) Jochem Kierig und
Dipl.-Ing. (FH) Kerstin Klein, WertermittlungsForum,
Barbarossastraße 2, 53489 Sinzig*

1) Gerichte, die bereits den elektronischen Rechtsverkehr (meist inkl. elektronischer Akteneinsicht) anbieten, finden Sie nach egvp oder elba getrennt, je nachdem welches System von den Gerichten verwendet wird unter:

www.egvp.de/gerichte.htm

www.justiz.rlp.de, Rubrik Gerichte und

www.oberverwaltungsgericht.niedersachsen.de, Rubrik „Das Gericht / Elektronischer Rechtsverkehr“.