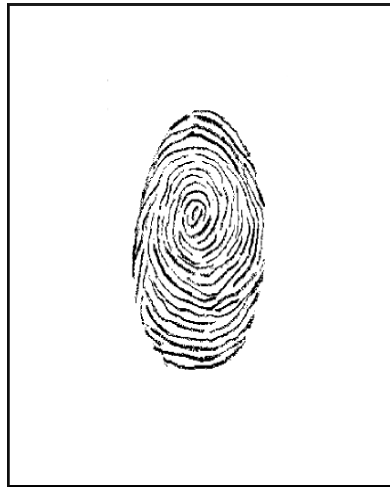


Praktische Anwendung Kryptographischer Prüfsummen



COMPUTERBILDNIS.COM

Angewandte Kryptographie: Prüfsummen

Praktische Anwendung Kryptographischer Prüfsummen

Peter Jockisch, Freiburg i. Br.
www.computerbildnis.com

24. Februar 2012

Computerdateien können auf viele Weisen unbemerkt manipuliert werden. Kryptographische Prüfsummen, Hashwerte, dienen dem Schutze Ihrer Daten: Durch Bildung eines elektronischen Fingerabdrucks einer Datei wird ein stets gleichbleibender Zahlenwert erstellt. Weicht dieser zu einem späteren Zeitpunkt ab, liegt Beschädigung oder Manipulation vor. Mit einem einzigen Mausklick läßt sich so jederzeit die Unversehrtheit einer Datei prüfen. Diese illustrierte Einführung behandelt Jacksum, ein freies und plattformunabhängiges Programm. Kryptographische Prüfsummen bilden die Grundlage für Signierung, Verschlüsselung, für Netzseiten- und E-Mail-Zertifikate, für die qualifizierte elektronische Signatur sowie für das technische Verständnis der revisionssicheren E-Mail-Archivierung, zu der alle Kaufleute gesetzlich verpflichtet sind.

Inhaltsverzeichnis

1 Funktionsweise	3
1.1 Elektronische Fingerabdrücke	3
1.2 Qualitätskriterien	4
1.3 Vorherrschende Standards im Westen und in Rußland	5
1.4 Existieren für die Öffentlichkeit gesperrte Technologien?	5
2 Anwendungsbeispiele: Geschäftswelt, Internet, Archivierung	7
2.1 Wahrung der Dateintegrität	7
2.2 Anhaltspunkt für den Bearbeitungsstand einer Datei	7
2.3 Wappnung gegen Wirtschaftskriminalität, Schutz vor Mobbing	7

2.4	Dateibezugnahme in Verträgen und Eingangsbestätigungen . . .	8
2.5	Fotografen, Fotomodelle, Künstler: Bildlizenzierungen	8
2.6	Telefonisch übermittelter Anhaltspunkt für die Echtheit versandter Dokumente	9
2.7	Hashwerte-Veröffentlichung als ersatzweiser Echtheitsnachweis . .	9
2.8	Dokumente mit Hashwerten veröffentlichen	10
2.9	Archivierung von Dateien	10
2.10	Weitere Anwendungsbereiche	11
2.11	Mißbrauchsmöglichkeiten	11
2.12	Softwareaktivierung und Rechneridentifikation über elektroni- sche Fingerabdrücke	12
3	Praxis	12
3.1	Jacksum besorgen und installieren	12
3.1.1	Installation von Java und Jacksum	13
3.1.2	Anwendung unter KDE Konqueror und KDE Dolphin . .	14
3.1.3	GNOME Nautilus	14
3.1.4	Anwendung unter Explorer: MS-Windows 7 und -XP . . .	14
3.2	Weitere Anwendungsmöglichkeiten	15
4	Konsolenbasierte Prüfsummenbildung	15
4.1	Bordeigene SHA-Algorithmen unter Unix/BSD- und GNU/Linux- Systemen	15
5	Informationsquellen zur angewandten Kryptographie und Computer- sicherheit	16
5.1	Die qualifizierte elektronische Signatur in der BRD	16
5.1.1	Leitfaden Elektronische Signatur	16
5.1.2	Signaturgesetzrelevante Begriffsbestimmungen in der BRD	16
5.1.3	Offizielle Netzseiten der BRD zur Elektronischen Signatur	16
5.2	Gesetzlich anerkannte, revisionssichere E-Mail-Archivierung . . .	17
5.3	Zwei zentrale Netzseiten zur angewandten Kryptographie	17
5.4	Englischsprachige Videoeinführungen bei Youtube	17
5.5	Historischer Rückblick bei Google Video	17
5.6	Erhöhte Sicherheit mit freien Betriebssystemen	18
5.6.1	Quellcode, Programmtext	18
5.6.2	Maschinencode, Binärcode	18
5.6.3	Freie Software	18
5.6.4	Quellcodekontrolle und Hintertürenfreiheit	18
5.6.5	Komplexität und Sicherheit versus Bedienungskomfort . .	19
5.6.6	Freie Betriebssystemalternativen, „Binary Blobs“	20
5.6.7	Dualboot-Option	20

5.6.8	Betriebssystemempfehlungen	21
5.6.9	Erstklassiges freies Betriebssystem: Ubuntu 10.04 LTS . . .	21
5.6.10	PC-BSD und gNewSense	21
5.7	Weitere Seiten zum Thema Computersicherheit	22

6	Impressum, Bezugsquellen, Urheberrecht, Lizenz	23
6.1	Impressum	23
6.2	Urheberrecht	23
6.3	Artikellizenz	23

1 Funktionsweise

1.1 Elektronische Fingerabdrücke

Menschen sind komplexe Lebewesen. Für ihre schnelle und unkomplizierte Identifizierung werden oftmals Fingerabdrücke erstellt. Nach demselben Prinzip können Computerdateien identifiziert werden: durch Erzeugung eines „elektronischen Fingerabdrucks“, der so genannten kryptographischen Prüfsumme, einer stets gleichbleibenden Zahl. Mittels standardisierter Verfahren kann so eine schnelle Integritäts- und Echtheitskontrolle von Dateien jedweder Art vorgenommen werden.

Menschliche Fingerabdrücke werden mit Stempelkissen erstellt, elektronische mit einem Prüfsummenprogramm.

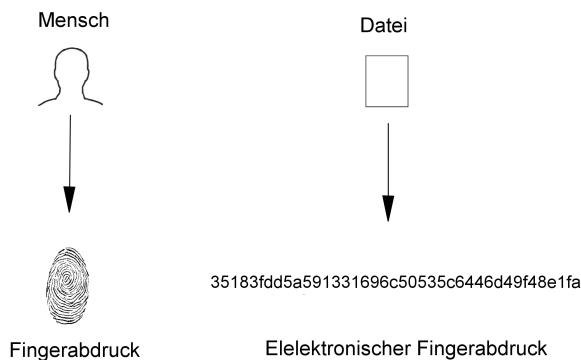


Abb. 1: Echtheitsnachweis bei Mensch und Computerdatei

1.2 Qualitätskriterien

Wir betrachten *kryptographische* Prüfsummen. Sie basieren auf Streuwert- bzw. Hashfunktionen, die zu einer beliebigen Datei Streu- bzw. Hashwerte als Ergebnis liefern. Dieser Wert wird auch Hashcode bzw. Hash genannt.

Eine Datei, sowie identische Kopien von ihr, weist stets dieselbe Hashwert-Prüfsumme auf. Ändert sich jedoch auch nur ein einziges Bit oder Zeichen durch Beschädigung oder Manipulation, sollte ein gänzlich anderer Hashcode entstehen.

Ein Hashfunktions-Prüfsummenverfahren sollte also zu unterschiedlichen Computerdateien immer unterschiedliche Werte liefern. Die berechnete Prüfsumme ist, abhängig vom verwendeten Verfahren, immer gleichlang. Deshalb kann natürlich nur eine begrenzte Anzahl von Zahlen dargestellt werden.¹

Unter Sicherheitsaspekten stellen sich nun verschiedene Angriffsszenarien dar, z. B.: Von einer gegebenen Originaldatei, beispielsweise einer geschäftlichen Bestellung, möchte ein Angreifer eine gefälschte Version mit einer manipulierten, erhöhten Bestellmenge erstellen, welche dieselbe Hashwert-Prüfsumme aufweist. Nachdem er die Änderungen vorgenommen hat, versucht er anschließend durch Ausprobieren, vielleicht mittels Einfügung unsichtbarer Steuerzeichen, eine Dateiversion mit identischer Prüfsumme zu erhalten.² Gelingt es nun dem Angreifer, in zeitlich vertretbarem Aufwand solch eine zweite Datei zu erzeugen, welche die erwünschten Manipulationen enthält und die Prüfsumme der Originaldatei aufweist, so ist das betreffende Hashfunktions-Verfahren „gebrochen“. Nach Bekanntwerden solch einer Schwäche sollte es keine Verwendung mehr finden. Durch stetige Forschungsarbeit werden Schwächen schon längere Zeit im voraus erkannt.

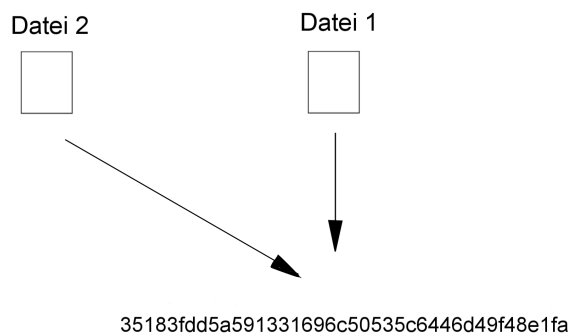


Abb. 2: Prüfsummenkollision

¹Es gibt praktisch unendlich viele Computerdateien, so daß mit einer Zahl fester Länge unmöglich jeder dieser Dateien ein unterschiedlicher Wert zugewiesen werden kann.

²Bei einem solchen Angriff kommen natürlich unterstützende Computerprogramme zum Einsatz.

Gäbe es einen unendlich berechnungsstarken Computer, so könnte, theoretisch, möglicherweise jedes Verfahren durch schlichtes Ausprobieren sämtlicher Möglichkeiten gebrochen werden (Brute Force Attack). Für die Praxis wird solch eine Vorgehensweise in der Mehrzahl aller Fälle als nicht praktikabel erachtet, da die erforderlichen Berechnungen fast nie in vertretbarer Zeit durchführbar sind. Die meisten Hashfunktionen wiesen bisher nur eine begrenzte Lebensdauer auf und wurden irgendwann aus Sicherheitsgründen von Nachfolgeverfahren abgelöst. Berechnungsstärkere Computergenerationen tragen zur Verkürzung der Lebensdauer bei. Neben den rechenkraftbasierten Angriffen existieren jedoch auch anders orientierte, und es kann niemals ausgeschlossen werden, daß mithilfe mathematischer Kreativität bereits heute praktikable Angriffe möglich sind; nicht alle wissenschaftlichen Erkenntnisse werden veröffentlicht, im Hintergrund arbeitet und forscht ein riesiges Heer von Mathematikern, insbesondere für Nachrichtendienste.

1.3 Vorherrschende Standards im Westen und in Rußland

Die westliche IT-Infrastruktur basiert gegenwärtig noch überwiegend auf dem SHA-1-Algorithmus (Secure Hash Algorithm 1).³ Dieser ist bereits angebrochen, die erforderliche Rechenzeit, um ihn zu korrumpieren, ist nachweislich gesunken, wobei sie gegenwärtig immer noch als unpraktikabel hoch eingeschätzt wird.⁴ Bereits heute existieren vorläufige Alternativen (z. B. SHA-512), die vielleicht noch etwas länger Bestand haben werden.

In Rußland und vielen weiteren GUS-Staaten⁵ ist GOST R 34.11-94⁶ beziehungsweise GOST 34.311-95⁷ der Hash-Standard in Behörden. Wie bereits bei SHA-1, wurden auch bei ihm strukturelle Schwächen gefunden.⁸

1.4 Existieren für die Öffentlichkeit gesperrte Technologien?

Schon seit langer Zeit existieren Überlegungen, daß bestimmte zu offiziellen Standards erhobene Kryptographie-Algorithmen inhärente mathematische Schwächen aufweisen könnten, die nur den Experten der Nachrichtendienste bekannt sind. Eine möglicherweise vorhandene Einflußnahme der Geheimdienste auf die Gestaltung von Sicherheitsprodukten (Software- und Hardware-Hintertürenproblematik, offene Fragen zu Standards usw.) ist Thema zahl-

³Spezifikation: <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf> und <http://tools.ietf.org/html/rfc3174>.

⁴„Hash mich – Konsequenzen der erfolgreichen Angriffe auf SHA-1“, Reinhard Wobst, Jürgen Schmidt, Heise Security, Stand: 18.02.2005, URL: www.heise.de/security/artikel/Konsequenzen-der-erfolgreichen-Angriffe-auf-SHA-1-270648.html. „Angriffe auf SHA-1 weiter vereinfacht“, 11.06.2009, www.heise.de/security/meldung/Angriffe-auf-SHA-1-weiter-vereinfacht-180587.html.

⁵<http://www.cis.minsk.by>

⁶<http://tools.ietf.org/html/draft-dolmatov-cryptocom-gost341194-07>

⁷www.gost.ru/wps/portal/pages.en.Main

⁸Heise-Verlag News-Meldung vom 20. August 2008: www.heise.de/security/meldung/oesterreichische-Kryptologen-attackieren-Hasvh-Funktionen-197880.html

reicher Artikel zur Computersicherheit.⁹ Mehrere renommierte Firmen haben bereits direkt oder indirekt bestätigt, bei ihrer Produktentwicklung mit Nachrichtendiensten zusammenzuarbeiten. Offiziell begründet wurde dies u.a. mit der Absicht, die technische Sicherheit von Firmenprodukten optimieren zu wollen. Manche Sicherheitsexperten gehen auch davon aus, daß die Nutzung der fortgeschrittensten Computertechnologien der Öffentlichkeit vor-enthalten wird, daß aktuell zukunftsweisende Technologien für die Öffentlichkeit gesperrt bleiben, um Nachrichtendiensten einen Berechnungskraftvorsprung zu garantieren.

Unter diesen Aspekten ist die Effektivität der real existierenden Verschlüsselungspraxis fragwürdig; auch dann, wenn durchgängig offene, freie IT-Infrastruktur zum Einsatz kommt. Korruptierte Zertifikatsinfrastrukturen sowie die zunehmende Miniaturisierung, versteckte Kamera- und Mikrofontechnologie eingeschlossen, ermöglichen weitere Angriffsszenarien.

Die Konsequente Nutzung öffentlich erhältlicher Prüfsummen-, Signierungs- und Ver-

⁹Siehe hierzu auch „Did NSA Put a Secret Backdoor in New Encryption Standard?“, Bruce Schneier, 15. November 2007 auf Wired.com: www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115, und „Der Verschlüsselungsstandard AES: Das Danaer-Geschenk der US-Regierung für die Welt?“, Infokrieg.tv, 18. August 2011: <http://infokrieg.tv/wordpress/2011/08/18/der-verschlüsselungsstandard-aes-das-danaer-geschenk-der-us-regierung-fur-die-welt>. Mittlerweile gilt es als offenes Geheimnis, daß von jedem Internetnutzer der Welt ein lebenslang gespeichertes Profil erstellt wird, einschließlich sozialer Graphen, die sämtliche Kontakte mit anderen Internetnutzern dokumentieren. Siehe hierzu beispielsweise den Abschnitt von Minute 00:56 bis 02:00 der „Kopp Nachrichten vom 21.06.2010 mit Eva Herrmann“, „US-Geheimdienste planen Internet-Kontrolle“.

Informationsabgriffe erfolgen automatisch an vielen Netzwerkschnittstellen, u.a. auf Stichworte hin ausgelöst. Anschauliche Grundlageneinführung: „Die Problematik von Data Mining und Profiling“, erschienen auf Sicherheitskultur.at: http://sicherheitskultur.at/data_mining.htm.

Heutige Algorithmen werten umfassend aus: Wer kommuniziert mit wem, welche sozialen Netzwerke existieren? Welche Interessensgebiete und tendentiellen Einstellungen sind vorhanden? „[...] ... denn wir wissen, wo Sie sind, mit Ihrer Erlaubnis. Wir wissen, wo Sie gewesen sind, mit Ihrer Erlaubnis. Wir können mehr oder weniger erahnen, worüber Sie nachdenken. [...]“, „[...] because we know where you are, with your permission. We know where you have been, with your permission. We can more or less guess what you are thinking about. [...]“, „Eric Schmidt at Washington Ideas Forum 2010“, Zitat bei 16:19, Einstiegspunkt in der 14. Minute, veröffentlicht im Youtube-Kanal von Google: <http://www.youtube.com/watch?v=CeQsPSaitL0#t=14m25s>. Siehe zu diesem Themenbereich auch einen deutschsprachigen Nachrichtenartikel vom 09.06.2006 zur „Real-Time Ambient-Audio Identification“-Technologie, <http://www.golem.de/0606/45819.html>.

Firmen und Konzerne, z. B. Suchmaschinenanbieter sowie Anbieter von sozialen Netzwerken und E-Mail-Diensten sind dazu in der Lage, auf Anfragen Dritter von jedem Nutzer ein persönliches Dossier zu erstellen, mit Interessensgebieten, vermuteten persönlichen Stärken und Schwächen, sozialen Graphen und weiteren Informationen. www.google-watch.org und www.wikipedia-watch.org zählen zu den größten Kritikern vorherrschender Suchmaschinenmonopolisierungstendenzen.

Seien Sie sich dieser Aspekte immer gewahr, wenn Sie kommunizieren. Gehen Sie davon aus, daß ein ans Weltnetz angeschlossener Rechner für manche Hersteller und Organisationen tatsächlich immer eine offen einsehbare Datenplattform ist. Inhalte jeder Art können vollautomatisch identifiziert, abgeglichen und „gemeldet“ werden, durch den routinemäßigen Versand der elektronischen Fingerabdrücke konsumierter Dateien, z. B. von Videofilmen, Tondateien, PDF-Dokumenten und anderen Dateitypen. Es gibt keine Privatsphäre mit elektronischen Geräten, höchstwahrscheinlich alle Inhalte sind auslesbar, jeder Lebensbereich ist betroffen: <http://sklaven-ohne-ketten.blogspot.com/2009/03/1-9-belaushtes-privatleben-die.html>.

schlüsselungstechnologie kann jedoch zumindest einen Teil der möglichen Angreifer abwehren.

2 Anwendungsbeispiele: Geschäftswelt, Internet, Archivierung

Auf die umfassenden Voraussetzungen für den gesetzlich anerkannten personengebundenen Echtheitsnachweis, der so genannten qualifizierten elektronischen Signatur, wird hier nicht näher eingegangen. Abschnitt fünf enthält weiterführende Informationsquellen. Die Anwendung kryptographischer Prüfsummen auf Computerdateien kann jedoch bereits *Anhaltspunkte* zur Echtheit und Unversehrtheit von Dateien geben, wie folgende Beispiele demonstrieren.

2.1 Wahrung der Dateintegrität

Sie erstellen eine Geschäftsbilanz und gehen anschließend in den Urlaub. Zur Qualitätskontrolle notieren Sie sich vor der Abreise die Hashwert-Prüfsumme der fertiggestellten Bilanzdatei. Nach dem Urlaub bilden Sie erneut die kryptographische Prüfsumme und verifizieren so, ob die Datei unversehrt ist oder ob sie beschädigt oder manipuliert wurde.

Unautorisierte Zugriffe können auf diese Weise entdeckt werden. Benachrichtigen Sie in solchen Fällen die Systemadministratoren und bestehen Sie auf einer Wiederherstellung der ursprünglichen Dateiversion.

Eine Versionsverwaltung¹⁰ alleine reicht nicht aus. Die Konsistenzprüfung über Prüfsummen funktioniert schneller, effektiver und sicherer. Ein separates Prüfsummenprogramm sollte daher immer verfügbar sein.

2.2 Anhaltspunkt für den Bearbeitungsstand einer Datei

Beim Verlassen einer Firma möchten Sie sich den letzten Bearbeitungsstand einer Computerdatei schriftlich bestätigen lassen. Hierfür empfehlen sich zwei verschiedene kryptographische Prüfsummenverfahren.¹¹ Auf diese Weise bleibt das Firmengeheimnis gewahrt, und Sie können sich trotzdem bis zu einem gewissen Grad absichern. Sollte es jemals Rückfragen geben, haben Sie einen schriftlichen Anhaltspunkt über Ihren letzten Bearbeitungsstand.

2.3 Wappnung gegen Wirtschaftskriminalität, Schutz vor Mobbing

Im Rahmen der allgemeinen Qualitätskontrolle und immer dann, wenn Korruption, Lügen, Intrigen, Mobbing, Sabotage und Wirtschaftskriminalität wahrscheinlich werden, empfiehlt sich zum eigenen Schutz der Gebrauch kryptographischer Prüfsummen, auch bei Präsentationen jedweder Art. Signierungssoftware scheidet oftmals aus, da sie naturgemäß mit

¹⁰<http://de.wikipedia.org/wiki/Versionsverwaltung>

¹¹Das ist langfristig sicherer, eines der beiden Verfahren hält vermutlich länger durch in der Zukunft.

Verschlüsselungsfunktionen gekoppelt ist und deshalb nicht auf jedem Arbeitsplatzrechner geduldet wird. Firmengeheimnisse könnten verschlüsselt nach außen gelangen bzw. Schadsoftware unentdeckt nach innen. Ein freies Prüfsummenprogramm – nicht zu verwechseln mit Freeware – kann jedoch verantwortlich auf Rechnern installiert werden.¹²

2.4 Dateibezugnahme in Verträgen und Eingangsbestätigungen

Bei schriftlichen Verträgen und Eingangsbestätigungen erleichtern elektronische Fingerabdrücke die Bezugnahme auf Computerdateien. Dateien jedweder Art können eindeutig über ihren Hashwert identifiziert werden (z. B. Textdokumente, Videofilme, *Gesprächsmitschnitte und Interviews*, allgemein Tondateien, Programme, CAD-Dateien). Auch erbrachte Dienstleistungen, die abschließend in Form eines Datenträgers, z. B. einer abzuliefernden CD-ROM oder DVD vorliegen, lassen sich auf diese Weise schriftlich bestätigen. Empfangsbestätigungen bilden ein breites Einsatzgebiet.

2.5 Fotografen, Fotomodelle, Künstler: Bildlizenzierungen

In bildgestaltenden Berufsfeldern durchlaufen Fotos bis zur Veröffentlichung viele Nachbearbeitungsphasen, eine Festlegung auf spezifische endgültige Dateien ist im Vorfeld meistens unpraktisch. Referenzdateien können jedoch grundsätzliche künstlerische/bildgestalterische Vorgaben für die Veröffentlichung bzw. langfristige Verwertung verbindlich regeln: Wahl des Bildausschnittes, grundsätzliche Kontrasteigenschaften, implizites Verbot von (weitergehenden) „Schönheitsretuschierungen“ etc. Bildbeschreibungen und Miniaturabbildungen der Originale werden dann samt zugehöriger Dateiprüfsummen im Verwertungsvertrag aufgenommen. Verwenden Sie hierbei möglichst nur solche Dateiformate, die entweder ganz ohne Komprimierung bzw. mit verlustfreier Komprimierung arbeiten, Formate, die auch Farbprofilinformationen speichern können. Bezugnahme auf Referenzfarbräume setzt natürlich ein ordentliches Farbmanagement, eine umfassende Vorbereitung des Geräteparks voraus.

Manchmal sind verbindlich fertiggestaltete Bilddateien möglich. Genügend Auflösungsreserven für die Skalierung (Größenanpassung) vorausgesetzt, können Fotos für eine Internetseite in allen Parametern exakt festgelegt werden. Bei Wahl eines passenden Standards (z. B. JPEG, PNG, GIF) ist eine hohe Wahrscheinlichkeit gegeben, daß die Bilder auch noch langfristig von zukünftigen Netzseiten-Leseprogrammen (Browsern) angezeigt werden können.

¹²Der Begriff „Freeware“ ist nicht eindeutig definiert. Er kann sich auf „Freie Software“ (Programmtext/Quellcode ist verfügbar) beziehen oder auch nicht. Tendentiell vorherrschend bezeichnet er *kostenlos verteilte Software*, deren Programmtext/Quellcode jedoch unveröffentlicht bleibt.

2.6 Telefonisch übermittelter Anhaltspunkt für die Echtheit versandter Dokumente

Dem Empfänger einer Datei oder eines per Briefpost versandten Datenträgers kann zur Kontrolle telefonisch die Hashfunktions-Prüfsumme mitgeteilt werden. Das Fälschen einer Stimme ist zwar möglich, aber aufwendig. Die personengebundene Signierung wäre jedoch komfortabler und sicherer.

2.7 Hashwerte-Veröffentlichung als ersatzweiser Echtheitsnachweis

Manche Staaten erlauben nur eingeschränkt Verschlüsselung und Signierung (personen-gebundener elektronischer Echtheitsnachweis). Bis zu einem gewissen Grad können kryptographische Prüfsummen als ersatzweiser Notbehelf dienen:

1. Erstellen Sie zunächst *separat* die Nachricht bzw. das Dokument als Computerdatei (Text- oder PDF-Datei, Bild, Video, u. a.). Fügen Sie die Datei einer E-Mail an und versenden Sie die Nachricht.
2. Veröffentlichen Sie auf einer Netzseite tagebuchähnlich die Hashcodes der versandten Dokumente. Zahlreiche seriöse kostenlose (werbefinanzierte) Webhoster bieten sich dafür an. Auch ohne (X)HTML-Kenntnisse lassen sich Internetseiten erstellen, z. B. mit dem freien grafischen Editor Kompozer (www.kompozer-web.de). Alternativ bieten sich kostenlose Blogsysteme an, die keine technischen Gestaltungskenntnisse voraussetzen.¹³
3. Der Empfänger der Datei kann nun einen Hashwerte-Abgleich vornehmen, indem er Ihre Netzseite bzw. Ihren Blog aufruft und den zugehörigen Hashcode zur symbolisch angedeuteten Nachricht liest.

Anonymität im Internet gibt es jedoch nicht, auch nicht mit Diensten wie Tor. Zu viele Software-, Hardware- und Kryptographieschnittstellen sind korrumpiert, mit Programm- bzw. Hardwarehintertüren. Eine gewisse Anonymität kann zwar durch die Nutzung von Internetcafé-Computern erreicht werden. An zahlreichen öffentlichen Plätzen befinden sich

¹³Achten Sie auf eine SSL-/TLS-gesicherte Paßwortübergabe beim Anmeldevorgang; das Benutzerpaßwort sollte verschlüsselt über das Internet transportiert werden. Ein mögliches kostenloses Blogsystem wäre z. B. Blogger.com (www.blogger.com), ein weiteres WordPress.com (<http://de.wordpress.com/features>) Beide sind einfach und unkompliziert handbar und sofort benutzbar. Kommentarfunktionen lassen sich deaktiviert halten. Machen Sie schematische Einträge, beispielsweise in der Form *Prüfsummenverfahren – Dateiprüfsumme*. Mehr Information bedarf es nicht. Bei umfangreichen täglichen Einträgen könnten Sie optional noch eine Dateinamensabkürzung hinzufügen. Aus dem E-Mailanhang „anfrage.pdf“ würde dann „a...e.pdf“ oder einfach nur „a...e“ werden.

Halten Sie Cookies in Ihrem Browser deaktiviert bzw. erlauben Sie diese nur ausgewählten Seiten oder nur temporär während der Sitzung. Firefoxerweiterungen wie „Better Privacy“ (<https://addons.mozilla.org/de/firefox/addon/6623>) sorgen für eine automatische Löschung von Flashcookies, vor während oder nach Sitzungsende. Weitere Hinweise zu datenschutzrelevanten Firefox-Addons und zu freier Software enthält die [Empfehlungen-Rubrik](#) auf www.computerbildnis.com.

jedoch Überwachungskameras, die mittels Gesichtserkennungsprogrammen und zeitlicher Auswertung entsprechende Zuordnungen vornehmen könnten. Darüberhinaus läßt sich der individuelle Tipprhythmus während jeder Eingabe auswerten. Ganz zu schweigen von der Tatsache, daß sich gegenwärtig eine Bevölkerungsmehrheit freiwillig mit Peilsender und Abhörwanze (Mobiltelefon) versieht, die auch nach der Entnahme der Akkus/Batterien mit internen Akkus weiterfunktionieren können.

2.8 Dokumente mit Hashwerten veröffentlichen

Für die Veröffentlichung von Dokumenten im Internet oder im Intranet (lokales Firmennetz) empfiehlt sich die Angabe von Hashwerten, eventuell auf einer Unterseite („Download“-Bereich). Die Nutzung eines gesetzlich anerkannten SSL-/TLS-Zertifikates¹⁴ zur verschlüsselten Übertragung der Prüfsummen verstärkt die Sicherheit. Durch Abgleichen der Hashwerte können sich Nutzer relativ sicher sein, daß die heruntergeladenen Dokumente frei von Schadcode (Viren usw.), Manipulationen und Transferschäden sind.

Von äußeren Instanzen ausgestellte Zertifikate sind jedoch möglicherweise mit Restrisiken verbunden.¹⁵

2.9 Archivierung von Dateien

Bei der Datei-Archivierung auf CD-ROMs und DVDs empfiehlt sich die Notierung des Datenträger-Hashcodes. Zur Überprüfung gleichen Sie in regelmäßigen Abständen den Ist-

¹⁴Zertifikate sind Ausweise für das Internet (Netzwerke allgemein), meistens E-Mail- oder Netzseitenzertifikate. Mit ihnen läßt sich die Datenübertragung auch verschlüsseln („https://[...]“).

In der Vergangenheit versahen Personen bzw. Ämter ihre Dokumente mit einem zusätzlichen Echtheitsnachweis, indem sie mit Siegelack und Siegelstempel komplexe Muster auf die Dokumente auftrugen. Heute übernehmen kryptographische Schlüssel bzw. Zertifikate die Funktion des Siegelstempels: Für ein Dokument, z. B. eine E-Mail-Datei, wird mit Hilfe eines Zertifikates (eines Ausweises) ein begleitender, personengebundener Echtheitsnachweis berechnet, die so genannte kryptographische Signatur. Nach Eingang der Nachricht stellt das E-Mail-Programm des Empfängers (u. a. mit Hilfe dieser Signatur) vollautomatisch fest, ob das Dokument wirklich vom angegebenen Versender (Zertifikatsinhaber/Ausweisinhaber) erstellt wurde.

E-Mail- und Netzseitenzertifikate haben also eine Ausweisfunktion, mit der Korrespondenzpartner und Internetseiten ihre Identität nachweisen können. Klassische Ausweise werden von staatlichen Behörden ausgestellt. E-Mail- und Netzseitenzertifikate werden von so genannten Zertifizierungsstellen ausgestellt (Certification Authorities, CAs). Und hier liegen die zwei entscheidenden Unterschiede: Klassische Ausweise sind untereinander alle gleichwertig und amtlich anerkannt, es gibt nur einen einzigen Aussteller, der zugleich als Beglaubigungsinstitution fungiert: den Staat. E-Mail- und Netzseitenzertifikate hingegen existieren in unterschiedlichen Güteklassen, mit unterschiedlicher Aussagekraft. Nur Zertifikate höchster Güteklasse (Class-3), ausgestellt von staatlich anerkannten Zertifizierungsstellen, werden rechtlich anerkannt.

Weiterführende Informationen im Abschnitt „Kryptographische Signatur und Verschlüsselung, E-Mail-Zertifikate“ auf ComputerBildnis.com: http://computerbildnis.com/recommendations_de/recommendations_de.html#E-Mail-Kryptographie-und-Zertifikate.

¹⁵Heise Security News-Meldung vom 25.03.2010: „EFF zweifelt an Abhörsicherheit von SSL“, www.heise.de/security/meldung/EFF-zweifelt-an-Abhoersicherheit-von-SSL-963857.html

wert mit dem ursprünglich notierten Hashwert ab. Auf diese Weise können frühzeitige Schäden erkannt werden. Das regelmäßige Umkopieren auf neue archivierungsspezialisierte Datenträger – in relativ kurzen Zeitabständen – ist leider unumgänglich.

2.10 Weitere Anwendungsbereiche

In der Informatik und in der Elektrotechnik existieren zahlreiche weitere Anwendungsmöglichkeiten, beispielsweise eine Variante der sicherheitserhöhten Speicherung von Benutzerkontodaten: Ein Klartextpaßwort läßt sich auch ausschließlich in Form seines zugehörigen Hashwertes speichern. Gibt der Nutzer sein Klartextpaßwort erneut ein, wird der Hashwert erneut gebildet und mit dem gespeicherten abgeglichen. Im Falle eines Dateneinbruchs oder Datendiebstahls gehen so vorerst keine Klartextpaßwörter verloren.¹⁶¹⁷

2.11 Mißbrauchsmöglichkeiten

Kryptographische Prüfsummen lassen sich auch für fragwürdige Zwecke einsetzen. Der Medienabspieler eines Softwareherstellers soll in der Vergangenheit ungefragt Hashcodes der abgespielten Dateien versandt haben. Theoretisch ließe sich über vollautomatischen Abgleich mit Datenbanktabellen feststellen, ob genutzte Inhalte lizenziert wurden und welche politischen Filme und Tondateien sich ein Nutzer bevorzugt anschaut.¹⁸ Die Datenmenge ist winzig und, wenn sie zusätzlich verschlüsselt wird, praktisch unentzifferbar. Das Ändern des Dateinamens ändert nicht die Prüfsumme. Auch andere Merkmale, wie z. B. Hardware- und Softwarekonfigurationen (einschließlich nichtlizenziertes Programme), lassen sich analysieren und vollautomatisch „melden“.

In der Computerforensik sowie in zahlreichen weiteren informationstechnischen Bereichen ist die Bildung bzw. Abfrage kryptographischer Prüfsummen allgegenwärtig. Eine durchaus konstruktive Anwendung, insbesondere auch unter dem Aspekt der Beweissicherung bei Computerdelikten, wie z. B. nach Netzwerkeinbrüchen.

In Diktaturen besteht die Gefahr, daß vor Ort oder aus der Ferne „Festplattendurchsuchungen“ vorgenommen werden. Durch Hintertüren von Software- und Hardwareherstellern können routinemäßig kryptographische Prüfsummen aller vorhandenen Festplattendateien erstellt werden und anschließend vollautomatisch mit den Prüfsummen indizierter Inhalte, wie z. B. politischer Aufklärungsfilme, abgeglichen werden. Auf diese Weise kann schnell und effektiv überprüft werden, ob Bürger dazu tendieren, eine eigene Meinung zu

¹⁶Gute zeitgemäße Streuwertfunktionen wirken wie Einwegfunktionen. Sie weisen einer Datei einen individuellen Hashwert zu. Der umgekehrte Weg, die Berechnung der Originaldatei aus dem Hashwert, ist jedoch nicht in praktikabler Zeit möglich – gemäß gegenwärtigem öffentlich-bekanntem Wissensstand.

¹⁷Ein Grundlagenartikel zu Paßwörtern: Daniel Bachfeld, „Cracker Bremse [...]“, 03.06.2011, URL: <http://www.heise.de/security/artikel/Passwoerter-unknackbar-speichern-1253931.html?view=print>.

¹⁸Rein technisch könnten auch proprietäre PDF-Programme über solch eine Funktion verfügen. Alternativ sind freie PDF-Betrachter erhältlich, aufgeführt bei www.pdfreaders.org. Eine umfassende, größtmögliche Sicherheit setzt jedoch immer auch eine freie Betriebssystembasis voraus.

pflegen, und ob sie politische Inhalte konsumieren, die im Widerspruch zu offiziell verkündeten Dogmen stehen. Freidenker lassen sich so leicht ausfindig machen.

2.12 Softwareaktivierung und Rechneridentifikation über elektronische Fingerabdrücke

Die Free Software Foundation (FSF)¹⁹ führt in einem Artikel zur Privatsphäre²⁰ Computermerkmale auf, über die sich ein Rechner eindeutig identifizieren und wiedererkennen läßt. Vermutlich werden solche Kenndaten in einem Hash zusammengefaßt und in einer Datenbank archiviert. Bei manchen proprietären Produkten ist die Softwareaktivierung an die ermittelte Hardwarekonfiguration gekoppelt. Der Versuch, die gekaufte Software gleichzeitig auf einem zweiten Rechner zu installieren scheidert dann oftmals.

3 Praxis

Aus der großen Menge freier Prüfsummenprogramme hebt sich *Jacksum* hervor. Veröffentlicht unter einer OSI-zertifizierten²¹ Freie-Software-Lizenz, der GPL, gelistet im FSF-Verzeichnis²² und basierend auf Java,²³ läuft es auf vielen Betriebssystemplattformen. Es eignet sich damit auch für heterogene IT-Infrastrukturen von Firmennetzwerken. Zahlreiche international gängige Prüfsummenverfahren werden berücksichtigt, die Dateimanagerintegration gewährleistet eine komfortable Bedienung. Dateimanagerversionen sind erhältlich für GNOME, KDE, ROX und XFCE (Unix/BSD, GNU/Linux) sowie für den Explorer von MS-Windows,²⁴ und den „Finder“ von Apple Macintosh. Vom Programmator, Johann Löffmann, wird eine Netzseite mit ausführlichen Informationen zu Jacksum gepflegt. Vorschläge zur Programmerweiterung („feature request“) können eingereicht werden, der Austausch unter den Nutzern wird ebenfalls gefördert.²⁵

3.1 Jacksum besorgen und installieren

Jacksum kann über den Dateimanager oder als Kommandozeilenprogramm aufgerufen werden. Die Dateimanagerversion setzt keine installierte Kommandozeilenversion voraus, sie arbeitet unabhängig.

¹⁹www.fsf.org

²⁰<http://de.windows7sins.org/privacy>

²¹www.opensource.org/licenses/alphabetical

²²<http://directory.fsf.org/project/jacksum>

²³Wikipedia-Artikel: [http://de.wikipedia.org/wiki/Java_\(Programmiersprache\)](http://de.wikipedia.org/wiki/Java_(Programmiersprache)), <http://de.wikipedia.org/wiki/OpenJDK>

²⁴„[...] funktioniert unter Windows NT/2000/2003/XP/2008/Vista/7 [...]“, Quelle (Stand: 21. Juli 2010): www.jonelo.de/java/jacksum/index_de.html#Download

²⁵www.jonelo.de/java/jacksum/index.html

Im folgenden wird die Anwendung unter GNOME, KDE und MS-Windows Explorer beschrieben. Auf die Benutzung unter ROX, XFCE und „Finder“ wird im offiziellen Fragen- und Antwortenbereich eingegangen.²⁶

3.1.1 Installation von Java und Jacksum

In Unix- und unixartigen Betriebssystem-Distributionen ist Java meistens schon enthalten.

Als MS-Windows-Benutzer rufen Sie eine Suchmaschinenseite auf, zum Beispiel Google, und tippen „JRE“ ein, das ist die Kurzbezeichnung für „Java Runtime Environment“. Dieser Schritt entfällt, wenn bereits eine Javaumgebung vorhanden ist. Sie kommen auf folgende Seite, bei der man kostenlos die Java-Umgebung herunterladen kann (Java für Sun Solaris und GNU/Linux eingeschlossen): <http://java.com/de/download/manual.jsp>. Installieren Sie nun Java.

Installation und Anwendung von Jacksum werden ausführlich unter http://www.jonelo.de/java/jacksum/index_de.html#Download sowie in den readme.txt-Dateien beschrieben. Das jeweilige Dateimanagermenü kann variieren, je nach ausgewählten Installationsoptionen. Debian- bzw. Ubuntu-Nutzer können die Kommandozeilenversion über die Paketverwaltung herunterladen (*System* → *Systemverwaltung* → *Synaptic-Paketverwaltung*).²⁷

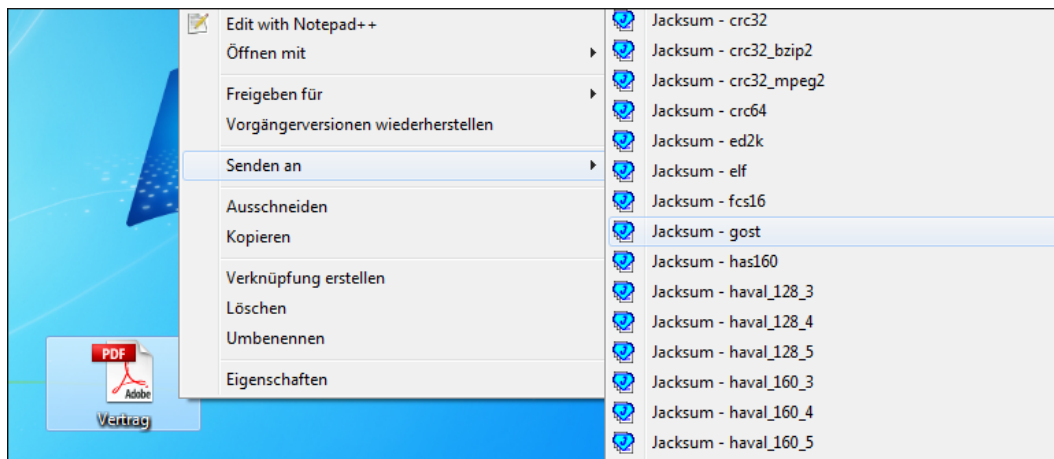


Abb. 3: Jacksum unter MS-Windows 7

²⁶http://www.jonelo.de/java/jacksum/index_de.html#FAQ

²⁷<http://packages.ubuntu.com/lucid/utils/jacksum>

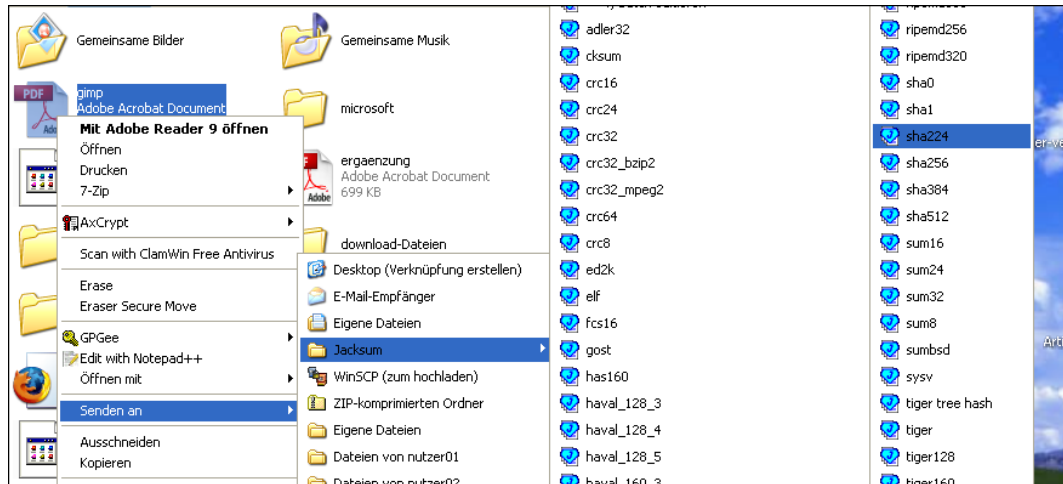


Abb. 4: Jacksum unter MS-Windows XP

3.1.2 Anwendung unter KDE Konqueror und KDE Dolphin

Öffnen Sie den Dateimanager. Klicken Sie zum Wählen der Datei auf die *rechte Maustaste* → „Aktion“ → „Jacksum“ → [gewünschte Funktion wählen].

3.1.3 GNOME Nautilus

Öffnen Sie den Dateimanager. Klicken Sie zum Wählen der Datei auf die *rechte Maustaste* → „Skripte“ → „Jacksum“ → [gewünschte Funktion wählen].

3.1.4 Anwendung unter Explorer: MS-Windows 7 und -XP

Besorgen Sie Jacksum auf www.jonelo.de/java/jacksum/index_de.html. Im Download-Bereich laden Sie die Windows-Explorer-Integration herunter (bei Bedarf zusätzlich die Kommandozeilenversion). Entpacken und installieren Sie das Programm.

Der zugehörige Hashwert einer Datei wird unter MS-Windows 7 und -XP gebildet, indem man mit der rechten Maustaste auf die ausgewählte Datei klickt, „Senden an“ wählt, dann auf „Jacksum“ geht und zum Schluß den gewünschten Prüfsummenalgorithmus auswählt. Prüfsumme sowie Dateiname samt Verzeichnispfad erscheinen in einem separaten Fenster und können kopiert werden. Mit „--3) Alle Algorithmen“ werden die Werte aller Verfahren auf einmal angezeigt.

3.2 Weitere Anwendungsmöglichkeiten

Die Anwendungsmöglichkeiten von Jacksum sind zahlreich. Über die Kommandozeilenversion entfaltet sich das ganze Potential dieser vorzüglichen Software, einschließlich der Interaktion mit anderen Programmen. Die Bereitstellung einer offenen Programmierschnittstelle (API) fördert die breite Akzeptanz.

Prüfsummen werden auch in der Elektrotechnik schon seit vielen Jahrzehnten eingesetzt, unter anderem zur Gewährleistung einer fehlerfreien Datenübertragung.

4 Konsolenbasierte Prüfsummenbildung

4.1 Bordeigene SHA-Algorithmen unter Unix/BSD- und GNU/Linux-Systemen

SHA-Algorithmen sind standardmäßig auf Unix- und unixartigen Systemen vorinstalliert. Öffnen Sie eine Befehlszeilenumgebung (Shell), schreiben Sie „sha“ und drücken Sie dann die Tabulatortaste für die Autovervollständigung, um sich alle vorhandenen SHA-Verfahren anzeigen zu lassen:

```
> sha
> sha1sum sha224sum sha256sum sha384sum sha512sum shasum
> sha
```

Gehen Sie in das entsprechende Verzeichnis, wählen Sie ein Verfahren, fügen Sie den Namen der gewünschten Datei an und drücken Sie die Eingabetaste. Im folgenden Beispiel wird die SHA1-Prüfsumme der Datei test.html gebildet:

```
> sha1sum test.html
4a204c74e481facb40fe674c4e23917d6dedf064 test.html
>
```

Der SHA1-Prüfsummenwert und der Name der zugehörigen Datei werden angezeigt.

Implementierung und Befehlsbezeichnungen können variieren. Praktisch alle Unix- bzw. unixartigen Systeme und Distributionen verfügen über entsprechende Vorinstallationen. Mit den GNU Core Utilities²⁸ können auch MS-Windows-Benutzer zahlreiche Unix-Befehlsoperationen ausführen.

Daneben gibt es dutzendfach freie Programme zur Bildung kryptographischer Prüfsummen, u. a. bei www.sourceforge.net.²⁹

²⁸www.gnu.org/software/coreutils, <http://gnuwin32.sourceforge.net/packages/coreutils.htm>

²⁹Z. B. ReHash, ein konsolenbasiertes Programm in C++, erhältlich für GNU/Linux und MS-Windows, das ebenfalls den GOST-Hashstandard enthält. Projektseite: <http://rehash.sourceforge.net>, Dokumentation: <http://rehash.sourceforge.net/rehash.html>. Textbasierte Programme ermöglichen die effektivste Nutzung von Computern. Einen hervorragenden Überblick bietet Andreas Poisel's www.automatisch.c

5 Informationsquellen zur angewandten Kryptographie und Computersicherheit

Eine Auswahl an weiterführenden Anschriften und Einführungen zur angewandten Kryptographie verweist auf Fortbildungsmöglichkeiten.

Flash-Videofilme von Google Video, Youtube und zahlreichen anderen Videoportalen lassen sich mit einer der kostenlos erhältlichen Videoerweiterungen (Add-Ons) für Mozilla-Firefox abspeichern, z. B. mit dem offiziell empfohlenen „Video DownloadHelper“.³⁰ Der freie VLC-Mediaplayer³¹ eignet sich vorzüglich für die Wiedergabe zahlreicher Medienformate, Flash-Videos eingeschlossen.

5.1 Die qualifizierte elektronische Signatur in der BRD

5.1.1 Leitfaden Elektronische Signatur

Der „Leitfaden Elektronische Signatur“ von Rolf Schmoldt bietet eine umfassende Einführung in die gesetzlich anerkannte elektronische Signatur in Deutschland: www.signatur-e-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf.

5.1.2 Signaturgesetzrelevante Begriffsbestimmungen in der BRD

Die Netzseite des „Bundesministeriums der Justiz“ zum „Gesetz über Rahmenbedingungen für elektronische Signaturen“ (Titel: „SigG – nichtamtliches Inhaltsverzeichnis“) enthält Begriffsbestimmungen (abgerufen am 01. August 2011): http://bundesrecht.juris.de/sigg_2001/index.html#BJNR087610001BJNE000201308

5.1.3 Offizielle Netzseiten der BRD zur Elektronischen Signatur

Eine Auswahl offizieller Informationsseiten der BRD-Bundesnetzagentur zur qualifizierten elektronischen Signatur:

- www.bundesnetzagentur.de → „Sachgebiete“ → „Qualifizierte elektronische Signatur“: http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/QES/QES_node.html
- Englischsprachige Ressourcen (mit offiziellen Gesetzestextübersetzungen): http://www.bundesnetzagentur.de/cln_1931/EN/Areas/ElectronicSignature/QES_node.html

³⁰<https://addons.mozilla.org/de/firefox/addon/3006>. Bei Mozilla erhalten Sie auch zwei der elementarsten Firefox-Erweiterungen für die Förderung der Privatsphäre: „BetterPrivacy“ und „NoScript“.

³¹www.videolan.org/vlc

5.2 Gesetzlich anerkannte, revisionssichere E-Mail-Archivierung

In manchen Wirtschaftszweigen werden E-Mails, die zu Geschäftsabschlüssen/-Aufträgen führen, rechtlich als Handelsbriefe betrachtet. Für ihre Archivierung reichen ein einfaches Abspeichern oder Ausdrucken nicht mehr aus, stattdessen muß revisionssicher archiviert werden, auf eine technische Weise, die ein nachträgliches, nicht feststellbares unbemerktes Manipulieren der E-Mail-Daten ausschließt. Dies erfolgt meistens mit Hilfe von kryptographischen Prüfsummen. Die Softwareempfehlungen auf ComputerBildnis.com enthalten Begriffserläuterungen und Verweise auf Einführungsartikel spezialisierter Rechtsanwälte.³²

5.3 Zwei zentrale Netzseiten zur angewandten Kryptographie

- Bert-Jaap Koops' „Cryptography Law Survey“ gibt Auskunft über die grundsätzliche Gesetzeslage zur Kryptographie in den einzelnen Staaten der Welt. Jeder Eintrag ist mit einer umfassenden weiterführenden Quellsammlung versehen: <http://rechten.uvt.nl/koops/cryptolaw>
- Stefan Kelm's „The PKI-Page“ umfaßt eine riesige, weltumspannende Sammlung von staatlich anerkannten Zertifizierungsstellen (CAs, Certification Authorities), Normen und Spezifikationen sowie zahlreichen weiteren Informationsquellen: www.pki-page.org

5.4 Englischsprachige Videoeinführungen bei Youtube

Das Videoportal Youtube (www.youtube.com) führt hochwertige Einführungen zum Thema angewandte Kryptographie. Eine kleine Sammlung von Videofilmverweisen enthält die Playlist „Encryption Basics“.³³

Zu Kryptographieprogrammen sind zahlreiche grafische Schnittstellen erhältlich. Moderne OpenPGP- und X.509-fähige E-Mail-Programme, wie z. B. Mozilla Thunderbird mit Enigmail, übernehmen die Signierung sowie Ver- und Entschlüsselung vollautomatisch im Hintergrund. Der Benutzer muß lediglich eine Paßphrase eingeben, die optional zwischengespeichert wird.

5.5 Historischer Rückblick bei Google Video

„Celebrating 30 Years of Public Key Cryptography“, ein zweistündiger Rückblick auf die Geschichte der Asymmetrischen Verschlüsselung, dokumentiert Beiträge zahlreicher Kryptographiegrößen.³⁴

³²http://computerbildnis.com/recommendations_de/recommendations_de.html#revisionssichere-E-Mail-Archivierung

³³www.youtube.com/view_play_list?p=DFE23D09B19761B4

³⁴<http://video.google.com/videoplay?docid=-643828532267823915&hl>

5.6 Erhöhte Sicherheit mit freien Betriebssystemen

5.6.1 Quellcode, Programmtext

Betriebssysteme und andere Computerprogramme werden in für Menschen angenehm lesbaren Programmiersprachen geschrieben, z. B. in C, C++. Dieser ursprüngliche Programmtext, der so genannte Quellcode, wird anschließend in den Binärcode/Maschinencode übersetzt, wodurch ein für den Computer lesbares, ausführbares Programm entsteht.

5.6.2 Maschinencode, Binärcode

Ab einer gewissen Größe lassen sich *ausschließlich im Binärcode vorliegende* Programme nur ineffektiv lesen und bearbeiten. Ihre Handhabung ist nicht mehr praktikabel und eine Rückübersetzung bzw. Disassemblierung nur eingeschränkt oder, wenn Teile des Programmcodes noch dazu verschlüsselt wurden, überhaupt nicht mehr möglich. Eine ähnliche Situation liegt vor, wenn ein Hersteller sein Gerät so hermetisch verschließt, daß der Anwender keine Reparaturen mehr vornehmen und keinen Einblick in die Funktionsweise bekommen kann.

5.6.3 Freie Software

Freie Software ist kostenlos erhältlich, sowohl als übersetzte, ausführbare Binärcodeversion wie auch als Quellcode. Der Originalprogrammtext darf angepaßt und modifiziert werden, und diese Veränderungen dürfen wiederum kostenlos weiterverbreitet werden. Verschiedene Lizenzmodelle finden Anwendung.³⁵

Unfreie, so genannte proprietäre Software, ist ausschließlich als Binärcodeversion beziehbar.

5.6.4 Quellcodekontrolle und Hintertürenfreiheit

Heimlich eingebaute Softwarehintertüren könnten Daten- und Wirtschaftsspionage ermöglichen, im Extremfall sogar gezielte Sabotage, insbesondere auch dann, wenn sie von Dritten entdeckt werden.

Aufgrund fehlender Quellcodeverfügbarkeit kann unfreie Software keiner öffentlichen Sicherheitsanalyse unterzogen werden. Ihre Betriebsbereitschaft hängt zunehmend von Aktivierungsservern des Herstellers ab. Versagen diese ihren Dienst, funktioniert auch völlig legal erworbene Software nur noch eingeschränkt oder wird sogar komplett stillgelegt. Dieses Szenario trat in den vergangenen Jahren bereits mehrfach ein, zahlreich dokumentiert durch Nachrichtenarchive: Ganze Betriebssysteme fielen aus, Virens Scanner verweigerten Signaturaktualisierungen.

³⁵www.opensource.org

Quellcodeoffenheit garantiert keine automatisch erfolgende Überprüfung der Programmcodestruktur durch Dritte, die Fehleraufdeckungswahrscheinlichkeit ist jedoch unvergleichbar höher.

Korrumpierte Elektronik, bekannte oder unbekannte „fortschrittliche“ Hardwarearchitekturen mit ab Werk eingebauten „Fernwartungsfunktionen“ stellen die andere Seite des Problems dar. Je nach Einsatzzweck sind Rechnerinsellösungen, die niemals ans Netz gehen, besser dazu geeignet, das Risiko von Wirtschaftsspionage zu minimieren. Eine ganze Reihe von physikalischen Aspekten muß zudem noch beachtet werden, insbesondere die seit langem bekannten Probleme der Abstrahlung und Abschirmung.³⁶

Die zunehmende Miniaturisierung von Fluggeräten eröffnet einen neuen Aspekt der Spionageabwehr, des aktiven Datenschutzes. Illustrierende Artikel und Videofilme: „[Mini-Quadroptero im Formationsflug – Wissenschaft & Technik](#)“³⁷ Das eingebettete Video separat: „[A Swarm of Nano Quadrotors](#)“. „[Aggressive Quadrotors Part III](#)“³⁸ und weitere Filme können auf dem Youtube-Kanal von [TheDmel](#) gesehen werden. Sogar Insekten sollen für Überwachungszwecke zum Einsatz kommen.³⁹

5.6.5 Komplexität und Sicherheit versus Bedienungskomfort

In ihrer reinen, ursprünglichen Form werden Programme über Textbefehle gesteuert. Desktoporientierte Betriebssysteme und Programme verwenden grafische Benutzerschnittstellen mit einer natürlichsprachlichen Menüsteuerung. Dadurch entfällt ein Erlernen der eigentlichen Befehle.

Durch grafische Benutzerschnittstellen und Vollautomatikfunktionen erhöht sich der Umfang des Programmcodes, wodurch auch die Gesamtkomplexität sowie die Anzahl eventueller Programmierfehler größer wird. Weniger Programmcode ist übersichtlicher und leichter zu analysieren.

Komplexitätsreduzierung und konsequente Anwendung von Kryptographie bilden die Leitlinie der OpenBSD-Entwickler (www.openbsd.org). Seit vielen Jahren weltweit erfolgreich im Einsatz, betrachten viele dieses freie Unix/BSD-System als das sicherste Betriebssystem der Welt.⁴⁰ OpenBSD schließt unfreie, nichtdokumentierte Hardwaretreiber grundsätzlich aus.

Je komplexitätsreduzierter ein Betriebssystem ist, je weniger Vollautomatikfunktionen vorhanden sind, desto mehr Einarbeitungszeit wird erforderlich. Normalanwender, die nicht

³⁶Beispielsweise: www.itworld.com, 12. März 2009, „[Researchers find ways to sniff keystrokes from thin air](#)“, by Robert McMillan: www.itworld.com/security/64193/researchers-find-ways-sniff-keystrokes-thin-air

³⁷<http://www.politaia.org/wissenschaft-forschung/mini-quadroptero-im-formationsflug-wissenschaft-technik>

³⁸<http://www.youtube.com/watch?v=S-dkonAXOIQ&feature=related>

³⁹„[Big Brother fürchtet Sie dermassen, dass er Käfer in fliegende Spion-Kameras verwandelt](#)“, <http://euro-med.dk/?p=25593>.

⁴⁰„[AsiaBSDCon 2009: The OpenBSD Release Process: A Success Story](#)“, ca. 30 Minuten: www.youtube.com/watch?v=i7pkyDUX5uM|&feature=channel

hauptberuflich oder hobbymäßig mit (software)technischen Computeraspekten vertraut sind, haben diese Einarbeitungszeit nicht. Bei der Wahl eines freien Betriebssystems muß daher ein Kompromiß zwischen Bedienungskomfort und Sicherheit gefunden werden.

5.6.6 Freie Betriebssystemalternativen, „Binary Blobs“

In vielen Branchen ist man zwingend auf eine proprietäre verschlossene Software angewiesen, da es (noch) keine gleichwertige freie Alternative gibt. Auch ist der Wunsch, mit Software seinen Lebensunterhalt zu verdienen und diese daher zu schützen, verständlich. Computersicherheit hat jedoch genauso ihre Berechtigung. Unzählige kommerzielle Softwarehersteller nutzen zudem völlig legal⁴¹ quelloffenen freien Programmcode, verschlossen in ihren Softwarearchitekturen. Manche Freie-Software-Lizenzen erlauben solch eine Nutzung.⁴²

Für viele Bereiche existieren vollwertige oder für die Mehrheit der Anwender vollkommen ausreichende freie Alternativen. Ein Softwareverzeichnis berichtet von insgesamt ca. 250.000 freien Projekten.⁴³ Besonders vorteilhaft: Für zahlreiche Anwendungszwecke gibt es nicht nur eine, sondern mehrere freie Alternativen. Sogar Betriebssysteme speziell optimiert für alte und sehr alte Computergenerationen werden entwickelt und gepflegt.⁴⁴

Die meisten sogenannten freien Betriebssysteme enthalten zahlreiche *optional* installierbare Binär-code-Treiber, z. B. Grafikkarten-Treiber, zu denen der Hersteller keinen Quellcode und keine Dokumentation veröffentlicht hat. Dadurch entstehen Sicherheitsrisiken sowie Wartungsprobleme. Zwar dürfen diese Binärtreiber kostenlos und als „freie Software“ vervielfältigt und vertrieben werden, aufgrund der Undokumentiertheit handelt es sich jedoch um Binary Blobs.⁴⁵

Die Aufnahme solcher Treiber geschieht nicht böswillig, Betriebssystem-Distributoren beabsichtigen lediglich eine breite Hardwareunterstützung. Trotzdem können die Sicherheitsrisiken nicht ausgeblendet werden.

5.6.7 Dualboot-Option

Gänzlich unfreie und freie Betriebssysteme können parallel auf einer Festplatte betrieben werden. Einige freie Betriebssysteme, z. B. Ubuntu, bieten während der Installation eine vollautomatische Umpartitionierung an, richten sich selbständig neben einem bereits vorhandenen System ein und installieren ein Auswahlmenü (Bootmanager).

⁴¹Oft jedoch auch illegal: <http://gpl-violations.org>

⁴²Z. B. die unter vielen Aspekten maximal Freiheit bietende BSD-Lizenz.

⁴³„Software-Verzeichnis Ohloh indiziert 250.000 freie Projekte“, 27.01.2009, www.heise.de/developer/meldung/Software-Verzeichnis-Ohloh-indiziert-250-000-freie-Projekte-202401.html

⁴⁴Eine Liste spezialisierter Distributionen für alte und sehr alte Computer, „Operating systems for really, really old computers“, <http://ubuntuforums.org/showthread.php?t=575456>; „Distributionen mit minimaler Hardwareanforderung“, http://de.wikipedia.org/wiki/Liste_der_Linux-Distributionen#Distributionen_mit_minimaler_Hardwareanforderung

⁴⁵Binary Blobs waren offizielles Thema der OpenBSD Version 3.9: www.openbsd.org/lyrics.html#39

Ob proprietäre Betriebssysteme in solch einer Dualbootinstallation bei Bedarf ferngesteuert auf für sie eigentlich nicht vorgesehene Festplattenbereiche (Partitionen) zugreifen, ist eine andere Frage.

5.6.8 Betriebssystemempfehlungen

OpenBSD läßt sich als Desktopsystem nutzen, für den Normalanwender ist jedoch eine zu hohe Einarbeitungszeit erforderlich. Aus der Vielzahl freier Betriebssysteme bzw. Distributionen – einige hundert – werden drei kurzportraitiert. Die Desktopkomfortansprüche des „Standardanwenders“ berücksichtigend, empfehlen sich beispielsweise folgende Systeme, die alle auch kostenlos aus dem Internet als ISO-Abbild heruntergeladen und ohne Installation ausprobiert werden können.

Diese Distributionen bilden einen kleinen Ausschnitt aus der Welt freier Betriebssysteme, deren große Anzahl hauptsächlich durch Spezialisierungen auf Anwendungszwecke und Berufsbranchen zustandekommt.

5.6.9 Erstklassiges freies Betriebssystem: Ubuntu 10.04 LTS

Basierend auf Debian GNU/Linux, erstmals erschienen im Jahr 2004, bietet Ubuntu Linux (www.ubuntu.com) ausgereiften, umfassenden Desktopkomfort: vollautomatische Installation, Vorkonfigurierung sowie Hardware- bzw. Geräteerkennung. Größtmöglicher Bedienungskomfort bildet seit Anbeginn den Schwerpunkt dieser beliebten, weltweit vermutlich am weitesten verbreiteten GNU/Linux-Distribution.

Version 10.04 LTS stellt einen Meilenstein dar. Ubuntu läßt sich nun unter fast allen Aspekten so einfach benutzen wie zwei bekannte proprietäre Betriebssysteme; in mehrfacher Hinsicht bietet es weit mehr Möglichkeiten und Komfort.⁴⁶ Viele Tausende von Programmen für die unterschiedlichsten Anwendungsbereiche lassen sich kostenlos herunterladen und zentral verwalten. GNOME (www.gnome.org), standardmäßig vorinstalliert, sowie KDE (www.kde.org) gehören zu den populärsten Desktopoberflächen; beider Erscheinungsbild läßt sich umfassend den persönlichen Vorlieben anpassen, beide Desktopsysteme können parallel installiert und genutzt werden. Die KDE-Variante Kubuntu dürfte insbesondere MS-Windows-Nutzer ansprechen.⁴⁷

Ubuntu ist frei, proprietäre Treiber können optional installiert werden.

5.6.10 PC-BSD und gNewSense

PC-BSD PC-BSD (www.pcbsd.org) ist FreeBSD (www.freebsd.org),⁴⁸ ein echtes Unix in einer Desktop-optimierten Version. Neben den vielen Tausenden frei erhältlichen

⁴⁶www.whylinuxisbetter.net/index_de.php?lang=de

⁴⁷Plasma-Desktop: www.kde.org/workspaces/plasmadesktop, www.kubuntu.org

⁴⁸„How the FreeBSD Project works“, 50 Minuten, Google Tech Talks: www.youtube.com/watch?v=nNkqKdLm1rU

Programmen für FreeBSD (Ports-System) zeichnet sich PC-BSD durch das PBI-Paket-System aus, das eventuelle Paket-/Softwarebibliotheksabhängigkeiten vermeidet. Über den Linuxemulationsmodus laufen auch GNU/Linux-Programme. Als Standardbenutzeroberfläche kommt KDE zum Einsatz,⁴⁹ wahlweise auch GNOME. Das Code-Audit (Programmcode-Analyse, -Qualitätssicherung) der *freien* BSD-Systeme und die daraus resultierende Stabilität und Sicherheit sind legendär; viele kommerzielle Softwarehersteller benutzen firmenintern FreeBSD. PC-BSD bietet eine hochkomfortable Installation,⁵⁰ Bedienung und Verwaltung.⁵¹ Die Hardwareunterstützung ist noch nicht vergleichbar umfassend wie bei Ubuntu Linux, es ist jedoch lediglich eine Frage der Zeit, bis auch PC-BSD uneingeschränkt für Normalanwender geeignet ist.

DesktopBSD (www.desktopbsd.net) richtet seinen Schwerpunkt ebenfalls auf klassischen Desktopkomfort.

gNewSense gNewSense (www.gnewsense.org) hat sich Freiheit von jeglichem schwarzen Programmcode, von Binary Blobs, zum Ziel gesetzt. Firefox, Thunderbird und andere Mozilla-Produkte sind in einer eigens angepaßten und umbenannten Version erhältlich. *gNewSense ist das einzige wirklich gänzlich freie Betriebssystem, das auch von Normalanwendern installiert und bedient werden kann.* Es gehört zu den wenigen 100 % Binary-Blob-freien Distributionen,⁵² die offiziell von der Free Software Foundation (www.fsf.org) empfohlen werden. Die FSF vertritt proprietären Anwendungen⁵³ und Betriebssystemen⁵⁴ gegenüber einen äußerst skeptischen Standpunkt.

5.7 Weitere Seiten zum Thema Computersicherheit

- „Heise Security“ bietet plattformübergreifend umfassende Informationen zur Computersicherheit. Die deutsche Version: www.heise.de/security
- Die englische Version, „The H Security“: www.h-online.com/security
- Cryptool, ein freies „E-Learning-Programm“ zum Themenbereich Kryptographie, vermittelt auf visuelle Weise Grundlagenwissen: www.cryptool.de.

⁴⁹KDE Visual Guide: www.kde.org/announcements/4.4/guide.php

⁵⁰„PC-BSD, Matt Olander, AsiaBSDCon 2008“, ca. 29 Minuten: www.youtube.com/watch?v=N0q37X-MJzY

⁵¹„Kris Moore: PC-BSD – Making FreeBSD on the Desktop a reality“, ca. 42 Minuten: www.youtube.com/watch?v=7VYyQvzdD9g&feature=channel

⁵²Liste der freien Distributionen: www.gnu.org/distros/free-distros.html

⁵³<http://www.fsf.org/campaigns>

⁵⁴Deutsch: <http://de.windows7sins.org>, englisch: <http://en.windows7sins.org>

6 Impressum, Bezugsquellen, Urheberrecht, Lizenz

6.1 Impressum

Peter Jockisch
Habsburgerstraße 11
79104 Freiburg i. Br.
Deutschland

Netzpräsenz: www.computerbildnis.com

E-Post: info@computerbildnis.com

Meine gesamte E-Post wird ausnahmslos immer kryptographisch signiert, Dateianhänge miteingeschlossen (PGP/MIME). OpenPGP-Schlüssel-ID erstes Quartal 2012: 9774AB05, zugehöriger Schlüsselfingerabdruck: 1BB0 C27C 4428 78AC 4B93 1542 6A74 17EB 9774 AB05. Ich benutze keinen anderen Schlüssel außer den mit obigen Kenndaten.

Einzige offizielle Schlüsselbezugsquelle: <http://www.peterjockisch.de/impressum/impressum.html>. Neue Schlüssel (Nachfolgeschlüssel) werden in der Nachrichtenrubrik von PeterJockisch.de angekündigt.

Ich versende grundsätzlich keine Werbe-E-Mails, Neuigkeiten können über RSS-Nachrichtenticker abgerufen werden.

Ich kommuniziere auf geschäftlicher Ebene grundsätzlich nicht über Telefon, das für einen Identitätsnachweis wenig geeignet ist. Telefonische Auskünfte werden grundsätzlich nicht erteilt. Ich besitze kein Mobiltelefon und lehne entsprechende Verträge oder Angebote ab.

Da Telefonie für den Identitätsnachweis absolut ungeeignet ist – jeder kann sich für jeden ausgeben – führe ich nur im engsten Freundes- und Familienkreis Telefonate, dies ausschließlich im Festnetz. Mobilfunktelefonie, SMS und Fax nutze ich prinzipiell nicht.

6.2 Urheberrecht

Urheberrecht an Text und Bildern sowie an Übersetzungsrechten 2008 – 2011 bei Peter Jockisch. Alle Illustrationen wurden selbsterstellt. Die Bildschirmfotos und die zur Illustration der Programmfunktionalität verwendeten, in Anleitungen abgebildeten Ikonen (Icons), sind im Einklang mit den Microsoft-Urheberrechtsrichtlinien zu Bildern, Stand: 15.04.2004, abgerufen am 04. Februar .2012.⁵⁵

Microsoft Windows®, evtl. weitere Bezeichnungen sowie Teile der in den Bildschirmfotos enthaltenen Logos, Grafiken, Software-Dialoge und Dateisymbole sind eingetragene Warenzeichen bzw. urheberrechtlich geschützte Begriffe und Werke der Firma Microsoft Deutschland GmbH, D-85716 Unterschleißheim, bzw. der Microsoft Corporation, Redmond, Washington 98052-6399, USA. Alle aufgeführten Markennamen, Handelsmarken und Werktitel sind das Eigentum ihrer jeweiligen Besitzer.

6.3 Artikellizenz

Diese Lizenz regelt die Nutzung des Artikels „Praktische Anwendung Kryptographischer Prüfsummen“, veröffentlicht auf www.computerbildnis.com und www.peterjockisch.de.

Artikelbezugsquelle

Artikelhauptseite, PDF- und Epub-Dateibezug: www.computerbildnis.com/it-articles_de/checksums_de/checksums_de_title.html.

⁵⁵Quelle: www.microsoft.com/germany/unternehmen/informationen/rechtlichehinweise/bilder.aspx#ECGAC, englische Version: www.microsoft.com/about/legal/permissions/default.aspx#EBD.

In der Enzyklopädie Knol wird eine HTML-Artikelversion gepflegt: <http://knol.google.com/k/peter-jockisch/praktische-anwendung-kryptographischer/28iq7as7cmqev/4>.

Urheber

Alleiniger Urheberrechteinhaber des Artikels: Peter Jockisch, Freiburg i. Br., Deutschland.

Integritätswahrung

Sie dürfen dieses Dokument, die *unveränderte* Original-PDF-Datei, in elektronischer oder gedruckter Form unter den hier aufgeführten Bedingungen 100 % frei von jeglichen Kosten oder Gebühren nutzen. Prüfsummen aller Artikelversionen können auf der Artikelhauptseite unter www.computerbildnis.com eingesehen werden. Eine Nutzung darf nur in lizenzkompatiblen Umgebungen erfolgen.

Keine schriftsatztechnische Integration in andere Werke

Der Artikel darf als eigenständige Einheit unter den in dieser Lizenz aufgeführten Bedingungen verwendet werden, eine (schrift-)satztechnische Übertragung/Integration in andere Werke oder Kompilationen, z. B. in Büchern und ähnlichen Druckprodukten, E-Büchern (Ebooks) usw., ist nicht erlaubt.

Eine lizenzkostenfreie Nutzung im Rahmen von *ausgedruckten oder fotokopierten* zusammengestellten kommerziellen Kursunterlagen ist erlaubt, die Eigenständigkeit des Artikels muß jedoch erkenntlich bleiben. Für diese separate Artikeleinheit dürfen Sie Ihren Kunden lediglich Ihre Selbstkosten (Materialkosten [Papier, Toner, Tinte, ...] und den Arbeitsaufwand zur Vervielfältigung) in Rechnung stellen.

Veröffentlichung im Internet und hausintern (Intranet)

Die technische (physikalische, serverbezogene) Veröffentlichung im Internet bleibt ComputerBildnis.com und PeterJockisch.de vorbehalten. Ein dauerhafter Direktverweis (Hotlinking) auf die PDF- bzw. Epub-Datei ist über PeterJockisch.de möglich.

Hinweise für das Setzen von Direktverweisen: Alle unter PeterJockisch.de veröffentlichten Artikel- und Buchversionen sind für eine permanente Direktverknüpfung vorgesehen, die Pfade und Dateinamen bleiben dauerhaft unverändert, auch nach Aktualisierungen. Kommerzielle Seiten mit paßwortgeschützten Bezahlbereichen dürfen ebenfalls Direktverweise setzen, jedoch darf nicht der Artikel selbst verkauft oder relizenziert werden.

Eine hausinterne bzw. firmeninterne Verteilung und Abrufbereithaltung über Netzwerkserver ist gestattet, lokal, regional, national und international, immer begrenzt auf den Rahmen des Intranets: Sie dürfen die Original-PDF- bzw. Epubdatei sowie Ausdrücke und Fotokopien auf interner Ebene kostenlos vervielfältigen, verteilen, nutzen, archivieren (auf Festplatten und anderen Datenträgern), zeitlich unbefristet, in privaten, in öffentlichen und auch in kommerziell ausgerichteten Einrichtungen, beispielsweise im Rahmen von kommerziell gehaltenen PC-Kursen.

Internetcafés dürfen dieses Dokument ebenfalls intern abrufbereit halten (für sich selbst und als Anleitung für ihre Kunden), einschließlich auf überregional betriebenen firmennetzwerkinternen Servern und direkt auf PC-Festplatten vor Ort (Verwaltungs-PCs und Internetcafébesucher-Terminals/-PCs), in Fillialen.

Die physikalische Zurverfügungstellung im Internet bleibt ausschließlich ComputerBildnis.com und PeterJockisch.de vorbehalten.

Ausdrucke

Sie dürfen dieses Dokument in Schwarzweiß oder Farbe ausdrucken und vervielfältigen sowie Fotokopien anfertigen, z. B. für Kursunterlagen. Wahlweise können Sie hierbei zwei Dokumentseiten zu einer Papierseite zusammenfassen – ausschließlich über die Druckoption Ihres PDF- bzw. Epub-Betrachters, nicht manuell über Schriftsatzprogramme.

Computerbildschirm und Projektion

Sie dürfen die PDF-Datei- und die Epub-Datei am Computerbildschirm und für Vorträge/Präsentationen mit Bildprojektoren nutzen.

Andere Formen der Nutzung

Die Verwendung für Lesegeräte oder Brailleausrucke ist erlaubt.

Keine Gebühren

Dieses Dokument darf in lizenzkompatiblen Umgebungen, zu 100 % frei von jeglichen Gebühren zeitlich unbefristet genutzt werden, kommerzielle Schulungen und Kurse miteingeschlossen. Der Artikel alleine darf jedoch weder verkauft noch relizensiert werden.

Ich erhebe keine wie auch immer gearteten Gebühren, weder direkt noch indirekt; auch habe ich keine Repräsentanten, und meine E-Mails werden ausnahmslos immer kryptographisch signiert, ich schreibe keine unsignierten E-Mails.

Die Finanzierung von ComputerBildnis.com wird indirekt über Werbeanzeigen auf der Netzseite erfolgen. Alle Artikel und Bücher bleiben grundsätzlich frei von Werbung und frei von Gebühren jeglicher Art. Alle Produkte sind ausschließlich direkt erhältlich (kostenlos herunterladbar). Für den Bezug sind weder E-Mail, noch Registrierung, noch persönliche Daten irgendwelcher Art erforderlich. Die physikalische Publikation im Internet bleibt ausschließlich ComputerBildnis.com und PeterJockisch.de vorbehalten, beide Seiten sind die einzigen offiziellen Bezugsquellen für kostenlose Artikel und Bücher von [Compu terBildnis.com](http://ComputerBildnis.com) bzw. von Peter Jockisch (Freiburg i. Br.) sowie der zugehörigen Prüfsummen.