

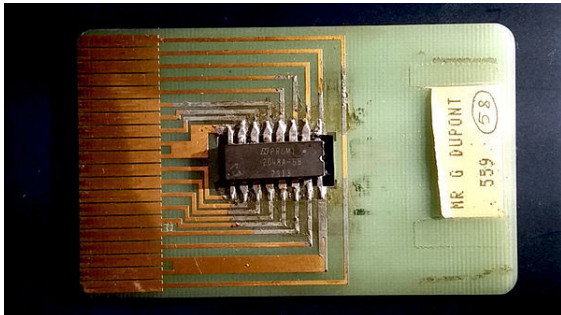
Chipkarte



Chipkarte

Chipkarte, oft auch als **Smartcard** oder **Integrated Circuit Card (ICC)** bezeichnet, ist eine spezielle Kunststoffkarte mit eingebautem integriertem Schaltkreis (Chip), der eine Hardware-Logik, Speicher oder auch einen Mikroprozessor enthält. Chipkarten werden durch spezielle Kartenlesegeräte angesteuert.^[1]

1 Geschichte



Prototyp der Chipkarte von Roland Moreno aus 1975

In der Geschichte der Chipkarte prägten zwei Erfinder mit ihren Patenten die Entwicklung der Chipkarte in der heutigen Form.

Als erster reichte am 10. September 1969 der deutsche Erfinder Jürgen Dethloff zusammen mit Helmut Gröttrup seine Idee, in einen „Identifikanden einen speziellen integrierten Kreis einzubauen“, zum Patent ein.^[2] Der zweite Erfinder ist der Franzose Roland Moreno, der sein Patent^[3] 1975 anmeldete. Auf der Webseite des *US Patent and Trademark Office* ist es unter dem Datum 30. Mai 1978 registriert. Er beschreibt darin ein „unabhängiges, elektronisches Objekt, entwickelt für die Speiche-

rung von vertraulichen Daten“, das den Zugriff nach der Eingabe eines „geheimen Codes“ (PIN) freigibt.

In den USA gilt **Vernon Schatz** als grundlegender Patent-Inhaber (Patent 1977).

2 Klassifikation

Chipkarten können nach unterschiedlichen Kriterien unterschieden werden. Die eingängigste ist die Unterscheidung zwischen *Speicher-Chipkarten* mit einfacher Logik und *Prozessor-Chipkarten* mit eigenem Karten-Betriebssystem und kryptografischen Fähigkeiten.

Diese Einteilung ging lange konform mit der Einteilung in *synchrone Karten* (Speicherchipkarten; Protokolle: 2wire, 3wire, ...) und *asynchrone Karten* (Prozessorchipkarten; Protokolle: T=0, T=1). Mittlerweile gibt es auch *Secure Memory Cards* mit erweiterten Sicherheitsmerkmalen (DES oder AES-Verschlüsselung) und Speicher-Chipkarten, die über *asynchrone Protokolle* funktionieren (GemClub Memo), letztere sind dadurch sehr einfach über das PC/SC-System in eigene Applikationen zu integrieren.

Chipkarten werden auch über die Schnittstelle nach außen unterschieden. Den *kontaktbehafteten Chipkarten* stehen die *kontaktlosen RFID Chipkarten*, oder auch *Transponderkarten*, wie die *Mifare*- oder *Legic*-Karten, gegenüber. Chipkarten mit mehreren (unterschiedlichen) Chips werden *hybride Karten* genannt, es gibt am Markt allerdings auch Chips, die über beide Schnittstellen angesprochen werden können (*Dual Interface Karten*). Zusammen mit PC/SC2 ergeben sich damit innovative Verwendungsmöglichkeiten.

3 Aufbau

Der wichtigste Bestandteil der Chipkarte ist der **integrierte Schaltkreis**, der die Fähigkeiten und somit das Anwendungsgebiet der Chipkarte bestimmt.

Der Chip wird vom Chipkartenmodul geschützt, so dass der Chip normalerweise von außen nicht sichtbar ist. Das Modul stellt auch die Verbindung zur Außenwelt dar, die typischen Goldkontakte des Chipkartenmoduls werden oft fälschlicherweise als Chip bezeichnet. Obwohl ein gebräuchlicher Chipkarten-Chip zur Kommunikation nur fünf Kontakte braucht, haben Chipkartenmodule immer, bestimmt durch die Größe des eingebauten Chips, sechs



Verschiedene Kontakte von Chipkartenmodulen

oder acht Kontakte, allerdings nur um den ISO-Normen zu entsprechen.

Letztendlich wird das Modul inklusive Chip in eine Karte eingebaut. Dazu wird in eine bereits bedruckte Karte eine Kavität geätzt und das Modul eingeklebt.

Viele Chipkarten, insbesondere für den Mobilfunk, haben eine eindeutige ICC-ID bzw. ICCID, diese ist 19- bis 20-stellig, darunter eine Prüfziffer.

4 Formate

Die Kartenabmessungen sind nach ISO 7816 standardisiert und gemäß dieser Norm in drei verschiedenen Größen verfügbar:

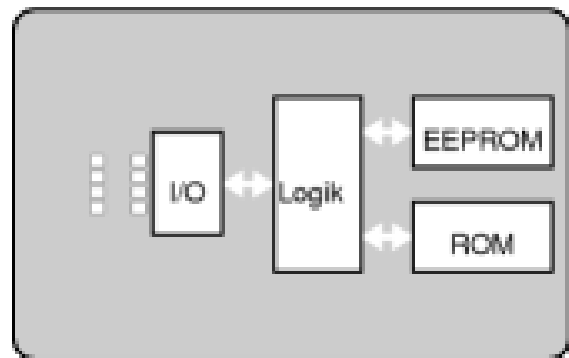
- **ID-1**: Das größte und am weitesten verbreitete Format (85,60 mm × 53,98 mm) wird bei **EC-Karten**, **Telefonkarten**, dem **EU-Führerschein** oder der **Krankenversicherungskarte** verwendet. Man spricht auch vom **Scheckkarten-Format**.
- **ID-00**: Das mittlere Format (66 mm × 33 mm) hat bisher keine größere Anwendung gefunden.
- **ID-000**: Das kleinste der Formate (25 mm × 15 mm) findet vor allem bei **SIM-Karten** in Mobiltelefonen Verwendung.

Daneben gibt es weitere typische Größen:

- **Mini-UICC** (12 mm × 15 mm): kaum größer als die Kontaktflächen
- **Visa-Mini** (65,6 mm × 40,0 mm): **Visa**-eigenes Format

Die Dicke der Karten aller Größen ist einheitlich und beträgt 0,762 mm (exakt 0,03 Zoll).

5 Speicherchipkarten



Blockschaltbild einer Speicherchipkarte

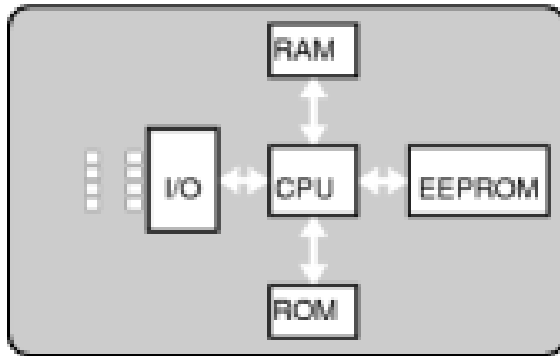
Die einfachen Chipkarten bestehen nur aus einem Speicher, der ausgelesen oder beschrieben werden kann, z. B. die **Krankenversicherungskarte** oder die **Telefonkarte**. Über die Schnittstelle ist es möglich, sequenziell auf die einzelnen Speicherzellen zuzugreifen. Verwendung finden Speicherkarten dort, wo es nur auf die Speicherung der Daten ankommt, nicht aber auf das Abwickeln komplexer Vorgänge.

Komplexere Chipkarten kombinieren mehrere Speichertechnologien in einer Karte und werden als Hybridkarten bezeichnet. So können Hybridkarten über einen kontaktbehafteten und einen kontaktlosen Chip, aber auch über einen Magnetstreifen mit **RFID-Chip** verfügen.

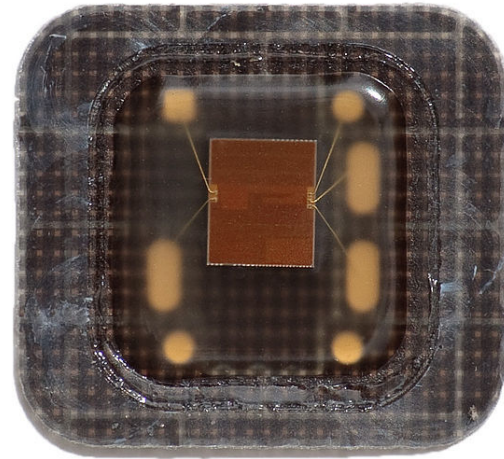
Abhängig von dem verwendeten Chip können die Daten durch PINs oder Passwörter vor dem Auslesen oder der Veränderung durch Dritte geschützt werden.

6 Prozessorchipkarten

Prozessorchipkarten verfügen über einen Mikroprozessor, über den man auf die gespeicherten Daten zugreifen kann. Es gibt oft keine Möglichkeit, auf den Datenbereich direkt zuzugreifen. Der Umweg über den Mikroprozessor erlaubt es, die Daten auf der Karte über kryptographische Verfahren vor fremdem Zugriff zu schützen. Die Möglichkeit, auf diesen Mikroprozessoren anwendungsspezifische Programme laufen zu lassen, bietet viele Vorteile im Vergleich zu Speicherkarten, z. B.



Blockschaltbild einer Prozessorchipkarte



Nahaufnahme vom Chipmodul von der Rückseite aus. Der Mikroprozessor ist das braune Rechteck in Bildmitte

bei Chipkarten, die als Zahlungsmittel verwendet werden (**GeldKarte**) oder wichtige Daten (z. B. SIM-Karten für Handys) enthalten. Oft enthält die Karte auch einen signierten Schlüssel und dient als Dekoderkarte (z. B. beim **Bezahlfernsehen** oder sonstigen Zugangssystemen). Bereits bei der Herstellung der Chips werden Teile des Karten-Betriebssystem (COS) und die vorgesehenen Anwendungen auf die Karte geladen.

Die Smartcards können als sicherer Informations- oder Schlüsselspeicher dienen, aber sie bieten auch verschiedene Sicherheitsdienste wie Authentifizierung, Verschlüsselung, Signatur usw. an, die in einer vertrauenswürdigen Umgebung genutzt werden können. Da die privaten Schlüssel auf der Smartcard gespeichert sind und diese nicht verlassen, ist das Erspähen des Schlüssels nicht möglich, weswegen eine Signaturerzeugung auf der Smartcard sehr sicher ist.

Auf Prozessorchipkarten läuft ein eigenes Betriebssystem. Dies kann zum Beispiel **BasicCard**, **CombOS**, **CardOS**, **JCOP**, **MTCOS**, **MultOS**, **SECCOS**, **Sicrypt**, **STARCOS** oder **TCOS** sein.

Die Prozessorchipkarten lassen sich wiederum in zwei Kategorien aufteilen. Dies sind Karten mit einem festen Befehlssatz, der nur vom Hersteller des Betriebssystems angepasst werden kann, und frei programmierbare Karten, die über eine Entwicklungsumgebung um eigene Befehle bzw. Kommandos erweitert werden können. Karten mit festem Befehlssatz implementieren in der Regel Kommandos gemäß dem ISO7816 Standard (ISO7816-4 und folgende). Beispiele für Karten mit festem Befehlssatz sind CardOS, STARCOS, SECCOS und TCOS. Frei programmierbare Karten folgen teilweise ebenfalls diesem Standard, können aber auch um weitere proprietäre Kommandos erweitert werden. Hierzu implementieren sie meist eine **Virtuelle Maschine**. Beispiele hierfür sind die Java-Karten (zum Beispiel JCOP), MULTOS und die BasicCard.

6.1 Chipkarten-Applikation

Die Applikationen auf den Prozessorchipkarten selbst sind, trotz Standardisierung durch **ISO 7816**, in hohem Maße vom Chipkartenbetriebssystem abhängig. **PKCS#15** standardisiert die Applikation auf der Chipkarte selbst, während für die Verwendung durch Rechnerapplikationen **PKCS#11** die standardisierte Schnittstelle ist. Daneben existieren noch proprietäre Schnittstellen wie **CSP** (Cryptographic Service Provider) von Microsoft.

6.2 Javakarte

Javakarten sind Mikroprozessorkarten mit einer reduzierten **Java-Virtual-Machine** als Betriebssystem. Bei diesen Karten kann ein Programmierer nach der Fertigstellung der Karte über ein Kartenlesegerät und eine spezielle Ladesoftware neue Programme, sogenannte Applets, auf die Karte laden. So können Karten mit sehr speziellen Funktionalitäten in Kleinserie kosteneffizient hergestellt werden. JavaCard Betriebssysteme sind z. B. **JCOP** (**IBM/NXP**) oder **SmartCafe** (**Giesecke & Devrient**). Details sind vom Industrieverband GlobalPlatform spezifiziert, so dass eine gewisse Interoperabilität gewährleistet ist.

6.3 BasicCard

Die **BasicCard** ist eine in **BASIC** programmierbare Mikroprozessorkarte, die wie auch die Java Card mit einer Virtual Machine arbeitet. Die in BASIC erstellten Anwendungen können nach der **Kompilierung** mit einem Kartenlesegerät in die Karte übertragen werden. Die Entwicklungsumgebung ist kostenlos verfügbar. Karten sind auch in kleinen Stückzahlen für jedermann verfügbar.

Die Karte eignet sich somit auch für kleinere und private Projekte.

7 Host/Software-API

Die Interaktion zwischen Computersystemen und Chipkartenleser bzw. Chipkartenapplikationen ist im PC/SC-Standard standardisiert. Die Version 2 der PC/SC-Spezifikation behandelt neben höherklassigen Kartenlesern auch die Einbindung von asynchronen Speicherchipkarten und kontaktlosen Chipkarten in das PC/SC-System, zum Beispiel wie ein **ATR** (Answer to Reset) dieser Karten gebildet wird. Einige Treiber von Kartenleserherstellern sind mittlerweile PC/SC2-konform. Die ältere CT-API („CardTerminal Application Programming Interface“) ist im Rahmen der von *Teletrust Deutschland* herausgegebenen MKT-Spezifikation (MKT steht für „Multifunktionales Kartenterminal“) definiert worden. Diese Spezifikation ist hauptsächlich im deutschsprachigen Raum verbreitet. CT-API wird vor allem deshalb genutzt, da hier die Verwendung von Elementen höherklassiger Chipkartenleser (Pinpad, Display) standardisiert ist. Der Zugriff über PC/SC war bis zu PC/SC2 proprietär.

8 Hersteller

In Deutschland sind die Konkurrenten **Giesecke & Devrient**, **Sagem Orga** und die **Bundesdruckerei** Marktführer, weltweit die **Gemalto nv** (50 % weltweit, 30 % in Europa) und **Oberthur Technologies**. Der Weltmarkt wird 2007 geschätzte 2,9 Milliarden Karten umfassen, davon geschätzte 70 % für Handys (SIM-Karten), 16 % EC-Karten und Kreditkarten, der Rest für Ausweise von Pässen bis Skiausweise, Fahrkarten etc.

Mit weltweit mehr als 10.000 installierten Systemen ist die **Mühlbauer AG** aus **Roding** einer der führenden Hersteller für Hardware- und Softwarelösungen rund um die Produktion und Personalisierung von Chip- und Kunststoffkarten.

9 Anwendungsbeispiele

Kontaktbehaftete wie kontaktlose RFID-Chipkarten werden zunehmend für immer mehr Applikationen benutzt. Die Eignung einer Chipkarte für eine konkrete Anwendung hängt von vielen Faktoren ab, in der Regel von der Notwendigkeit einer Datenübertragung via Funktransponder, der Speichergröße und den Sicherheits- und Verschlüsselungsmechanismen. Eine Auswahl über mögliche Chipkartenanwendungsgebiete:

- Ausweise

- Zeiterfassung
- Zutrittskontrolle
- Zahlungsverkehr

10 Testen von Chipkarten

Mit der immer größer werdenden Verbreitung von Chipkarten wird es auch immer wichtiger, die Leistungsfähigkeit dieser Karten zu gewährleisten bzw. zu verifizieren. Die Tests erstrecken sich dabei von Prüfungen des Kunststoffkörpers bis zu Applikationstests der Chipkartenanwendung. Ein OpenSource-Werkzeug, mit dem sich diese Applikationstests komfortabel durchführen lassen, ist **GlobalTester**, basierend auf Global Platform, einem Standard für offene und interoperable Infrastrukturen für Chipkarten und Terminals.

11 Siehe auch


- JobCard
- Elektronische Geldbörse
- GeldKarte
- Quick (Geldkarte)
- Elektronische Gesundheitskarte
- Reisepass
- Digitales Belegwesen
- E-Ticket
- Bürgerkarte
- Telefonkarte
- Application Protocol Data Unit (APDU) Kommunikationsprotokoll

12 Literatur

- Wolfgang Rankl, Wolfgang Effing: *Handbuch der Chipkarten. Aufbau, Funktionsweise, Einsatz von Smart Cards*. 5. überarbeitete und erweiterte Auflage. Hanser Verlag, München 2008, ISBN 978-3-446-40402-1.
- Wolfgang Rankl: *Chipkarten-Anwendungen. Entwurfsmuster für Einsatz und Programmierung von Chipkarten*. Hanser Verlag, München u. a. 2006, ISBN 3-446-40403-1.

13 Weblinks

 **Commons: Smart cards** – Sammlung von Bildern, Videos und Audiodateien

 **Wiktionary: Chipkarte** – Bedeutungserklärungen, Wortherkunft, Synonyme, Übersetzungen

- Klaus Finkenzeller: kontaktlose Chipkarten

14 Einzelnachweise

- [1] *Definition Chipkarte*. Abgerufen am 16. Februar 2015.
- [2] Patentschrift DE000001945777A vom 13. September 1968, Seite 8, zu recherchieren im **Depatis-System** des Deutschen Patent- und Markenamts
- [3] Systems for storing and transferring data in der *USPTO Patent Full-Text and Image Database (englisch)*

Normdaten (Sachbegriff): **GND: 4147723-6**

15 Text- und Bildquellen, Autoren und Lizenzen

15.1 Text

- **Chipkarte** *Quelle:* <https://de.wikipedia.org/wiki/Chipkarte?oldid=167536828> *Autoren:* Aka, LosHawlos, Crissov, Arved, Matthäus Wander, Seewolf, Nephelin, Raymond, Zwobot, Ocrho, D, Murli, Southpark, Jpp, Paparodo, Perrak, MartinWoelker, Peter200, Sadduk, Liquidat, Theclaw, Pta, TheK, Special~dewiki, Koerpertraining, Cepheiden, Thomas Willerich, Silberchen, T-ater, HAL Neuntausend, MarioS, Kuli, Forevermore, Mchelge, Andreas -horn- Hornig, Monarch, VisualBeo, Polluks, Caronna, Bierdimpfl, Pelz, Bombenleger, Diba, Harnsworth, M. Schlusche, Himuralibima, Jergen, Jailbird, FlaBot, Gerbil, Antaios, Emes, Hubertl, Snupie37, Frquadrat, Evaa, Kolja21, Scooter, Spawn Avatar, Wikij, Peisi, RobotE, Octoate, JanRieke, RobotQuistnix, WikiCare, YurikBot, Sjo, WikiJourney, Stargaming, Eskimbot, Wikipit, Kaisersoft, Pen-pen, Guenson, Goodbye, Jörg Behrens, Thornard, Dc4mg, Wdwd, DirkDe, DeMonsoon, Roberta F., Tönjes, Stefan.lefnaer, Doppi22, Semper, Spuk968, FiftySeven, Thijs!bot, HubiB, Summ, YMS, Johanna R., Bernard Ladhenthin, Schon-Vergeben, Quickfix, Muck31, Mojo1442, Viker~dewiki, ComillaBot, Nolispanmo, CommonsDelinker, FANSTARbot, Dr. Karl-Heinz Best, HHE99, BeeKaaEll, Diwas, Gerakibot, VolkovBot, P UdK, AlnoktaBOT, Snahlemmuh, TXiKiBoT, Claus Ableiter, Regi51, Claude J, Hannes Röst, Smoove-Raver, Juliabackhausen, Willchisum, BotMultichill, SieBot, Fipptehler, Der kleine grüne Schornstein, Dlm310, Zbisasimone, OKBot, Trustable, Aktionsbot, Fkbreitl, PipeBot, Querverplänkler, Woche, Sieobserver, Nzm, Der Naturfreund, Penemue, Nongrafics, Zorrobot, Franz Halver, Jeremiah21, Ptbotgourou, Nallimbot, Rumbero, Williwilli, Rubinbot, Xqbot, Scebert, MerlLinkBot, Nicole Baumann, BenzolBot, GedSperber, Nothere, NeGiAm, Izackhack, TjBot, DerGraueWolf, Martin1978, HRoestTypo, EmausBot, ReinerSpass, Imbericle, ZéroBot, Cologinix, Satansfreund, Mstrueh, Randolph33, Pavbrand, 9mag, Kasirbot, Becker-partner, SchalkG, Mosfet81, Ewetzlma, Mmovchin, Monow, Addbot, Jonas Tietgen, Werddemer, ITsecu, KlausDieterSchmitt, Schnabeltassentier, IamvibratioN, Sebastian.T.Schork, GermanTechNerd und Anonyme: 153

15.2 Bilder

- **Datei:Chipkarte.jpg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/a/a9/Chipkarte.jpg> *Lizenz:* CC-BY-SA-3.0 *Autoren:* Eigenes Werk
Originaltext: selbst fotografiert *Ursprünglicher Schöpfer:* de:Benutzer:Monarch
- **Datei:Commons-logo.svg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/4/4a/Commons-logo.svg> *Lizenz:* Public domain *Autoren:* This version created by Pumbaa, using a proper partial circle and SVG geometry features. (Former versions used to be slightly warped.) *Ursprünglicher Schöpfer:* SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.
- **Datei:Differentsmartcardpadlayouts.jpg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/8/80/Differentsmartcardpadlayouts.jpg> *Lizenz:* GFDL *Autoren:* I scanned these and merged them together *Ursprünglicher Schöpfer:* Hywel Clatworthy
- **Datei:Mh_chipkarte_asynchron.png** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/d/d1/Mh_chipkarte_asynchron.png *Lizenz:* CC-BY-SA-3.0 *Autoren:* Übertragen aus de.wikipedia nach Commons. *Ursprünglicher Schöpfer:* Der ursprünglich hochladende Benutzer war LosHawlos in der Wikipedia auf Deutsch
- **Datei:Mh_chipkarte_synchron.png** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/7/7c/Mh_chipkarte_synchron.png *Lizenz:* CC-BY-SA-3.0 *Autoren:* Übertragen aus de.wikipedia nach Commons. *Ursprünglicher Schöpfer:* Der ursprünglich hochladende Benutzer war LosHawlos in der Wikipedia auf Deutsch
- **Datei:Prototype_moreno2.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/e/ed/Prototype_moreno2.jpg *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* ByB
- **Datei:QSicon_rot_Uhr.svg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/2/20/QSicon_rot_Uhr.svg *Lizenz:* Public domain *Autoren:* abgeleitet von File:QS icon orange abwartend.svg *Ursprünglicher Schöpfer:* AleXXw, Zesal
- **Datei:Qsicon_Quelle.svg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/b/b7/Qsicon_Quelle.svg *Lizenz:* CC BY 3.0 *Autoren:* based on Image:Qsicon_Quelle.png and Image:QS icon template.svg *Ursprünglicher Schöpfer:* Hk kng, Image:Qsicon_Quelle.png is by User:San Jose, Image:QS icon template.svg is by User:JesperZedlitz
- **Datei:Smart-Card-Chip_back.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/0/0d/Smart-Card-Chip_back.jpg *Lizenz:* CC BY-SA 3.0 *de Autoren:* Selbst fotografiert *Ursprünglicher Schöpfer:* jailbird
- **Datei:Wiktfavicon_en.svg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/c/c3/Wiktfavicon_en.svg *Lizenz:* CC BY-SA 3.0 *Autoren:* ? *Ursprünglicher Schöpfer:* ?

15.3 Inhaltslizenz

- Creative Commons Attribution-Share Alike 3.0