
1 Einführung

In vielen Dienstleistungsbereichen, in der Beschaffungs- und Distributionslogistik, im Handel, in Produktionsbetrieben und Materialflußsystemen haben automatische Identifikationsverfahren (Auto-ID) in den letzten Jahren große Verbreitung gefunden. Aufgabe und Ziel der Auto-ID ist die Bereitstellung von Informationen zu Personen, Tieren, Gütern und Waren.

Die weitverbreiteten Barcode-Papierstreifen, die schon vor vielen Jahren eine Revolution bei Identifikationssystemen auslösten, sind heute in zunehmenden Fällen nicht mehr ausreichend. Zwar sind Barcodes äußerst billig, ihr Engpaß ist jedoch die geringe Speicherfähigkeit sowie die Unmöglichkeit der Umprogrammierung.

Eine technisch optimale Lösung ist die Speicherung der Daten in einem Siliziumchip. Aus dem täglichen Leben ist hierzu die Chipkarte mit Kontaktfeld (Telefonchipkarte, Bankenkarte) die bekannteste Bauform eines elektronischen Datenträgers. Die mechanische Kontaktierung wie bei der Chipkarte ist jedoch in vielen Fällen unzweckmäßig. Weitaus flexibler ist eine kontaktlose Übertragung der Daten zwischen dem Datenträger und einem zugehörigen Lesegerät. Idealerweise wird auch die zum Betrieb des elektronischen Datenträgers benötigte Energie durch das Lesegerät kontaktlos übertragen. Entsprechend der eingesetzten Energie- und Datenübertragungsverfahren werden kontaktlose ID-Systeme als *RFID-Systeme* (Radio Frequency Identification) bezeichnet.

Die Anzahl an Firmen, welche sich aktiv mit der Entwicklung und Vermarktung von RFID-Systemen befassen, zeigt, daß dies ein unbedingt ernstzunehmender Markt ist. Für das Jahr 2000 wird der weltweite Gesamtumsatz für RFID-Systeme auf über 2 Milliarden US\$ geschätzt. Der *RFID-Markt* gehört derzeit zu dem am schnellsten wachsenden Teil der Funkindustrie, Handys und schnurlose Telefone mit eingeschlossen [isd].

Darüber hinaus hat sich die kontaktlose Identifikation in den letzten Jahren immer mehr zu einem eigenständigen interdisziplinären Fachgebiet entwickelt, das in keine der klassischen Schubladen mehr paßt. Es fließen hier Elemente aus den verschiedensten Branchen zusammen: HF-Technik und EMV, Halbleitertechnik, Datenschutz und Kryptographie, Telekommunikation, Fertigungstechnik und viele verwandte Fachgebiete.

Zur Einführung gibt das folgende Kapitel einen kurzen Überblick über verschiedene Auto-ID-Systeme, die als verwandte oder benachbarte Systeme zur RFID angesehen werden können.

1.1 Automatische Identifikationssysteme

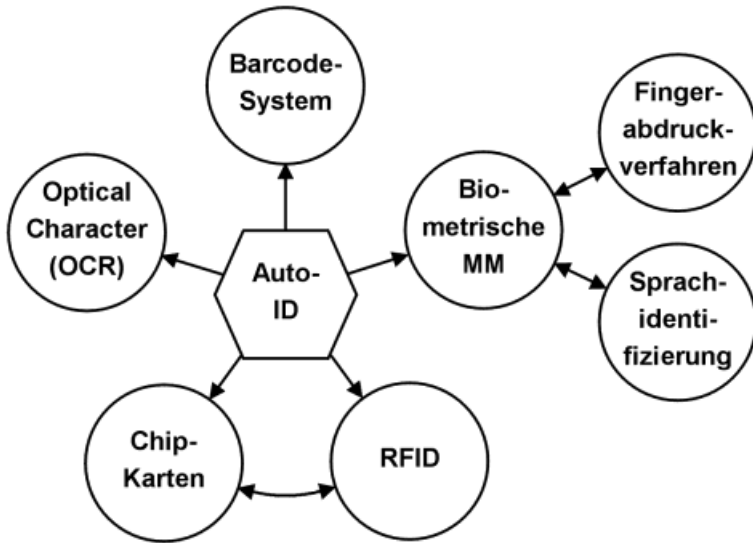


Abb. 1.1: Zusammenfassende Übersicht der wichtigsten Auto-ID Verfahren.

1.1.1 Barcode-Systeme

Barcodes (Strichcodes) haben sich in den letzten 20 Jahren immer weiter gegenüber anderen Identifikationssystemen durchsetzen können. Das Umsatzvolumen für Barcode-Systeme lag zu Beginn der 90er Jahre nach Expertenmeinung bei 3 Mrd. DM im westeuropäischen Raum [virnich].

Der Barcode ist ein Binärcode aus einem Feld von parallel angeordneten Strichen (engl. bars) und Trennlücken. Diese sind nach einem vorbestimmten Bild angeordnet und stellen Elemente von Daten dar, die auf ein zugehöriges Zeichen verweisen. Die Sequenz aus breiten und schmalen Strichen bzw. Lücken kann numerisch oder alphanumerisch interpretiert werden. Die Ablesung geschieht durch optische Laserabtastung, d. h. durch die unterschiedliche Reflexion eines Laserstrahles an den schwarzen Strichen und weißen Lücken [ident 1]. Trotz identischem physikalischem Aufbau bestehen jedoch beträchtliche Unterschiede im Codeaufbau der heutzutage etwa zehn eingesetzten Barcodes.

Der mit Abstand am weitesten verbreitete Barcode dürfte dabei der *EAN-Code* (European Article Number) sein, welcher 1976 speziell für die Belange des Lebensmittelhandels konzipiert wurde. Der EAN-Code stellt eine Weiterentwicklung des US-Amerikanischen UPC (Universal Product Code) dar, der in den USA bereits 1973 eingeführt wurde. Der UPC stellt heute eine Untermenge des EAN-Codes dar und ist daher mit diesem kompatibel [virnich].

Der EAN-Code setzt sich aus 13 Ziffern zusammen: Dem Länderkennzeichen, der bundeseinheitlichen Betriebsnummer (bbn), der Artikelnummer des Herstellers sowie einer Prüfziffer.

Länderkennzeichen	Bundeseinheitliche Betriebsnummer bbn					individuelle Artikelnummer des Herstellers					PZ
4 0	1	2	3	4	5	0	8	1	5	0	9
BRD	Fa. Musterwerk Identstrasse 1 80001 München					Schokoladenhase 100g					

Bild 1.2: Beispiel für den Aufbau eines Barcodes in EAN-Codierung (EAN = Europäische Artikelnumerierung).

Außer dem EAN-Code konnten sich in anderen Branchen vor allem die folgenden Barcodes durchsetzen:

- Code Codabar: Medizinisch-klinische Anwendungen, Bereiche mit hohen Sicherheitsanforderungen.
- Code 2/5 interleaved: Autoindustrie, Warenlager, Paletten, Schiffscontainer und Schwerindustrie.
- Code 39: Verarbeitende Industrie, Logistik, Universitäten und Büchereien.



Bild 1.3: Dieser Barcode ist auf der Rückseite dieses Buches angebracht und enthält die ISBN des Buches.

1.1.2 Optical Character Recognition

Der Einsatz von *Klarschriftlesern* (optical character recognition = OCR) begann schon in den 60er Jahren. Hierfür wurden spezielle Schrifttypen entwickelt, die durch ihre Stilisierung nicht nur von Menschen, sondern auch automatisch von Maschinen gelesen werden können. Die wichtigsten Vorteile der *OCR-Systeme* sind die hohe Informationsdichte sowie die Möglichkeit, im Notfall (oder einfach zur Kontrolle) die Daten auch visuell erfassen zu können [virnich].

Die Einsatzgebiete für OCR liegen heute in der Produktion, in Dienstleistungs- und Verwaltungsbereichen, sowie in Banken, zur Registrierung von Schecks¹. Die flächendeckende Verbreitung von OCR-Systemen wird jedoch durch ihren hohen Preis sowie durch die im Vergleich zu anderen ID-Verfahren komplizierten Lesegeräte behindert.

1.1.3 Biometrische Verfahren

Biometrie ist laut Duden-Fremdwörterbuch „die Wissenschaft von der Zählung und (Körper-)Messung an Lebewesen“. Im Zusammenhang mit Identifikationssystemen ist Biometrie der Oberbegriff für alle Verfahren, die Personen durch den Vergleich von unverwechselbaren und individuellen Körpermerkmalen identifizieren. In der Praxis sind dies Fingerabdruck- und Handabdruckverfahren, Sprachidentifizierung und seltener die Augen-Netzhaut- (bzw. auch Iris-) Identifizierung.

1.1.3.1 Sprachidentifizierung

Zur Identifikation einzelner Personen werden in neuerer Zeit spezielle Systeme zur Sprecherverifikation (Sprechererkennung) angeboten. Hierbei spricht der Benutzer in ein Mikrofon, das mit einem Computer verbunden ist. Dieser wandelt die gesprochenen Worte in digitale Signale um, die von der Identifizierungs-Software ausgewertet werden.

Ziel der Sprecherverifikation ist es, die angebliche Identität einer Person anhand ihrer Stimme zu überprüfen. Dabei werden die Sprachmerkmale der Sprechenden Person mit einem vorliegenden Referenzmuster überprüft. Bei Übereinstimmung kann dann eine Reaktion ausgelöst werden (z. B. „Tür öffnen“).

1.1.3.2 Fingerabdruckverfahren (Daktyloskopie)

In der Kriminalistik ging man bei der Identifizierung von Straftätern bereits um die Jahrhundertwende zu Fingerabdruckverfahren über. Hierbei geht es um den Vergleich der Papillaren und Hautleisten der Fingerspitzen bzw. Fingerkuppen, die man nicht nur vom Finger selbst, sondern auch von berührten Gegenständen abnehmen kann.

Bei der Personenidentifikation mittels Fingerabdruckverfahren, meist für eine Zutrittskontrolle, wird die Fingerkuppe auf ein spezielles Lesegerät gelegt. Das System berechnet aus dem eingelesenen Muster einen Datensatz und vergleicht diesen mit einem gespeicherten Referenzmuster. Moderne Fingerabdruck-ID-Systeme benötigen weniger als eine halbe Sekunde zur Erkennung und Prüfung eines Fingerabdruckes. Um gewalttätigen Betrugsversuchen vorzubeugen, wurden sogar Fingerabdruck-ID-Systeme entwickelt, welche erkennen können, ob ein lebender Finger vorgelegt wird [schmidhäusler].

¹ In der untersten Zeile von Schecks findet man persönliche Daten (Name, Kontonummer) als OCR-Schrift aufgedruckt.

1.1.4 Chipkarten

Als *Chipkarte* bezeichnet man einen elektronischen Datenspeicher, gegebenenfalls mit zusätzlicher Rechnerleistung (Mikroprozessorkarte), welcher – der besseren Handhabung wegen – in eine Plastikkarte im Kreditkartenformat eingebaut ist. Erste Chipkarten wurden bereits um 1984 als vorbezahlte Telefonchipkarten eingesetzt. Zum Betrieb werden Chipkarten in ein Lesegerät eingesteckt, das mit Kontaktfedern eine galvanische Verbindung zu den Kontaktflächen der Chipkarte herstellt. Über die Kontaktflächen wird die Chipkarte aus dem Lesegerät mit Energie und einem Takt versorgt. Die Datenübertragung zwischen dem Lesegerät und der Karte wird auf einer bidirektionalen seriellen Schnittstelle (I/O-Port) abgewickelt. Nach dem Innenleben der Chipkarten unterscheidet man zwischen zwei Grundtypen: Speicherkarte und Mikroprozessorkarte.

Einer der wichtigsten Vorteile der Chipkarte liegt darin, daß die in ihr gespeicherten Daten gegen unerwünschten (Lese-) Zugriff und Manipulation geschützt werden können. Chipkarten machen fast alle Dienstleistungen, die mit Informations- oder Geldtransaktionen verbunden sind, einfacher, sicherer und billiger. Im Jahre 1992 wurden deshalb weltweit 200 Mio. Chipkarten ausgegeben (davon 20 % alleine in Deutschland!). Im Jahre 1995 waren es bereits 600 Mio. Stück, davon 500 Mio. Speicherkarten und 100 Mio. Mikroprozessorkarten. Damit stellt der Chipkartenmarkt einen der am schnellsten wachsenden Mikroelektronik-Teilmärkte dar.

Ein Nachteil der kontaktbehafteten Chipkarten ist die Anfälligkeit der Kontakte für Abnutzung, Korrosion und Verschmutzung. Vor allem häufig benutzte Lesegeräte verursachen hohe Kosten durch Ausfall. Zudem können frei zugängliche Lesegeräte (Telefonhäuschen) nicht gegen Sabotage geschützt werden.

1.1.4.1 Speicherkarten

Bei *Speicherkarten* (Abbildung 1.4) wird über eine sequentielle Logik (State-Machine) auf den Speicher – meist ein EEPROM – zugegriffen. Hierbei sind auch einfache Sicherheitsalgorithmen, z. B. Stromverschlüsselung (Streamcipher) realisierbar. Die Funktionalität von Speicherkarten ist meist auf eine sehr spezielle Anwendung optimiert. Die Flexibilität der Anwendung ist hierfür zwar stark eingeschränkt, dafür sind Speicherkarten jedoch besonders preisgünstig. Speicherkarten werden deshalb vor allem in preissensitiven Massenanwendungen eingesetzt [rankl]. Ein Beispiel dafür ist die Versichertenkarte der gesetzlichen Krankenkassen [lemme].

1.1.4.2 Mikroprozessorkarten

Mikroprozessorkarten (Abbildung 1.5) enthalten – wie schon die Bezeichnung zum Ausdruck bringt – einen Mikroprozessor, der mit einem segmentierten Speicher (ROM-, RAM- und EEPROM-Segment) verbunden ist.

Das maskenprogrammierte ROM enthält ein Betriebssystem (Übergeordneter Programmcode) für den Mikroprozessor und wird während der Chipfabrikation aufge-

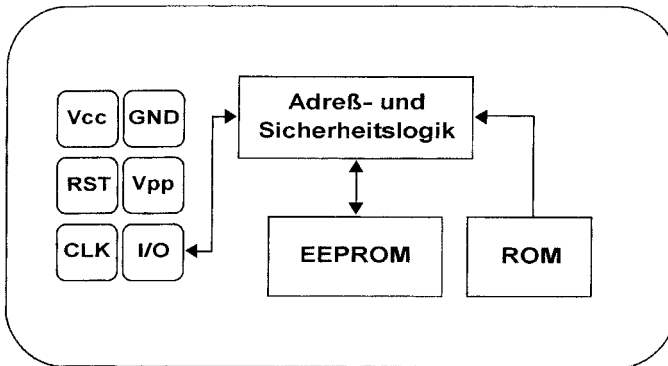


Bild 1.4: Typische Architektur einer Speicherkarte mit Sicherheitslogik.

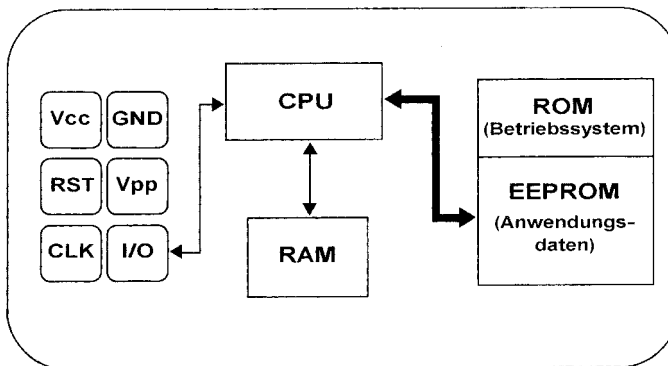


Bild 1.5: Typische Architektur einer Mikroprozessorkarte.

bracht. Der Inhalt des ROM ist herstellungsbedingt für alle Mikrochips des gleichen Produktionsloses identisch und kann auch nicht mehr überschrieben werden.

Im EEPROM des Chips befinden sich Applikationsdaten und applikationsspezifischer Programmcode. Dieser Speicherbereich kann jedoch nur unter Kontrolle des Betriebssystems beschrieben oder gelesen werden.

Das RAM ist der temporäre Arbeitsspeicher des Mikroprozessors. Die gespeicherten Daten gehen nach Abschalten der Versorgungsspannung verloren.

Mikroprozessorkarten sind sehr flexibel. Moderne Chipkartenbetriebssysteme ermöglichen es auch, unterschiedliche Anwendungen in einer einzigen Karte zu integrieren (Multiapplikation). Die applikationsspezifischen Programmteile werden dazu erst nach der Kartenproduktion in das EEPROM geladen und können über das Betriebssystem gestartet werden.

Mikroprozessorkarten werden vor allem in sicherheitssensitiven Anwendungen eingesetzt. Ein Beispiel hierfür sind Chipkarten für GSM-Handys oder die neuen EC-Karten (electronic cash). Die Programmiermöglichkeit der Mikroprozessorkarten ermöglicht außerdem die schnelle Anpassung an neue Applikationen [rankl].

1.1.5 RFID-Systeme

RFID-Systeme sind den oben beschriebenen Chipkarten eng verwandt. Auch hier werden die Daten auf einem elektronischen Datenträger – dem Transponder – gespeichert. Die Energieversorgung des Datenträgers sowie der Datenaustausch zwischen Datenträger und Lesegerät erfolgt jedoch nicht durch galvanisches Kontaktieren, sondern unter Verwendung magnetischer oder elektromagnetischer Felder. Die technischen Verfahren hierzu wurden aus der Funk- und Radartechnik übernommen. Die Bezeichnung RFID steht deshalb für Radio-Frequency-Identification, also Identifikation durch Radiowellen.

Aufgrund zahlreicher Vorteile der RFID-Systeme gegenüber den anderen Identifikationssystemen beginnen RFID-Systeme neue Massenmärkte zu erobern. Ein Beispiel hierfür ist der Einsatz kontaktloser Chipkarten als Ticket für den öffentlichen Nahverkehr.

1.2 Vergleich verschiedener ID-Systeme

Ein Vergleich zwischen den oben aufgeführten Identifikationssystemen (Tabelle 1.1) zeigt die Schwächen und Stärken von RFID zu anderen Systemen. Auch hier zeigt sich die enge Verwandtschaft zwischen kontaktbehafteter Chipkarte und RFID-Systemen, jedoch werden bei letzteren alle Nachteile im Zusammenhang mit der stör anfälligen Kontaktierung (Sabotage, Verschmutzung, nur eine Steckrichtung, zeitaufwendiges Einstecken usw.) vermieden.

Tabelle 1.1: Der Vergleich verschiedener RFID-Systeme zeigt deren Vor- und Nachteile.

Parameter \ System:	Barcode	OCR	Sprechererkennung	Biometrie	Chipkarte	RFID-Systeme
Typische Datenmenge/ Byte:	1 ~ 100	1 ~ 100	–	–	16 ~ 64k	16 ~ 64k
Datendichte	gering	gering	hoch	hoch	sehr hoch	sehr hoch
Maschinenlesbarkeit	gut	gut	aufwendig	aufwendig	gut	gut
Lesbarkeit durch Personen	bedingt	einfach	einfach	schwer	unmöglich	unmöglich

(Fortsetzung nächste Seite)

Tabelle 1.1 (Fortsetzung): Der Vergleich verschiedener RFID-Systeme zeigt deren Vor- und Nachteile.

System: Parameter:	Barcode	OCR	Sprecherer- kennung	Biometrie	Chipkarte	RFID- Systeme
Einfluß von Schmutz/ Nässe	sehr stark	sehr stark	–	–	möglich (Kontakte)	kein Einfluß
Einfluß von (opt.) Abdeckung	totaler Ausfall	totaler Ausfall	–	möglich	–	kein Einfluß
Einfluß von Richtung und Lage	gering	gering	–	–	eine Steck- richtung	kein Einfluß
Abnutzung/Verschleiß	bedingt	bedingt	–	–	Kontakte	kein Einfluß
Anschaffungskosten/ Leseelektronik	sehr gering	mittel	sehr hoch	sehr hoch	gering	mittel
Betriebskosten (z.B. Drucker)	gering	gering	keine	keine	mittel (Kontakte)	keine
unbefugtes Kopieren/ Ändern	leicht	leicht	möglich ^{*)} (Tonband)	unmöglich	unmöglich	unmöglich
Lesegeschwindigkeit (incl. Handhabung des Datenträgers)	gering ~ 4 s	gering ~ 3 s	sehr gering > 5 s	sehr gering > 5 ... 10 s	gering ~ 4 s	sehr schnell ~ 0,5 s
Maximale Entfernung zwischen Datenträger und Lesegerät	0 ... 50 cm	< 1 cm (Scanner)	0 ... 50 cm	direkter Kontakt ^{**)}	direkter Kontakt	0 ... 5 m, Mikrowelle

*) Die Gefahr des „Replay“ kann durch Auswahl eines zu sprechenden Textes mit einem Zufallsgenerator verringert werden, da nicht mehr im voraus bekannt ist, welcher Text gesprochen werden muß.

***) Dies gilt nur für Fingerabdruck-ID. Bei Augen-Netzhaut- oder Iris-Auswertung ist ein direkter Kontakt nicht nötig bzw. möglich.

1.3 Bestandteile eines RFID-Systems

Ein *RFID-System* besteht immer aus zwei Komponenten:

- dem *Transponder*, der an die zu identifizierenden Objekte angebracht wird,
- dem Erfassungs- oder *Lesegerät*², das je nach Ausführung und eingesetzter Technologie als Lese- oder Schreib/Lese-Einheit erhältlich ist.

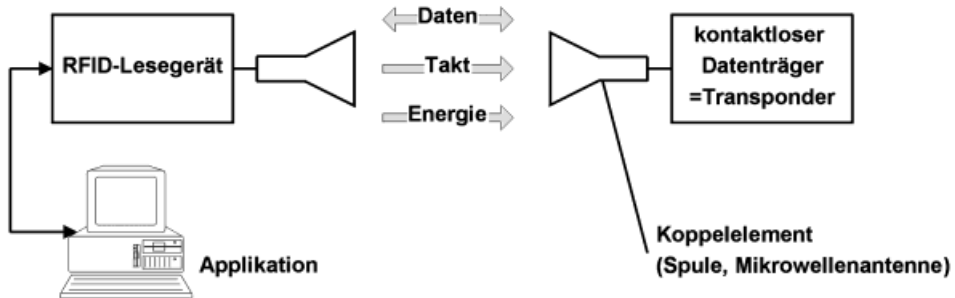


Bild 1.6: Lesegerät und Transponder sind die Grundbestandteile jedes RFID-Systems.

Ein Lesegerät beinhaltet typischerweise ein Hochfrequenzmodul (Sender und Empfänger), eine Kontrolleinheit sowie ein Koppellement zum Transponder. Daneben sind viele Lesegeräte mit einer zusätzlichen Schnittstelle (RS 232, RS 485, ...) ausgestattet, um die erhaltenen Daten an ein anderes System (PC, Automatensteuerung, ...) weiterzuleiten.



Bild 1.7: RFID-Lesegerät und kontaktlose Chipkarte im praktischen Einsatz. (Foto: Kaba Security Locking Systems AG, CH-Wetzikon)

² In diesem Buch wird das Erfassungsgerät – der üblichen umgangssprachlichen Verwendung entsprechend – immer als **Lesegerät** bezeichnet, unabhängig davon, ob Daten damit nur gelesen oder auch geschrieben werden.

Der Transponder, der den eigentlichen *Datenträger* eines RFID-Systems darstellt, besteht üblicherweise aus einem Koppellement sowie aus einem elektronischen *Mikrochip*. Außerhalb des Ansprechbereichs eines Lesegerätes verhält sich der Transponder, der in der Regel keine eigene Spannungsversorgung (Batterie) besitzt, vollkommen passiv. Erst innerhalb des Ansprechbereichs eines Lesegerätes wird der Transponder aktiviert. Die zum Betrieb des Transponders benötigte Energie wird ebenso wie Takt und Daten durch die Koppelunit (kontaktlos) zum Transponder übertragen.

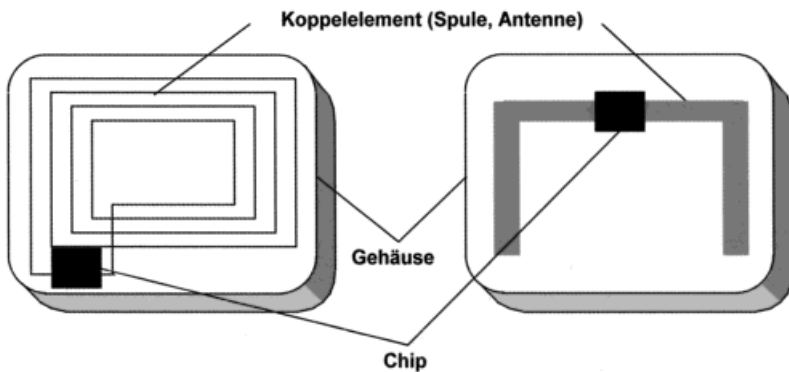


Bild 1.8: Prinzipieller Aufbau des RFID-Datenträgers, des Transponders.
Links: induktiv gekoppelter Transponder mit Antennenspule,
rechts: Mikrowellen-Transponder mit Dipolantenne.