

## Die RFID- und NFC-Technologie - eine kurze Einführung

Diese Einführung soll dem Leser in Form eines Frage-Antwort-Katalogs einige Grundkenntnisse zum Einsatz von RFID-Datenträgern (RFID = **R**adio **F**requency **I**Dentification; übersetzt: Radio-Frequenz-Identifikation) für die Zutrittssteuerung sowie die damit verbundenen Applikationen wie Zeit- und Betriebsdatenerfassung (BDE), Kantinen- und Food-Automaten-Abrechnung usw. vermitteln. Der Schwerpunkt liegt auf dem Einsatz sogenannter passiver Systeme, bei denen der RFID-Chip keine eigene Energieversorgung hat, sondern seine Energie aus dem Feld der Schreib-/Leseeinheit bezieht.

Andere Applikationen werden der Vollständigkeit wegen erwähnt, aber nicht detailliert besprochen. Dazu zählen auch die Warenkettierung, Sicherung und Verfolgung von Gepäck oder Paketsendungen. In Zukunft werden mehr RFID-Chips bei diesen Anwendungen als in der Zutrittssteuerung eingesetzt werden, aber die Anforderungen an die dabei eingesetzten RFID-Chips sind meist einfacher.

Ergänzende Informationen und Anwendungsgebiete der RFID-Technik sind im BHE-Praxis-Ratgeber Zutrittssteuerung ausführlich erklärt.

### Was ist RFID und welche Technologien gibt es zu beachten?

RFID-Systeme bestehen grundsätzlich aus zwei Komponenten, nämlich den mobilen Identmedien bzw. Datenträgern und dem stationären, meist integrierten Leser (z.B. in ZK-Gerät/Terminal) oder für einige Anwendungen auch tragbaren Leser, der die vom Chip gesendeten Daten berührungslos empfängt, aufbereitet und weiterleitet. Bei dem RFID-Lesesystem handelt es sich meist um ein Schreib-/Lesemodul mit Antenne, das der Einfachheit nachfolgend nur als Leser bezeichnet wird.

Für den Datenträger mit integriertem RFID-Chip und Antenne und seiner „Kunststoffhülle“, ist auch die Bezeichnung Transponder gebräuchlich. Der RFID-Chip ist also in einem Trägerobjekt integriert (s. Abb.), beispielsweise in einem Klebetikett (auch als Tag bezeichnet), einer Plastikkarte (Mitarbeiterausweis) oder in einem Schlüsselanhänger. Nachfolgend wird nur noch der Begriff „Transponder“ verwendet.



Abb. 1 Bauformen von RF-Identmitteln

Dabei unterscheidet man aktive Systeme (der Transponder hat eine eigene Stromversorgung) und passive Systeme (der Transponder nimmt seine Betriebsenergie aus dem Feld des Lesers/ ZK-Gerätes oder des Terminals).

**RFID-Systeme nutzen unterschiedliche Frequenzen vom Langwellen- bis zum Mikrowellenbereich, die sich auch auf die Lesedistanz auswirken. Die von der Transponder-Bauart, der verwendeten Transponder-Spulenlänge und Größe der stationären Antenne und der Sendeleistung des RFID-Lesers abhängigen Leseabstände reichen von Berührung (Touch), wenigen Zentimetern (Proximity) bis zu mehreren Metern (Longrange).**

Ursprünglich wurde die Technik im Frequenzbereich 100 - 150 kHz, meist 125 kHz betrieben. Heute erfolgt dies meist noch in alten und „einfacheren“ Anwendungen bei denen Datensicherungs- und Verschlüsselungsmaßnahmen für Speicherung und Übertragung meist nur in Ansätzen vorhanden sind. Aus Sicherheitsgründen werden diese Frequenzbereiche nicht mehr empfohlen.

Heutzutage wird meist der 13,56 MHz-Bereich genutzt, für den auch Normen bestehen. Hier sind verschiedene Systeme mit gut strukturierten Sicherungsmaßnahmen verfügbar. Ausgehend von den zuständigen Normen wird wie folgt unterschieden:

- Proximity coupling Chipkarten nach ISO/IEC 14443 für Lesereichweiten bis ca. 10 cm, gängig für Zeit und Zutritt.
- Vicinity coupling Chipkarten nach ISO/IEC 15693 für Lesereichweiten bis ca. 1 m. Einige Transponder bieten dies auch an, und speziell bei Ausweisen für Ski-Gebiete finden diese wegen der besseren Reichweite durchaus zunehmend Verwendung.

Neben der Möglichkeit, auf einem RFID-Chip mehrere Applikationen zu betreiben und diese auch gegeneinander abschotten zu können, gibt es differenzierte Lese- und auch Schreibschutzmaßnahmen. Meist beruhen sie auf Passwörtern, also auf dem Wissen des Zugriffsberechtigten der Chipdaten. Es gibt aber auch zumindest ein System, bei dem statt des Wissens der Besitz verwendet wird, die Zugriffsberechtigung also über Autorisierungsmittel gesteuert werden kann.

Die bereits erstellten Normen und ein Großteil der anstehenden Normungsvorhaben beziehen sich auf diesen Frequenzbereich, schließen teilweise aber auch andere Frequenzbereiche ein. Auch die NFC-Technik nutzt vorwiegend diesen Frequenzbereich. Weitere Systeme verwenden die Frequenzbänder um 433 MHz, 868 MHz, 2,45 GHz oder 5,6 GHz. Hier kommen vornehmlich aktive oder halbaktive RFID-Chips zum Einsatz.

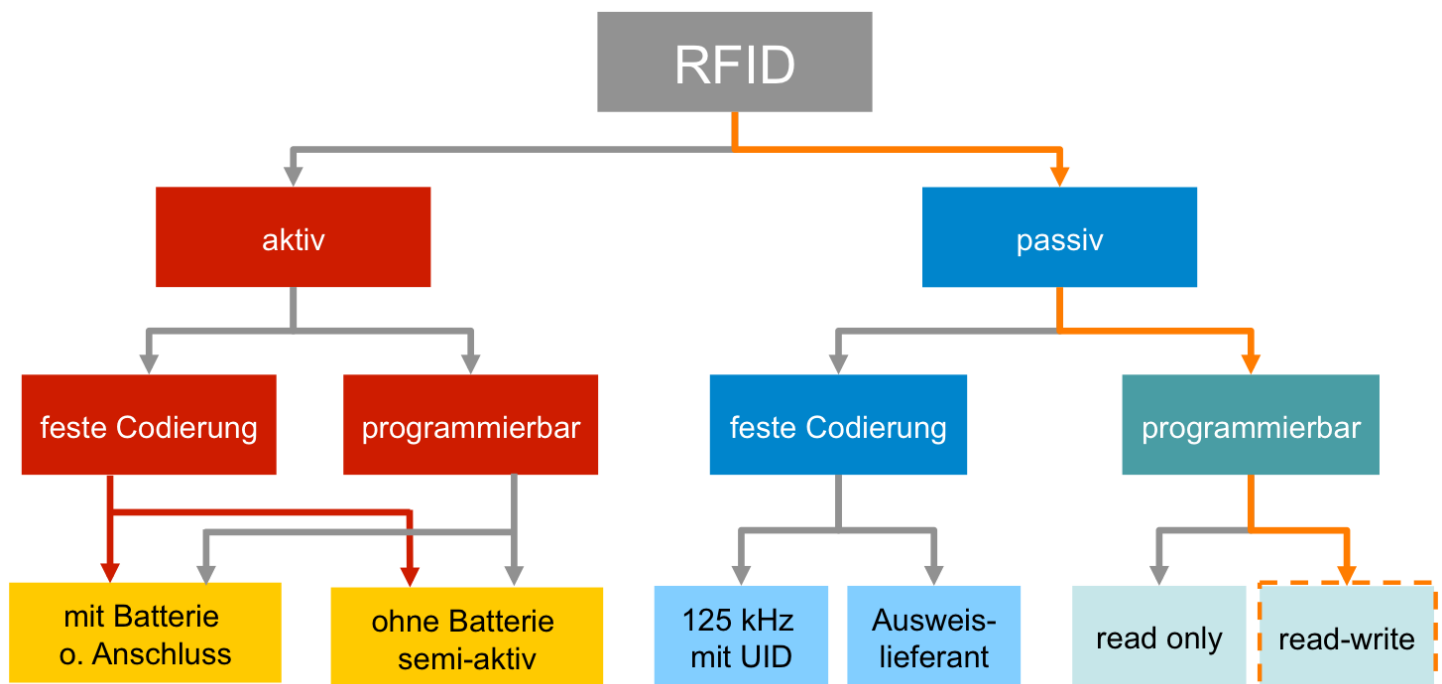


Abb. 2 Unterteilung der RFID-Systeme in aktive und passive Verfahren

Für die Unterteilung der RFID-Systeme für die Zutrittssteuerung kann die in Abb. 2 aufgezeigte Unterteilung herangezogen werden. Bei den aktiven Systemen unterscheidet man zwischen wirklich „aktiven“ Transpondern, bei denen die RFID-Chips ihre eigene Batterie oder einen Versorgungsspannungsanschluss haben, und den „semi-aktiven“ Transpondern, die zwar teils auch eine Batterie besitzen, deren Energie aber nur zum Erhalt und nicht zum Senden der Daten genutzt wird. Diese „semi-aktiven“ Transponder modulieren und reflektieren die vom Schreib-/Lesegerät kommenden Nachrichten („backscattering-mode“). Daher ist quasi eine Art „Sichtkontakt“ erforderlich, d.h. die beiden Antennen von Leser und Transponder müssen möglichst parallel zueinander ausgerichtet sein. Der Einsatz erfolgt bspw. zur Erkennung von Kraftfahrzeugen.

## RFID-Lesedistanzen

Beim Einsatz von passiven RFID-Systemen mit kleinen bzw. integrierten Antennen, wie sie in Zutrittslesern, Terminals oder mechatronischen Türbeschlägen angeboten werden, beträgt die Lesedistanz <10 cm. Mit Einzelantennen sind Distanzen von ca. 0,5 m und mit Antennen in Gate-Anordnung von ca. 1 m erreichbar. Neben der eingeschränkten max. Sendeleistung der Lesestationen sind dafür zwei technische Begrenzungen maßgebend, nämlich einerseits die Übertragung der Hilfsenergie und andererseits die Detektion der Feldschwächung durch die Schreib-/Lesestation.

Bei aktiven RFID-Systemen ist zu berücksichtigen, dass eine reproduzierbare Ausrichtung von Ausweis bzw. Transponder und Lesegerät zueinander vorausgesetzt werden kann, z.B. bei Toren oder Schranken für Geländeeinfahrten. Ihre Reichweite beträgt ca. 5 - 10 m, weshalb sie oft auch als Longrange-Reader bezeichnet werden.

Aktive Systeme wickeln mit ihren Schreib-/Leseinheiten praktisch einen „echten“ Funkverkehr ab, daher überbrücken sie auch Distanzen bis zu ca. 30 m (Beispiel: Transponder am Autoschlüssel). Es muss aber darauf geachtet werden, dass die Transponder sich nicht im Empfangsbereich mehrerer Schreib-/Lesestationen befinden, wenn das System nicht über eine Adressierung der gewünschten Station verfügt. In diesem Zusammenhang ist zu berücksichtigen, dass es bei der gleichzeitigen Kommunikation von mehreren ID-Mitteln mit einem Leser zu Problemen in der Zutrittssteuerung kommen kann.

***Für die meisten Anwendungen zur Personenidentifikation reichen Lesedistanzen von < 10 cm aus, dies gilt insbesondere für Zutrittsleser oder Zeiterfassungs- und mechatronische Tür-Terminals. Diese Lesedistanzen werden auch in der Norm ISO 14443 definiert.***

## Longrange- und Hands-free-RFID-Systeme

RFID-Leser für große Lesedistanzen eignen sich besonders, wenn Personen mehrmals täglich mit Warentransport Zutrittsstellen passieren müssen. Die im Zutrittsbereich verdeckt eingebaute Antenne des Lesesystems liest den in der Kleidung oder Tasche befindlichen Ausweis berührungslos. Soweit der Ausweis zur optischen Kontrolle offen getragen werden muss, kann er mit einem Clip an der Kleidung befestigt werden. Die großen Lesedistanzen erfordern jedoch Leser mit leistungsfähigeren Antennen. Es gibt Systeme, bei denen man mit dem Transponder die Türen auch aus Entfernungen von mehreren Metern öffnen kann.

Bei der Planung eines Zutritts-/Zufahrtssteuerungssystems mit Longrange-RFID-Systemen muss zuerst festgelegt werden, welche maximalen Erkennungsreichweiten erforderlich sind und mit welcher Geschwindigkeit z.B. Fahrzeuge das Antennenfeld passieren können. Die Reichweite hat Einfluss auf die Antennenart und -größe sowie den damit verbundenen Preis. Außerdem sollten die Antennen bei der Zufahrtssteuerung möglichst nicht auffällig sein, um von vornherein Manipulations- oder Sabotageakte auszuschließen.

Für Entfernungen zwischen 40 Zentimetern und 10 Metern werden entweder aktive Transponder oder batteriebetriebene Verstärker (Booster) zum Einstecken einer RFID-Karte verwendet. Diese Identmedien lassen sich z. B. in Lastwagen oder Busse ein- bzw. anbauen. Nähert sich ein Fahrer mit seinem Lkw einer zufahrtsgesicherten Lagerhalle, braucht er sein Fahrzeug nicht zu verlassen, denn es wird durch die codierte Ausweisnummer des Identmediums eindeutig identifiziert.

Bei der Installation von sogenannten Handsfree-Systemen mit ca. 30 - 50 cm Wirkdistanz muss beachtet werden, dass sich das Antennenfeld symmetrisch nach vorne und nach hinten ausweitet. Erfolgt beim hinteren Feld eine Dämpfung durch magnetische Materialien, wird automatisch auch das vordere Feld kleiner. Deshalb nimmt die Lesedistanz von Handsfree-Antennen z.B. vor eisenbewehrten Betonwänden stark ab.

In der Zutrittssteuerung haben die passiven, im Feld lesbaren und beschreibbaren 13,56 MHz-RFID-Transponder mit kryptierter Datenübertragung auf der Luftstrecke und mit mehreren gegeneinander abgrenzbaren Applikationsfeldern die größte Bedeutung. Daher beziehen sich die weiteren Ausführungen auf die gemäß ISO DIN 14443 genormten RFID-Systeme.

## RFID-Historie

Vorläufer der aktiven RFID-Systeme war ein Gerät zur Freund-Feind-Erkennung, mit dem die USA ihre Kampfflugzeuge im 2. Weltkrieg austatteten.

Den 1948 von Stockman veröffentlichten Aufsatz „Communications by Means of Reflected Power“ kann man als eigentliche Geburtsstunde der RFID bezeichnen, auch wenn mangels integrierter Schaltungen noch keine größeren Anwendungen möglich waren.

Die Erfindung des integrierten Schaltkreises 1958 von Jack Kilby ermöglichte ab ca. 1960 die Herstellung von kleinen Transpondern. In den 60er Jahren des letzten Jahrhunderts kamen die 1-bit-Systeme, z.B. zur elektronischen Warensicherung gegen Ladendiebstahl auf. In den 70er und Anfang der 80er Jahren folgten weitere, wenn auch publizistisch wenig bekannte Anwendungen. Bedingt durch die geringe Verbreitung und die damit verbundenen hohen Chip-Preise sowie eine noch nicht ausgereifte Technologie, wurde diese Technik nur in Spezialanwendungen genutzt. In den 1970er Jahren wurden RFID-Systeme in der Landwirtschaft zur Kennzeichnung von Haus-/ Nutztieren eingesetzt. Kurz danach kamen weitere Anwendungen hinzu, wie die Nutzung in der Containerlogistik oder bei der automatischen Fertigung.

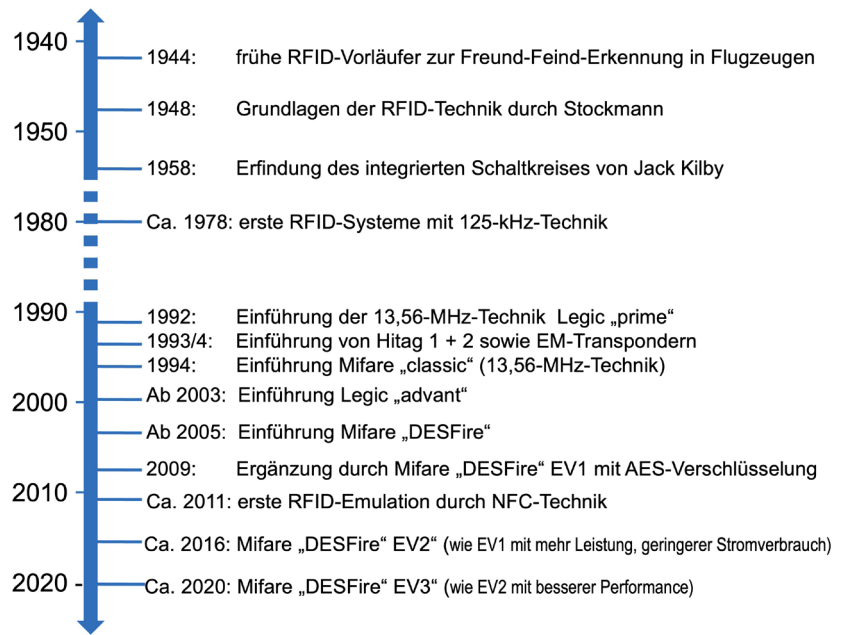


Abb. 3 Historie der RFID-Transpondersysteme

Eine der ersten publizistisch bekannten Aktionen war ab 1988 eine Impfkation bei sardischen Hunden und deren Kennzeichnung mit RFID in Form von glasgekapselten Transpondern. Ansonsten wurde in den 80er Jahren die Entwicklung der RFID-Systeme in den Vereinigten Staaten und einigen skandinavischen Ländern soweit vorangetrieben, dass diese im Straßenverkehr für Mautsysteme eingesetzt werden konnten. Die Chip-Entwicklung wurde für weitere Anwendungen fortgesetzt z. B. für Wegfahrsperren, Skipässe, Tankkarten und als Mitarbeiterausweis. In dieser Zeit setzte auch die Nutzung von RFID zur Personenidentifikation bei Zeit-, Kantinen- und Zutrittssystemen ein.

Als 1992 das erste 13,56 MHz-RFID-System vorgestellt wurde, begann der Durchbruch dieser Technik auf breiter Basis. Dieser ist einerseits auf die größere speicherbare Datenmenge, andererseits auch auf die komfortable Handhabung (kein Einstecken oder Durchziehen des Ausweises, sondern einfaches, fast ungerichtetes Vorhalten vor die Leserantenne) und die guten Sicherheitsmaßnahmen zurückzuführen.

Neben dem Einsatz in der Zutrittssteuerung und den damit oft verbundenen organisatorischen Applikationen begegnen uns RFID-Chipkarten im Alltag immer häufiger, angefangen bei dem elektronischen Personalausweis, Führerschein, EC- oder Versicherungskarte, Schüler- oder Studentenausweis, bis hin zu Kunden- und Bonuskarten. Auf all solchen Karten werden je nach Anwendung spezifische Informationen auf dem RFID-Chip gespeichert.

## Wo kommt RFID zum Einsatz?

Das klassische Einsatzgebiet von RFID liegt in der Zutrittssteuerung und verbunden damit in anderen betrieblichen, kartengesteuerten Anwendungen, wie in der Zeit- und Kantinendatenerfassung sowie der Zugangs- und Zugriffssteuerung zu Rechnern, Maschinen und Automaten (z.B. Drucker). Da RFID-Chips nicht nur ausgelesen, sondern auch beschrieben werden können, bieten sich hier neue funktionale Möglichkeiten. So können z.B. Zutrittsberechtigungen ausgewertet und zusätzlich die letzten Buchungen auf dem Ausweis eingetragen werden. Diese Möglichkeiten werden insbesondere in Anlagen genutzt, die mit online-Terminals und mechatronischen offline-Schließzylindern/ -Türbeschlägen ausgestattet sind.

Werden in Unternehmen weitere organisatorische Anwendungen wie Kantine und Food-Automaten mit RFID-Ausweisen bedient, ist dabei meist ein Geldbetrag auf dem Ausweis gespeichert, der mit jedem Warenbezug angepasst wird. Damit eignen sich Transponder auch sehr gut für Kantinen- und Hotellösungen.

	Frequenz	Distanz	Übertragungsgeschwindigkeit	Anwendung
Langwelle (LF)	30 ... 300 kHz 125 kHz	0,5 m passiv	gering	Tiermarkierung, einfache Zutrittsleser, robuste Technik, auf metallischen und wasserhaltigen Unterlagen gut lesbar.
Kurzwellen (HF/RF)	3 ... 30 MHz <b>13,56 MHz</b>	0,5 m passiv	hoch	<b>Zutrittssteuerung</b> , sehr preisgünstige Tags, auf metallischen und wasserhaltigen Unterlagen schwer lesbar.
Dezimeterwelle (UHF)	0,3 ... 3 GHz	3 ... 8 m passiv	hoch	Logistik, Weitbereichsleser, Hand-free-Aufgaben, auf metallischen und wasserhaltigen Unterlagen sehr schlecht lesbar.
Mikrowelle (SHF)	> 3 GHz	5 ... 10 m aktiv	sehr hoch	Mautsysteme, teuer, auf metallischen und wasserhaltigen Unterlagen nicht lesbar.

Abb. 4 Anwendungen nach Frequenzbereich

Zunehmend erfolgt auch der Einsatz beim asset tracking, also der Verfolgung und Ortung von Gegenständen. Dazu zählen z.B. die Abfertigung des Fluggepäcks und die Verfolgung und Sicherung bei Waren- und Paketbeförderung. Das gilt auch für die Anwendungen, die statt der Warenauszeichnung mit Barcodes RFID-Aufkleber (Labels) verwenden. Hier spielt vor allen Dingen die schnellere Erfassung vieler Transponder in einem RFID-Feld (Pulk-Auslesung durch anti-collision-Eigenschaften der Chips) und die dadurch mögliche „permanente Inventur“ eine große Rolle, die auf Dauer Einsparpotentiale freisetzt.

Zu erwähnen ist noch die Kennzeichnung von Wäsche, insbesondere Mietwäsche, mit RFID-Chips. Diese halten meist die „Lebensgeschichte“ des Wäschestücks fest (ein Beweis, dass RFID Transponder als Etiketten auch den Kochvorgang unbeschadet überstehen). Zu beachten ist aber, dass bei all diesen Anwendungen eine Multi-Applikationsfähigkeit nicht erforderlich ist. Auch die Ansprüche an die Datensicherheit sind anders gelagert. Daher sind die speziell für diese Anwendungen entwickelten RFID-Chips für die Zutrittssteuerung nur in Ausnahmefällen einzusetzen.

Allen Anwendungen kommt zugute, dass RFID-Chips auch über etwas größere Entfernung ohne direkte Sichtverbindung ausgelesen werden können. Auch mehrere gleichzeitig im Feld befindliche RFID-Chips können einzeln erfasst werden, was z.B. bei Warenauszeichnung und Gepäckverfolgung ein wichtiger Aspekt ist.

### Wie funktionieren passive RFID-Systeme?

Passive RFID-Systeme nutzen gleichzeitig die Eigenschaften des eisenlosen Transformators („Lufttransformator“ zur kabellosen Stromübertragung) für die Energieübertragung und der drahtlosen Kommunikation für die Datenübertragung.

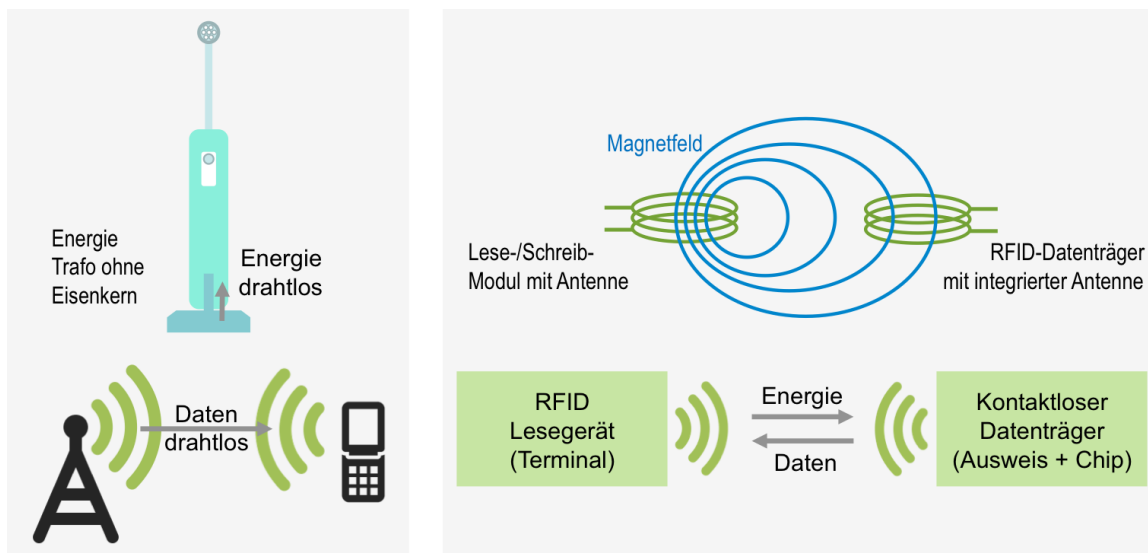


Abb. 4 Prinzip passiver RFID-Systeme

Nun kann ein passiver Transponder jedoch mangels eigener Energieversorgung keine drahtlose Kommunikation im eigentlichen Sinne ausführen, sondern kann nur das Feld der Schreib-/Lesestation durch Einschalten einer zusätzlichen Belastung modulieren. Diese Belastung demoduliert die Schreib-/Lesestation per Fußpunktwidestand in ihrem Antennenschwingkreis. Der darf deshalb keine allzu hohe Güte besitzen, da er sonst die Lastmodulation nicht bemerkt.

Außerdem haben passive RFID-Chips keine eigene Spannungsversorgung. Sie beziehen ihre Energie statt dessen aus dem Kommunikationsfeld ihrer Schreib-/Lesestationen und erreichen deshalb in der Praxis - abhängig von der Übertragungsfrequenz und Antennengröße - nur eine begrenzte Lese-Reichweite.

Für die klassische Zutrittssteuerung und Zeiterfassung reichen Lesedistanzen von < 10 cm aus, bei denen diese Gesichtspunkte noch eine untergeordnete Rolle spielen. Zu beachten ist aber, dass viele ISO 14443-kompatiblen Chips auch keine größere Wirkdistanz zulassen, also für sogenannte handsfree-Anwendungen nicht infrage kommen.

### **Eigenschaften von RFID im Umfeld der Zutrittssteuerung?**

Zutrittssteuerung und Zeiterfassung benötigen

- langlebige, belastbare und gut handhabbare Identifikationsmittel
- einfaches, sicheres und schnelles Auslesen der ID-Mittel am Buchungsterminal
- hohe Auslesesicherheit und kurze Behandlungszeiten pro Buchung, damit hohen Durchsatz pro Terminal/Tür
- genormte Verfahren nach ISO/IEC 14443 bieten Multiapplikationsfähigkeit für weitere organisatorische Anwendungen und Verschlüsselung (hohe Sicherheit und Schutz vor Hacking)

Diese zusätzlich bereits geschilderten Eigenschaften wie Lesen und Schreiben im Feld, mehrere Applikationen pro RFID-Chip sowie weitgehende Umweltfreundlichkeit der (passiven) Transponder (z.B. Ausweise oder Schlüsselanhänger) kommen den neuen Forderungen an Zutritts- und Zeiterfassungssystemen entgegen. Diese RFID-Mittel sind also für das Erkennen der Nutzer in diesen Anlagen ein wesentlicher Baustein, zumal - abhängig von der RFID-Technologie und Speicherkapazität - auch biometrische Templates auf ihnen gespeichert werden können.

### **Risiken, Sicherheit und Akzeptanz beim Einsatz von RFID bei der Zutrittssteuerung**

Im Sinne der Fälschbarkeit der ID-Mittel ist RFID den herkömmlichen Techniken wie z.B. Magnetstreifen weit überlegen, die Fälschung bzw. das Nachmachen von Ausweisen ist meist an die Kenntnis von Passwörtern oder an den Besitz von Autorisierungsmitteln gebunden, die nicht frei verfügbar sind. Auch wenn in den letzten Jahren einige spektakuläre Veröffentlichungen über das Entschlüsseln und Fälschen von RFID-Chips mit 125 kHz und der ersten Generation der 13,56 MHz-RFID-Chips erfolgten, ist der Aufwand für die Überwindung der Sicherheitsmaßnahmen erheblich höher als bei den herkömmlichen Ausweistechiken.

Diese „Fälschungen“ haben dazu geführt, dass neue RFID-Chips mit besseren, auch vom Anbieter und Betreiber auswählbaren Sicherheitsmaßnahmen entwickelt wurden, deren verschlüsselte Kryptoalgorithmen für die Datenspeicherung und insbesondere die Datenübertragung allgemein als langzeitsicher und auf lange Sicht unknackbar gelten.

Da diese technischen Features schnelle und sichere Schreib-/Leseverfahren zwischen Karte und Terminal voraussetzen, wurde die zuvor übliche und veraltete 125 kHz-Technologie durch die 13,56 MHz-Technik abgelöst. Diese Verfahren orientieren sich an der eigens dafür erstellten Norm ISO/IEC 14443 1-4. Um die Forderung nach Schutz gegen Fernkopieren und Abhören zu erfüllen, wird hierbei auf der Luftstrecke (zwischen Karte und Leser) verschlüsselte Kommunikation eingesetzt. Dieser „Kopierschutz“ verhindert ein Duplizieren von Berechtigungen und macht ein Mitlesen von über die Luftstrecke zwischen Karte und Beschlag ausgetauschten Daten unmöglich.

Bereits in frühen Ausgaben der technischen Richtlinien des BSI wurden ausschließlich RFID-Medien nach ISO/IEC 14443, mit Secure Access Module (SAM) und AES 128 Verschlüsselungsverfahren oder gleichwertigen offenen Verfahren vorgegeben, z.B. Mifare Desfire EV3.

**Akzeptanzprobleme** sind praktisch nicht vorhanden, da das CE-Zeichen die Gewähr bietet, dass hinsichtlich Sicherheit und Strahlenschutz alle Regeln eingehalten werden. Fragen des Datenschutzes sind bei geschlossenen Systemen (alle Systeme, die im Umfeld und Einwirkungsbereich eines Betreibers liegen und deren Benutzer mehr oder weniger vorherzubestimmen sind) bereits in der Betriebsvereinbarung behandelt worden. Das gilt damit praktisch für alle Zutrittsanlagen und die damit verbundenen organisatorischen Anwendungen.

### Verbreitung von RFID- und NFC/Bluetooth-Systemen

Neuanlagen entstehen fast nur noch auf der Basis von RFID. Sogar kontaktbehaftete Mikrocontroller, die bisher noch ein höheres Rechenvermögen aufweisen, werden durch RFID oder bei Bankkarten durch NFC (Near Field Communication), ein auf der RFID-Technik basierender internationaler Übertragungsstandard, ersetzt, weil kontaktbehaftete Ausweise und ihre Leseeinheiten der starken Belastung durch viele Buchungen nicht immer gewachsen sind. RFID begegnet uns täglich - in der Bankkarte, in Waren, in Pässen, Führerscheinen, dem elektronischen Personal- und Mitarbeiterausweis. Neben klassischen RFID-Lesern kann das Auslesen der Chips mittlerweile mit jedem aktuellen Smartphone erfolgen. Die Möglichkeiten und Anwendungsbereiche für NFC sind vielfältig. Für einige Anwendungen, insbesondere dem mobilen Zutritt (Mobile Access) können NFC- oder Bluetooth fähige Smartphones eine gute Alternative zum RFID-Ausweis darstellen.



Dafür existieren etliche Apps unter Android und iOS. Gerade jüngere Mitarbeiter begrüßen es, wenn sie nicht immer einen separaten Ausweis mit sich führen müssen, sondern sich mit dem Smartphone identifizieren können, da sie diesen nicht so leicht zuhause vergessen.

### Was ist bei der Auswahl eines Identträgers zu beachten?

Der Einführungsaufwand oder die Auswahl eines neuen RFID-Identträgers wird leider unterschätzt. Eine falsche Entscheidung kann zu vielen Einschränkungen und zu erhöhten Nachfolgekosten führen. Auch ist der Speicherbedarf für zukünftig geplante Aufgaben, z.B. als Medium für die Speicherung eines biometrischen Templates (z.B. vom Fingerprint), bei der Verifikation (Ausweis plus biometrisches Merkmal) zu berücksichtigen. Häufig wird vom Verkäufer die Sicherheit einer bestimmten RFID-Codierung herausgestellt, dabei aber verschwiegen, dass diese nicht genormt (z.B. ISO 14443) und nicht dem aktuellen Stand der Technik entsprechen. Durch die Kombination mehrerer Codierungen auf einem Ausweis, werden die Eigenschaften, Funktionsweisen und Anwendungsmöglichkeiten dieser verschiedenen Technologien vereint. Beispielsweise kann ein RFID-Ausweis noch mit einem QR-Code und/oder einem kontaktbehafteten Chip ergänzt werden.

### Kosten/Nutzen-Betrachtung

Der Anbieter muss zunächst einmal, ähnlich wie bei der Einführung neuer Techniken, mit Investitionen für die Ablösung alter ID-Systeme, Kauf und Montage neuer RFID-Leser sowie teilweise auch Erwerb von Lizenzen rechnen. Der Anlagenbetreiber muss bei Ablösung von Altsystemen (z.B. bisher 125 kHz) einen etwas höheren Preis für die Transponder in Kauf nehmen, insbesondere wenn Kombiausweise (z.B. 125 kHz mit 13,56 MHz) eingeführt werden. Gegenüber kontaktbehafteten ID-Systemen führt die meist höhere Standfestigkeit und damit längere Lebensdauer der RFID-Mittel letztendlich zu geringeren Betriebskosten.

Terminals mit RFID-Modulen sind mittlerweile preisgleich oder sogar günstiger als solche mit Lesern für herkömmliche kontaktbehaftete Codiertechniken. Insgesamt ist also eine Anlage mit RFID-Technik in den Gesamtkosten gleichzusetzen mit einer Anlage mit herkömmlichen ID-Mitteln. Die Multiapplikationsfähigkeit moderner RFID-Ausweise erlaubt ihre Nutzung für mehrere Anwendungen. So sind sie neben der Zutrittssteuerung und Zeiterfassung z. B. auch für Follow-Printing oder die Kantinendatenerfassung nach dem Debitverfahren (Verkauf gegen Abbuchung des Geldbetrages vom Konto auf dem Ausweis) sehr gut einsetzbar.



Die bereits geschilderten Vorzüge von RFID gegenüber herkömmlichen Techniken können damit praktisch ohne Aufpreis genutzt werden. Das RFID-Informationen-Portal (<http://www.rfid-basis.de/kosten.html>) gibt zu RFID und den dazu erforderlichen Investitionskosten ergänzende Informationen.

## Ausblick

RFID ist bereits so weit ausgereift, dass wir zwar eine stetige technische und anwendungsorientierte Weiterentwicklung erwarten dürfen, aber keine grundsätzlichen Quantensprünge. Ein Zukunftsszenario wird also in erster Linie die Ideen darstellen, die für Zutritt und Zeit mehr oder weniger unabhängig von RFID entwickelt werden.

Allerdings könnten sich die Bestrebungen, mit Biometrie abgesicherte Personalausweise/Pässe mit RFID-Chips zu versehen, so auswirken, dass nur die Ausweiskennung oder in Verbindung damit auch die biometrischen Daten auch in „privaten“ Anlagen für Zeit und Zutritt genutzt werden. Dem steht aber die heutige Gesetzeslage zumindest in Deutschland entgegen.

Eine Weiterentwicklung im Bereich der RFID-Technik ist die bereits erwähnte Nachfeldkommunikation „NFC“, die i.d.R. in Zusammenhang mit Zahlungskarten und Smartphones verwendet wird. Hierbei wird das Smartphone zum Träger der ID-Kennung seines Besitzers. Erteilung und Änderung von Zutrittsrechten sind sehr einfach und schnell „per Anruf“ zu erledigen. Näheres zu diesem Thema kann man im BHE-Praxis-Ratgeber Zutrittssteuerung finden.

## Wo kann man mehr über RFID erfahren?

In den Internet-Suchmaschinen findet man riesige Trefferfelder für „RFID“. Erst eine thematische Eingrenzung führt zu überschaubaren Trefferlisten. Auch die Webseiten der Anbieter bieten neben den Produkten oft Grundlagenwissen zu RFID. Weiterführende Informationen findet man z.B. unter

<https://de.wikipedia.org/wiki/RFID>

<https://www.bsi.bund.de> (Stichwort RFID)

<https://www.aim-d.de/?s=RFID>

Zusätzlich kann z.B. das nachfolgend aufgeführte Standardwerk empfohlen werden:

Finkenzeller, Klaus, 2015 8. Auflage, 09/2023

RFID-Handbuch, Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC

Carl Hanser Verlag München, 8. Auflage, 2023 ISBN 978-3-446-43943-6 978-3-446-44885-8

<https://www.hanser-elibrary.com/isbn/9783446439436>

<https://www.hanser-fachbuch.de/fachbuch/artikel/9783446448858>