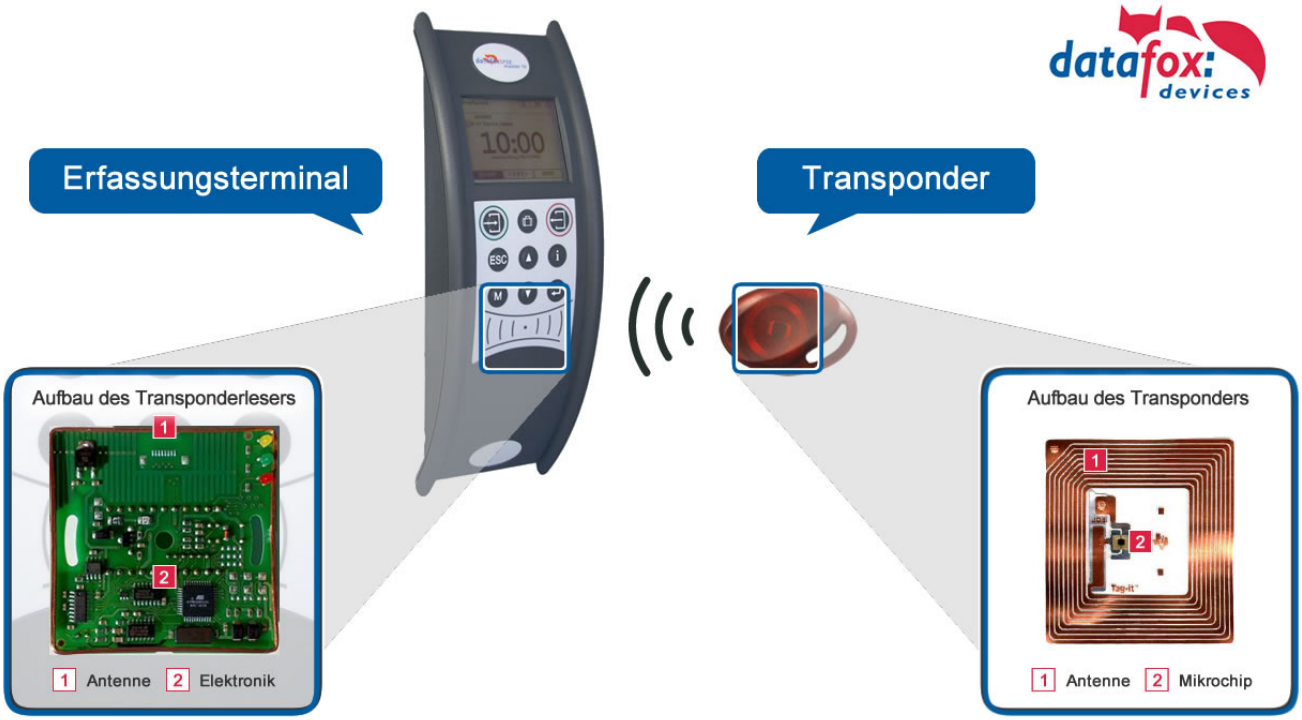
Datafox GmbH • Dermbacher Straße 12-14 • D-36419 Geisa • www.datafox.de

RFID-Leseverfahren

Übersicht zum Verstehen und Auswählen

1. RFID Technik zum Verstehen:

1.1 Anwendungs-Prinzip



1.2 RFID-Technologien

Im Bereich der kontaktlosen Identifikation (RFID = Radio Frequency IDentification) unterteilt man Transponder in zwei Typen:

Passive Transponder

Unter passiven Transpondern versteht man Systeme, die die zur Kommunikation und zur Abarbeitung interner Prozesse benötigte Energie ausschließlich aus dem Feld der Schreib-/Leseeinheit beziehen.
Passive Transponder benötigen keine eigene Stromversorgung, können aber nur auf kurze Distanzen arbeiten. Bekannteste Bauart ist die Radio Frequency Identification RFID. Typische Anwendungen: Identifizierung von Objekten, Haustierregistrierungs-Chips oder Chipkarten für ein Zugangs-Kontrollsystem. Ein aktiver Sensor (in Verbindung mit dem Computer) liest und decodiert die Daten, die der passive Transponder sendet.
Da keine eigene Stromversorgung benötigt wird, ergeben sich sehr geringe Abmessungen, die den Einbau von passiven Transpondern in kleine Gehäuse überhaupt erst möglich machen. Somit können Gegenstände oder Personen einfach und unkompliziert mit einem elektronisch lesbaren Datenträger ausgestattet werden.

Aktive Transponder

Aktive Systeme verfügen über eine eigene Energieversorgung. Entweder haben sie eine eingebaute Batterie oder werden an ein externes Stromnetz angeschlossen. Dadurch sind nicht nur größere Kommunikationsreichweiten möglich, auch die Verwaltung größerer Datenspeicher bzw. der Betrieb integrierter Sensorik wird realisierbar. Einfache aktive Transponder werden zum Beispiel bei der Identifizierung von Personen oder Gegenständen verwendet:

1.3 Übliche Bauformen von Transpondern

ISO Card

Schlüsselanhänger

Coin Tag

Disc Tag

Disc PET

Glastag

Smart Label 13,56 MHz

2. Transponder-Ausweise sicher lesen und identifizieren

Die Sicherheit einer Erfassungslösung und damit die Qualität der Erfassung sind das Wichtigste für die Anwendungen im Bereich Zeiterfassung und Zutrittskontrolle, als auch Objektkennzeichnung.

Datafox bietet über die Terminal-Ausstattung und Einrichtung per Datafox-Studio einige Möglichkeiten an, um verschiedene Sicherheitsstufen zu realisieren.

Kriterien für die Bewertung der Sicherheit:

a.) Eindeutigkeit des Ausweises
b.) Verhinderung der Erzeugung von Duplikaten
c.) Ausschluss-Möglichkeit von entwendeten oder verloren gegangenen Ausweisen.

2.1 Seriennummer bzw. Unikatsnummer (UID) des Ausweises + Listenprüfung

Die UID wird von dem Transponder gelesen. Der ermittelte Wert wird zwischengespeichert.
Auf dem Terminal befindet sich eine Liste mit allen berechtigten UID´s. Der ermittelte Wert wird mit den Listeneinträgen verglichen. Nur wenn eine Übereinstimmung mit einem Eintrage in der Liste vorliegt, wird die Buchung gespeichert oder die Erfassung fortgesetzt.

a.) Eindeutigkeit	Der Hersteller stellt die Eindeutigkeit der UID sicher. Alle uns bekannten RFID-Ausweise verfügen über eine Seriennummer (UID).
b.) Duplikatsverhinderung	Die Seriennummer kann nicht verändert werden. Eine Einschränkung der Sicherheit liegt generell vor, wenn nicht alle Stellen der Seriennummer verwendet werden. Dann gibt es automatisch Duplikate von Ausweisen. Beispiel von der 13 stelligen Nummer von Unique werden nur 8 Stellen verwendet. Dann sind z.B. alle Ausweise mit xxxxx12345678 nicht zu unterscheiden. Somit sind die Ausweise 1000012345678 und 2000012345678 bei dem Lesen nicht zu unterscheiden. Es gibt dann also weltweit 99.999 Duplikate. Daher bitte immer die volle Stellenanzahl verwenden!
c.) Ausschluss	Nur Seriennummern, in der hinterlegten Liste werden angenommen. Bei Ausweisverlust muss nur eine angepasste Liste in die Terminals übertragen werden.
Sicherheit	**sehr hoch**

2.2 Segmentwert des Ausweises + Listenprüfung

Oft ist es erwünscht, dass die Ausweisnummer identisch mit der Personalnummer ist. Dann kann die UID nicht verwendet werden, sondern es muss ein definiertes Segment mit der gewünschten Nummer programmiert werden.
Der programmierte Segmentwert wird von dem Transponder gelesen. Dieser Wert wird zwischengespeichert. Auf dem Terminal befindet sich eine Liste mit allen berechtigten Ausweisnummern. Der ermittelte Wert wird mit den Listeneinträgen verglichen. Nur wenn eine Übereinstimmung stattfindet, wird die Buchung gespeichert oder die Erfassung fortgesetzt.

a.) Eindeutigkeit	Die Eindeutigkeit kann nicht sichergestellt werden. Es können zum einen in einer Anlage mehre Ausweise die gleich Nummer programmiert bekommen oder auch Überschneidungen mit anderen Anlagen vorliegen.
b.) Duplikatsverhinderung	Ausweise können von unberechtigten Personen ausgelesen werden und dann Duplikate erzeugt werden.
c.) Ausschluss	Nur programmierte Nummern die in der hinterlegten Liste vorkommen werden angenommen. Bei Ausweisverlust muss nur eine angepasste Liste in die Terminals übertragen werden.
Sicherheit	**sehr niedrig**

2.3 Segmentwert des Ausweises + Passwort

Der Transponder-Ausweis wird bei der Programmierung zusätzlich mit einem Kommunikations-Passwort versehen. Diese Ausweise lassen sich dann nur noch auslesen, wenn der Leser vorher das Passwort sendet. Dieses Passwort wird auch über das Setup des Terminals hinterlegt, so dass die Terminals die Ausweise lesen können. Transponder mit falschem Passwort werden vom Terminal ignoriert.

a.) Eindeutigkeit	Die Eindeutigkeit kann nicht sichergestellt werden. Es können mehre Ausweise die gleich Nummer programmiert bekommen. Die Überschneidung mit anderen Anlagen wird durch das Passwort weitestgehend ausgeschlossen. Bei der Vergabe der Passwörter gibt es 2 verschiedene Ansätze. 1.) Der Anwender vergibt das Passwort selbst. Hier können zufällig Überschneidungen zu anderen Anlagen entstehen. Die Wahrscheinlichkeit ist gering, weil die Passwörter sehr lang sind. Verfahren sind z.B. Mifare oder Hitag. 2.) Die Passwörter werden zentral vom Hersteller vergeben. Hier sind Überschneidungen ausgeschlossen. Verfahren sind z.B. Legic oder SimonsVoss. Legic basiert auf einer IAM-Karte (Taufkarte). Auf dieser befindet sich die Basis-Codierung mit der jedes Gerät des Systems (Leser oder Terminal) initialisiert (getauft) sein muss. Das Löschen und Beschreiben von Ausweisen (Transponder) ist ebenso nur mit dieser IAM-Karte möglich.
b.) Duplikatsverhinderung	Dadurch, dass die Ausweise durch das Passwort vor unberechtigtem Auslesen gesichert sind, kann das Erzeugen von Duplikaten weitestgehend ausgeschlossen werden.
c.) Ausschluss	Einzelne Ausweise können nicht ohne weiteres ausgeschlossen werden. Damit können unberechtigte Personen mit verloren gegangenen oder gestohlenen Ausweisen buchen. Eine Möglichkeit ist eine Negativ-Liste = ausgeschlossene Ausweise im Terminal. Besser setzt man aber gleich eine Positiv-Liste = zugelassene Ausweise ein.
Sicherheit	**mittel**

2.4 Segmentwert des Ausweises + Passwort + Listenprüfung

Der Transponder-Ausweis wird bei der Programmierung zusätzlich mit einem Kommunikations-Passwort versehen. Diese Ausweise lassen sich dann nur noch auslesen, wenn der Leser vorher das Passwort sendet. Dieses Passwort wird auch über das Setup des Terminals hinterlegt, so dass die Terminals die Ausweise lesen können. Transponder mit falschem Passwort werden vom Terminal ignoriert.
Der ermittelte Wert wird zusätzlich mit den Listeneinträgen verglichen. Nur wenn eine Übereinstimmung vorliegt, wird die Buchung gespeichert oder die Erfassung fortgesetzt.

a.) Eindeutigkeit	Siehe 2.3
b.) Duplikatsverhinderung	Siehe 2.3
c.) Ausschluss	Nur programmierte Nummern die in der hinterlegten Liste vorkommen werden angenommen. Bei Ausweisverlust muss nur eine angepasste Liste in die Terminals übertragen werden.
Sicherheit	**hoch**

Ergänzende Hinweise:

- Die Verwendung von Ausweisen kann in Verbindung mit Biometrie/Fingerprint noch sicherer gemacht werden. Bei der Verifikation wird das von dem Ausweisbesitzer hinterlegte Template mit einem einzulesenden verglichen. Nur bei Übereinstimmung der Templates werden die Buchungen angenommen.
- Datafox bietet Bedruckung von Ausweisen an.
- Datafox bietet Programmierung von Segmenten an.

3. Von Datafox unterstützte RFID - Verfahren:

Der Umfang der Informationen, welche auf einem Transponder gespeichert werden können, ist abhängig von dem verwendeten RFID-Typ und dem zugehörigen Leseverfahren.
Einfache Verfahren unterstützen nur eine einmalige Seriennummer die sogenannte ID. Diese ID kann nur gelesen werden.
Komplexe Verfahren bieten verschiedene Segmente und Sektoren, die z.T. auch passwortgeschützt sind, an. Diese Segmente können gelesen und beschrieben werden. Damit können neben der Ausweis-Nr. z.B. auch Zusatz-Informationen, wie Status, Abteilungszugehörigkeit, persönliche Daten wie Blutgruppe, Zutrittsberechtigungen, Geldkonten, etc. auf dem RFID-Medium abgelegt werden.

Nachfolgend die Übersicht der von Datafox unterstützten RFID-Verfahren.

Leser	Leseverfahren	Frequenz	Tech. Daten	Beschreibung
TSR32	Unique / EM4102	125 kHz	Nur Seriennummer	Unique / EM4102 ist ein reines Leseverfahren. Die Nummer der Karte ist eine weltweit eindeutige ID und wird in allen erdenklichen Bereichen eingesetzt. Auf der Karte ist eine 64bit Information gespeichert, wobei für die eindeutige ID nur 40bit verwendet werden. Die übrigen Bits dienen u.a. einer Prüfsumme.
	Hitag1	125 kHz	64 Segmente je 4 Byte 0 = Seriennummer 1 - 31 = Passwörter, 32 bis 63 = frei verfügbar	Hitag1 ist in 16 Blöcken á 4 Segmente organisiert. Jedes Segment ist 32 Bit lang. Die Blocknummern 4 bis 7 können wahlweise Passwort geschützt (Secret) oder frei verwendet werden (Public). Die frei verfügbaren Segmente können z. B. für das Speichern einer Firmenkennung, der Kartennummer, Geldkonto für Kantinen, etc. verwendet werden.
	Hitag2	125 kHz	8 Segmente je 4 Byte: 0 = Seriennummer 1 bis 3 = Passwörter, 4 bis 8 frei verfügbar.	Hitag2 ist in 8 Segmenten organisiert. Jedes Segment ist 32Bit lang. Die frei verfügbaren Segmente können z. B. für das Speichern einer Firmenkennung, der Kartennummer, Geldkonto für Kantinen, etc. verwendet werden.
	HitagS	125 kHz	Seriennummer (Segment 0) und je nach Ausführung Segmente 1 - 63 frei verfügbar	Bei diesem Verfahren unterscheidet man zwischen „HitagS H32“, „HitagS H56“ und „HitagS H48“. HitagS H32 bedeutet, dass dieser Transponder nur einen 32 Bit Wert, die Seriennummer der Karte, besitzt (siehe Unique). Das H56 gibt an, dass der Transponder 8 Register für je einen 32 BitWert, zusammen 256 Bit, besitzt (siehe Hitag2). Mit H48 wird angegeben, dass der Transponder 64 Register zu je 32 Bit, zusammen 2048 Bit, besitzt (siehe Hitag1). Die frei verfügbaren Segmente können z. B. für das Speichern einer Firmenkennung, der Kartennummer, Geldkonto für Kantinen, etc. verwendet werden.
	Titan / EM4450 (Hewi)	125 kHz	34 Segmente: 0 bis 2 = Passwörter 3 bis 31 = frei verfügbar 32 bis 33 Serial/Device ID	Titan (EM4450) ist in 34 Segmenten organisiert. Jedes Segment ist 32 Bit lang. Die Seriennummer befindet sich in Segment 32. Die frei verfügbaren Segmente können z. B. für das Speichern einer Firmenkennung, der Kartennummer, Geldkonto für Kantinen, etc. verwendet werden.
	DOM Hitag1	125 kHz	Seriennummer lesen	Hitag1 mit Cryptoprozessor, deshalb ist nur die Seriennummer lesbar
	DOM Hitag2	125 kHz	Seriennummer lesen	Hitag1 mit Cryptoprozessor, deshalb ist nur die Seriennummer lesbar
ProxPoint® Plus OEM Module 4065	HID ProxPoint	125 kHz	Nur Ausweisnummer	Facility Code und Card Number oder nur Cardnumber je nach Format des Ausweises von 26Bit-Format bis 84Bit-Format Korrekte Nummerermittlung nur bei veröffentlichten Format H10301, H10302 und H10304. Bei allen anderen nicht veröffentlichten Formaten wird der binäre Wert incl. Paritätsbit in Hexadezimalformat geliefert.

Datafox RFID - Leseverfahren

IClass OEM 50	HID IClass	13,56 MHz	Nur Ausweisnummer	Facility Code und Card Number oder nur Cardnumber je nach Format des Ausweises von 26Bit-Format bis 84Bit-Format Korrekte Nummerermittlung nur bei veröffentlichten Format H10301, H10302 und H10304. Bei allen anderen nicht veröffentlichten Formaten wird der binäre Wert incl. Paritätsbit in Hexadezimalformat geliefert.
Mifare Easy	Mifare Classic	13,56 MHz	Seriennummer und 16 Sektoren mit je einem Schreib- und Lesepasswort Als 1Kbyte und 4Kbyte Variante verfügbar	Mifare Classic 1k ist in 16 Sektoren á 4 Blöcken zu je 16 Byte organisiert. Mifare Classic 4k ist in 32 Sektoren á 4 Blöcken zu je 16 Byte und in 8Sektoren a 16Blöcke zu je 16Byte organisiert. Jeder 4. Block dient der Administration der Daten auf dem Transponder und enthält aufgeteilt in einen Key-A und einen Key-B, je 6 Byte lang ein Passwort für Schreib und Leserechte sowie die „Access Condition“ in der die Sektorformate definiert sind. Je nach Anwendung können alle Blöcke eines Sektors im Default-Format vorliegen (d.h. Key A ist der Lese- und Schreibschutzschlüssel) oder im Data bzw. Value-Format, wobei Key A das Lesekennwort und Key B der Masterschlüssel für Lesen und Schreiben ist. Vorteilhaft sind die hohe Geschwindigkeit und das große Speichervolumen wodurch sich dieser Transponder sehr gut für die Biometrie eignet.
	Mifare Desfire	13,56 MHz	Nur Seriennummer	Daten liegen in einem Dateisystem verschlüsselt vor. Zugriff über Applikationen und Datei.
	Mifare Ultralight	13,56 MHz	Nur Seriennummer	Mifare Ultralight besteht aus 16 Seiten a 4Byte und hat eine 7 Byte Seriennummer
TWN3 Multi-ISO (verfügbar ab ca. Anfang 2012)	Mifare Classic	13,56 MHz	Seriennummer und 16 Sektoren mit je einem Schreib- und Lesepasswort Als 1Kbyte und 4Kbyte Variante verfügbar	Mifare Classic 1k ist in 16 Sektoren á 4 Blöcken zu je 16 Byte organisiert. Mifare Classic 4k ist in 32 Sektoren á 4 Blöcken zu je 16 Byte und in 8Sektoren a 16Blöcke zu je 16Byte organisiert. Jeder 4. Block dient der Administration der Daten auf dem Transponder und enthält aufgeteilt in einen Key-A und einen Key-B, je 6 Byte lang ein Passwort für Schreib und Leserechte sowie die „Access Condition“ in der die Sektorformate definiert sind. Je nach Anwendung können alle Blöcke eines Sektors im Default-Format vorliegen (d.h. Key A ist der Lese- und Schreibschutzschlüssel) oder im Data bzw. Value-Format, wobei Key A das Lesekennwort und Key B der Masterschlüssel für Lesen und Schreiben ist. Vorteilhaft sind die hohe Geschwindigkeit und das große Speichervolumen wodurch sich dieser Transponder sehr gut für die Biometrie eignet.
	Mifare Desfire	13,56 MHz	Seriennummer und Dateisystem mit Schreib- und Lesepasswort Als 2, 4, 8Kbyte und 72Kbyte Variante verfügbar	Daten liegen in einem Dateisystem verschlüsselt vor. Zugriff über Applikationen und Dateien. Je nach Ausweistyp können von 2kByte bis zu 72kByte, 28 Applikationen mit je bis zu 13 Schlüsseln/Passwörtern und pro Applikation 32 Dateien möglich sein. Mifare Desfire ist eines der sichersten Transponderverfahren weltweit.
	Mifare Ultralight	13,56 MHz	Nur Seriennummer	Mifare Ultralight hat 64Byte Kapazität besteht aus 16 Seiten a 4Byte und hat eine 7 Byte Seriennummer
	Mifare Ultralight C	13,56 MHz	Nur Seriennummer	Mifare Ultralight C hat 192Byte Kapazität besteht aus 48 Seiten a 4Byte und hat eine 7 Byte Seriennummer. Benutzerdaten können in einem Bereich von 35 Seiten (148Byte) gelesen und geschrieben werden. Der Mifare Ultralight C hat einen Cryptoprozessor der eine 3DES Verschlüsselung benutzt.
	Mifare Plus SL1 und SL2	13,56 MHz	Seriennummer und 16 Sektoren mit je einem Schreib- und Lesepasswort (Nur Sicherheitsstufe 1 und 2)	MifarePlus ist strukturell wie ein Mifare Classic nur das er in verschiedenen Sicherheitsstufen verfügbar ist. Sicherheitsstufe 1 4Byte UID (kann mehrfach vorkommen) und 6Byte Keys Sicherheitsstufe 2 7Byte UID (weltweit einmalig) und 16Byte Keys

	Mifare Plus SL3	13,56 MHz	Nur Seriennummer (Sicherheitsstufe 3)	7Byte UID (weltweit einmalig) / Zugriff nur mit SAM(Crypto-Prozessor-Unit) über APDUs(direkte Tranponderbefehle)
	I Code SLI, SLI-S, SLI-L	13,56 MHz	Serienummer und 8 – 64 Blöcke zu je 4Byte	UID Mode 40Bit UID Block Mode (4Byte pro Block) 8, 28 , 32, 40 und 64 Blöcke je nach Ausweischipsatz
	ICODE UID	13,56 MHz	Seriennummer und 12Byte Daten	Der Speicher hat eine Kapazität von 96 Bit / 12 Byte. UID (40Bit) USER DATA (192Bits) CRC16 of user data (16Bit) Destroy Code(24Bit) Die UID(Seriennummer) kann nicht geändert werden.
	ICODE EPC	13,56 MHz	Nur 12Byte Daten	Der Speicher hat eine Kapazität von 96 Bit / 12 Byte. USER DATA (136Bits) CRC16 of user data (16Bit) Destroy Code(24Bit) Der Ausweis verfügt über keine UID(Seriennummer).
	MyD	13,56 MHz	Seriennummer und 96 – 1024 Blöcke zu je 8Byte	MyD ist ein Transponder der Firma Infineon und kann bis zu 10Kbyte (1024Blöcke) haben. Diese Ausweise besitzen eine Seriennummer und einen Datenbereich. Ähnlich wie bei Mifare ist der Block 0 die Seriennummer.
Primo110	Legic Prime	13,56 MHz	Seriennummer und 256 oder 1024Byte	Legic kommt nur im deutschsprachigen Raum zum Einsatz. Es gibt segmentierte und nicht segmentierte Speicherkarten. Bei einer nicht segmentierten Karte werden die Daten mittels einer Positions- und Längenangabe gelesen. Bei segmentierten Karten muss zu einer Längenangabe zusätzlich das Segment angegeben werden, von dem die Daten gelesen werden sollen.
Primo130	Legic Prime	13,56 MHz	Seriennummer und 256 oder 1024Byte	Legic kommt nur im deutschsprachigen Raum zum Einsatz. Es gibt segmentierte und nicht segmentierte Speicherkarten. Bei einer nicht segmentierten Karte werden die Daten mittels einer Positions- und Längenangabe gelesen. Bei segmentierten Karten muss zu einer Längenangabe zusätzlich das Segment angegeben werden, von dem die Daten gelesen werden sollen.
	Legic Advant	13,56 MHz	Es werden beide Advanttypen unterstützt ISO14443 und ISO15693 Seriennummer und 128 bis 4096Byte	Es gibt segmentierte und nicht segmentierte Speicherkarten. Bei einer nicht segmentierten Karte werden die Daten mittels einer Positions- und Längenangabe gelesen. Bei segmentierten Karten muss zu einer Längenangabe zusätzlich das Segment angegeben werden, von dem die Daten gelesen werden sollen. Es kann ein Segment auch über einen Suchstring gewählt werden.
i-Button	i-Button	Kontaktbe-haftetes Verfahren	feste 15 stellige Seriennummer	Hierbei handelt es sich um ein Kontakt-Leseverfahren. Der i-Button besitzt nur eine Seriennummer, welche bei Kontakt mit dem Transponder gelesen wird.
Smart Relais	SimonsVoss	25 kHz	10 stellige Nummer 1 bis 5 = Anlagennummer 6 bis 10 = Ausweis	SimonsVoss ist ein aktives berührungsloses Leseverfahren. Jede Karte besitzt einen eindeutigen 10 stelligen Dezimalcode. Die Stelle 1-5 ist die Firmenkennung, Stelle 6-10 ist die Ausweisnummer. Es können bis zu 8000 Ausweise mit Profil auf einem SmartRelais gespeichert werden.
XS070	Nedap	125kHz	Nur Seriennummer	Nedap ist ein reines Leseverfahren, die Ausweise liefern nur eine Nummer.

Nähere Informationen zu den unterstützen Optionen innerhalb eines Leseverfahren finden Sie in dem Handbuch des jeweiligen Geräts. Die Handbücher stehen Ihnen als PDF-Dokument auf unserer Homepage zum Download zur Verfügung.

Sollte das von Ihnen benötigte Leseverfahren nicht in der Übersicht aufgeführt sein, dann sprechen sie uns einfach an. Wir erweitern die möglichen Leseverfahren permanent und auch für Kundenprojekte.