

VDA

**Grundlagen
zum RFID-Einsatz
in der Automobilindustrie**

5500

Mit der vorliegenden unverbindlichen VDA-Empfehlung werden folgende Zielsetzungen verbunden:

- Standardisierung von technischen Anforderungen an passive RFID-Transponder
- Definition von Grundsätzen zum Aufbau von RFID-spezifischen Datenstrukturen
- Zusätzliche optische Kennzeichnung von RFID-gekennzeichneten Objekten
- Definition von Grundsätzen für den RFID-spezifischen Datenaustausch

Version 1.2 vom Juni 2015
(ersetzt Version 1.1 vom April 2015)

Auto ID Projektgruppe

Herausgeber: Verband der Automobilindustrie
Behrenstrasse 35
10117 Berlin
Telefon 030/897842-0
Telefax 030/897842-606
Internet: www.vda.de

Copyright
Nachdruck und jede sonstige Form
der Vervielfältigung ist nur mit
Angabe der Quelle gestattet.

VDA

Verband der
Automobilindustrie

Haftungsausschluss

Die VDA-Empfehlungen sind frei verfügbar und haben lediglich empfehlenden Charakter. VDA-Empfehlungen bieten unternehmensübergreifende Orientierung, berücksichtigen jedoch keine fallspezifischen Rahmenbedingungen. Sie bedürfen der weiterführenden Auslegung und Interpretation prozessbeteiligter Geschäftspartner.

VDA-Empfehlungen berücksichtigen den zum Zeitpunkt der jeweiligen Ausgabe herrschenden Standardisierungsgrad und Stand der Technik. Durch das Anwenden der VDA-Empfehlungen entzieht sich niemand der Verantwortung für sein eigenes Handeln. Jeder handelt insoweit auf eigene Gefahr. Eine Haftung des VDA und derjenigen, die an den VDA-Empfehlungen beteiligt sind, ist ausgeschlossen.

Nutzer werden gebeten, auf Mängel und ausstehende Abstimmungsinhalte hinzuweisen, und sich über den VDA am fortlaufenden Standardisierungsprozess zu beteiligen.

Änderungsverzeichnis

Datum	Aktion	Beschreibung
15.06.2015	Ergänzung	AFI 0x90 für die Identifizierung von Fahrzeugen ergänzt (Abschnitt 7.1)

Inhaltsverzeichnis

	Haftungsausschluss.....	2
1	Einleitung.....	7
2	Technische Anforderungen an RFID-Transponder.....	9
	2.1 Funktionsweise passiver RFID-Transponder	9
	2.2 Luftschnittstelle und Frequenzbereiche.....	10
	2.3 Aufbau und Größe der Speicherbereiche.....	11
	2.4 Transponderauswahl, Positionierung und Befestigung	12
	2.5 Rahmenbedingungen für den Transpondereinsatz	14
	2.6 Zusätzliche Umwelteinflüsse und Lebensdauer	15
3	Allg. Grundsätze beim Aufbau von RFID-Datenstrukturen	17
	3.1 Nutzung von Speicherbereichen	17
	3.2 Auswahl von Datenstandards (ISO/IEC, GS1)	17
	3.3 Beschreiben des Speicherbereichs MB 01 (ISO/IEC)	17
	3.4 Beschreiben des Speicherbereichs MB 11 (ISO/IEC)	21
	3.5 Umsetzung des Schreib-/Leseschutzes und Kill-Befehl	24
4	Zusätzliche optische Kennzeichnung von Objekten	28
	4.1 Verwendung von Klarschrift und 1D/2D-Codes (ISO/IEC)	28
	4.2 Verwendung des RFID-Symbols	29
5	Unternehmensinterner und -übergreifender Datenaustausch.....	30
	5.1 Datenaustausch zwischen RFID-Geräten und IT-Systemen	30
	5.2 Unternehmensübergreifender Datenaustausch.....	32
6	Referenzen.....	33
7	Anhang.....	34
	7.1 Application Family Identifiers (ISO/IEC)	34
	7.2 Kodierungstabelle (6-bit Encoding)	35
	7.3 Kodierungsbeispiel MB 01 (ISO 17367)	36

Abbildungsverzeichnis

Abbildung 1: RFID-Potentiale in der Automobilindustrie	7
Abbildung 2: Aufbau eines RFID-Transponders	9
Abbildung 3: RFID-Speicherbereiche nach ISO/IEC 18000-63	12
Abbildung 4: Exemplarische RFID-Anwendungen	14
Abbildung 5: Aufbau der Speicherbank MB 01	18
Abbildung 6: Aufbau von Steuerinformationen in MB 11	21
Abbildung 7: Transponderzustände gemäß ISO/IEC 18000-63.....	25
Abbildung 8: RFID-Symbol	29
Abbildung 9: Datenübertragung von der RFID-Applikation an IT-Backends.....	30

Tabellenverzeichnis

Tabelle 1: Weltweit freigegebene RFID-Frequenzbänder (UHF)	10
Tabelle 2: Transpondertypen und geeignete Oberflächenmaterialien	13
Tabelle 3: Vor- und Nachteile von Befestigungsarten.....	13
Tabelle 4: Umwelteinflüsse und deren Ausprägungen	15
Tabelle 5: Kodierung des Speicherbereichs MB 01	20
Tabelle 6: Kodierung des Speicherbereichs MB 11 ≤ 1024 Bit Nutzdaten	23
Tabelle 7: Aufbau der Steuerinformation für MB 11 > 1024 Bit Nutzdaten	24
Tabelle 8: Lock-Optionen für RFID-Transponder gemäß ISO/IEC 18000-63	26
Tabelle 9: Exemplarische Codierung von 1D/2D-Codes	28
Tabelle 10: Exemplarischer Aufbau von 1D/2D-Datenstrukturen	29
Tabelle 11: Grundlegende Informationen von AutoID-Ereignissen.....	31
Tabelle 12: URI-Nomenklatur von AutoID-Objekten	31
Tabelle 13: URI-Nomenklatur von AutoID-Objekten (ISO/IEC, generisch)	31
Tabelle 14: Aufbau der URI-Nomenklatur von AutoID-Lesepunkten	31
Tabelle 15: Aufbau der URI-Nomenklatur von AutoID-Leseorten	32
Tabelle 16: Application Family Identifiers (AFIs) nach ISO/IEC.....	34
Tabelle 17: ASCII-Character-to-6-Bit-Encoding nach ISO 17363-17367	35

Abkürzungsverzeichnis

AFI	Application Family Identifier
an	alphanumerisch
API	Application Programming Interface
ASCII	American Standard for Information Interchange
DI	Data Identifier
DSFID	Data Structure Format Identifier
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EOT	End of Transmission
EPC	Electronic Product Code
EPCIS	Electronic Product Code Information Services
GS	Group Separator
GS1	Global Standards One
HazMat	Hazardous Materials
IEC	International Electrotechnical Commission
IP	International Protection
ISO	International Organization for Standardization
ITU	International Telecommunications Union
MB	Memory Bank
OID	Object Identifier
PC	Protocol Control
RFID	Radio Frequency Identification
RS	Record Separator
TID	Tag Identification
UHF	Ultra High Frequency
UII	Unique Item Identifier
UM	User Memory
VDA	Verband der Automobilindustrie
VIN	Vehicle Identification Number
XML	Extensible Markup Language

1 Einleitung

Der Einsatz von Radio Frequency Identification (RFID) trägt zur Steigerung der Prozesseffektivität und -effizienz innerhalb der Automobilindustrie bei. Das gilt insbesondere für den Einsatz von passiven UHF-Transpondern (Ultra High Frequency). Typische Anwendungsfälle sind die Steuerung und Verfolgung von Fahrzeugen, Bauteilen und (Mehrweg-)Behältern. RFID wird seit vielen Jahren erfolgreich in der Automobilindustrie eingesetzt. Bisher kam RFID überwiegend in unternehmensinternen, geschlossenen Kreisläufen zum Einsatz (closed loop). Seit einigen Jahren rückt der RFID-Einsatz in unternehmensübergreifenden, offenen Kreisläufen in den Fokus (open loop).

Der Einsatz von RFID in der unternehmensübergreifenden Supply Chain ermöglicht die Realisierung einer Reihe von wirtschaftlichen Potentialen:

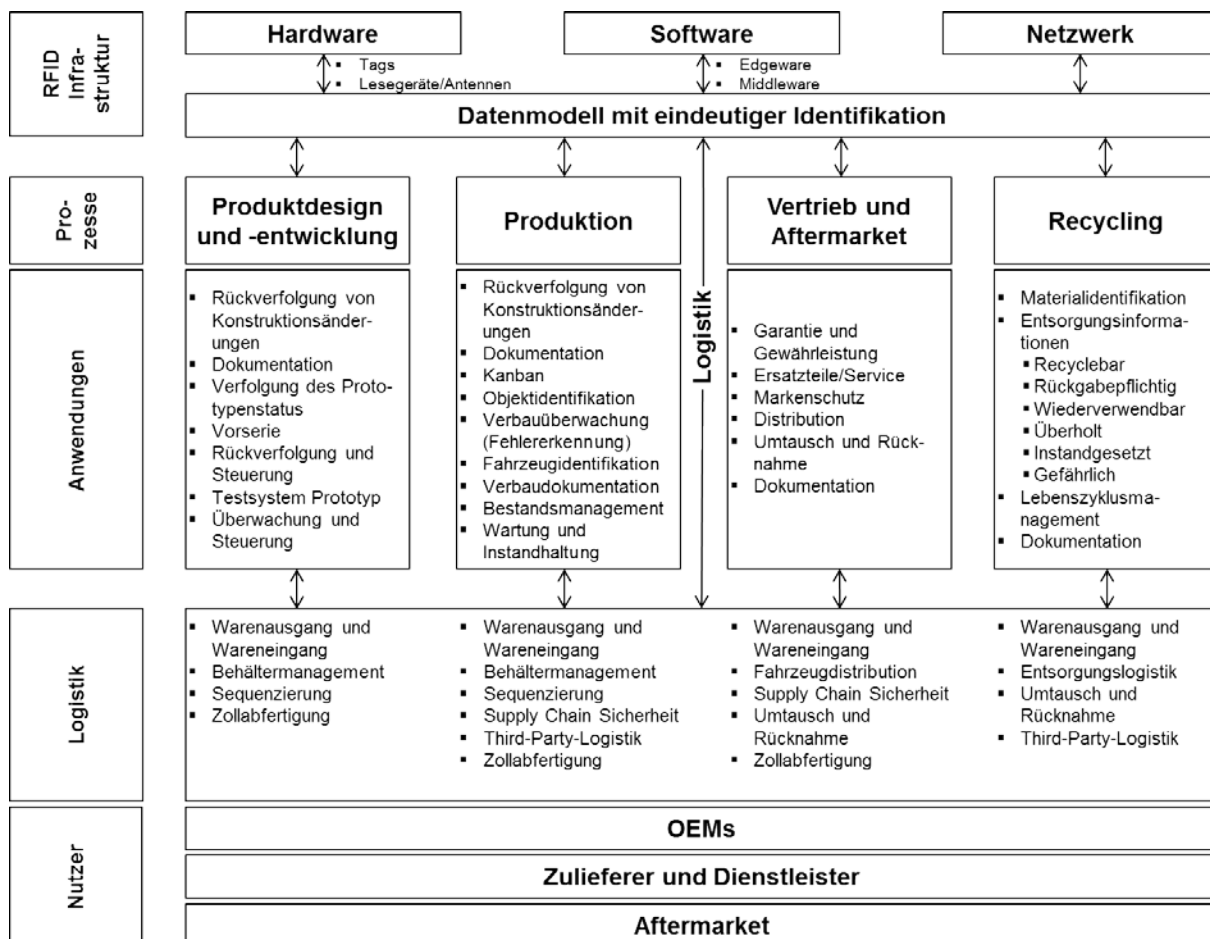


Abbildung 1: RFID-Potentiale in der Automobilindustrie

Gleichzeitig setzt der unternehmensübergreifende RFID-Einsatz Standards und Richtlinien voraus, damit die verwendeten RFID-Transponder und gespeicherte Dateninhalte über Unternehmensgrenzen hinaus von allen Prozessbeteiligten genutzt werden können. Vor diesem Hintergrund hat der Verband der Automobilindustrie (VDA) die folgenden, industriespezifischen Empfehlungen für den Einsatz der RFID-Technologie erarbeitet:

- VDA 5501 – RFID im Behältermanagement der Supply Chain
- VDA 5509 – AutoID/RFID-Einsatz und Datentransfer zur Verfolgung von Bauteilen und Komponenten in der Fahrzeugentwicklung
- VDA 5510 – RFID zur Verfolgung von Teilen und Baugruppen
- VDA 5520 – RFID in der Fahrzeugdistribution

Diese Industrieempfehlungen spiegeln wesentliche Anwendungsbereiche des RFID-Einsatzes in den unternehmensübergreifenden Prozessen der Automobilindustrie wider. Die Industrieempfehlungen VDA 5501, 5509, 5510 und VDA 5520 beschreiben technische Anforderungen an RFID-Transponder und die Gestaltung von Datenstrukturen. Die VDA 5500 fasst Gemeinsamkeiten und damit grundsätzliche Anforderungen zusammen und fungiert damit als übergeordneter, allgemeiner Leitfaden zu den oben genannten, anwendungsspezifischen Industrieempfehlungen.

Der Aufbau dieses Dokuments gestaltet sich wie folgt: In Kapitel 2 werden technische Anforderungen an den Einsatz passiver RFID-Transponder definiert. Kapitel 3 spezifiziert Grundsätze bei der Gestaltung RFID-spezifischer Datenstrukturen. Kapitel 4 beschreibt die zusätzliche optische Kennzeichnung von RFID-Objekten. Kapitel 5 thematisiert den RFID-spezifischen, unternehmens-internen Datenaustausch zwischen RFID-Geräten und IT-Systemen sowie den unternehmensübergreifenden Datenaustausch im RFID-Kontext.

Anwendungsbeispiele, applikationsspezifische Anforderungen an RFID-Transponder und RFID-Datenstrukturen, die zusätzliche optische Kennzeichnung von RFID-Objekten, und die Gestaltung des Datenaustauschs werden in Abhängigkeit von den jeweiligen Anwendungsfällen in den Industrieempfehlungen VDA 5501, 5509, 5510 und VDA 5520 konkretisiert.

2 Technische Anforderungen an RFID-Transponder

Im Folgenden werden allgemeingültige, technische Anforderungen an passive RFID-Transponder beschrieben.

2.1 Funktionsweise passiver RFID-Transponder

Passive RFID-Systeme bestehen aus folgenden Komponenten:

- RFID-Schreib-/Leseinheit inkl. Antenne (stationär, mobil)
- RFID-Transponder für die Identifizierung von Objekten

Die RFID-Transponder bestehen aus einem Mikrochip und einer Antenne (vgl. Abbildung 2). Die passiven RFID-Transponder werden mithilfe von Funkwellen durch die RFID-Schreib-/Leseinheiten mit Energie versorgt. Durch Modulation der Funkwellen kann der RFID-Reader mit dem Transponder kommunizieren. Der Transponder antwortet durch modulierte Reflexion (Backscattering) der Funkwellen. Passive RFID-Transponder benötigen daher keine eigene Energieversorgung. Aus diesem Grund sind passive RFID-Transponder besonders flexibel in Bezug auf die Größe und Bauform. Die Tatsache, dass passive RFID-Transponder über keine eigene Energieversorgung besitzen, macht sie darüber hinaus besonders kostengünstig in der Beschaffung und Instandhaltung. Die Reichweite passiver RFID-Systeme beträgt je nach Art der verwendeten Hardware-Komponenten und in Abhängigkeit von den jeweiligen Rahmenbedingungen üblicherweise zwischen 1-10 m. Hohe Variabilität, Reichweite und Kostenvorteile ermöglichen ein großes Anwendungsspektrum innerhalb der Automobilindustrie.

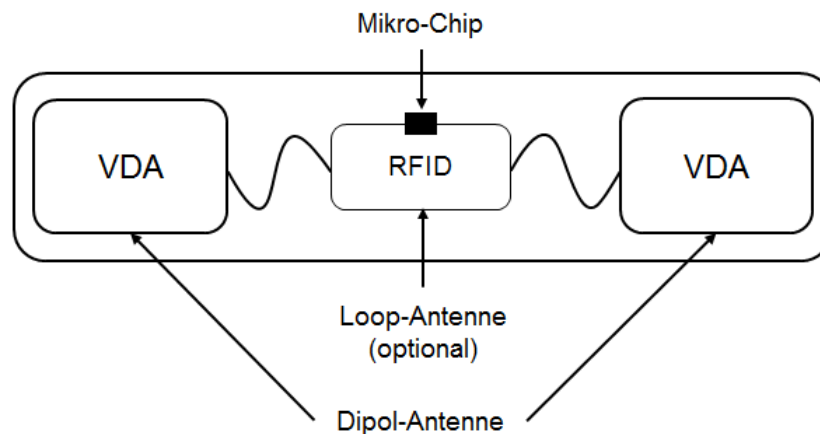


Abbildung 2: Aufbau eines RFID-Transponders

Hinweis

Standardtransponder besitzen üblicherweise eine Kombination zweier Antennentypen (Hybridantenne). Im Nahfeld, also wenige Zentimeter zwischen Sendeantenne und Transponderantenne, wird eine Loop-Antenne eingesetzt (vgl. Abbildung 2). Durch induktive Kopplung können dadurch sehr nah beieinander platzierte Transponder separiert mit Energie versorgt und programmiert werden (z. B. RFID-Drucker). Eine Dipolantenne im Transponder übernimmt die Kommunikation im normalen Anwendungsfall (Fernfeld). Dabei ist zu beachten, dass es verschiedene Polarisierungstypen gibt: Sind die Antennen eines Transponders horizontal ausgerichtet (vgl. Abbildung 2), dann wird von horizontaler Polarisierung gesprochen. Wird die linear polarisierte Antenne der RFID-Schreib-/Leseinheit ebenfalls horizontal ausgerichtet, so können mit wenig Sendeleistung große Distanzen erreicht werden. Werden die Antennen um 90° gedreht, dann wird von vertikaler Polarisierung gesprochen. Häufig werden Antennen mit drehender Polarisierung (zirkuläre Polarisierung) eingesetzt, sodass die Polarisierung des RFID-Transponders eine untergeordnete Rolle spielt. Prinzipiell bestimmt die Wahl der Antennentypen und deren Ausrichtung jedoch maßgeblich die Leistungsfähigkeit von passiven RFID-Systemen (Leserate, Reichweite).

2.2 Luftschnittstelle und Frequenzbereiche

Die Luftschnittstelle der passiven RFID-Transponder entspricht den Vorgaben der ISO/IEC 18000-63/EPC Class1 Gen2. Bei der Wahl des Transponders sind die unterschiedlichen von der International Telecommunications Union (ITU) festgelegten Frequenzbereiche für UHF-Kommunikation zu berücksichtigen. Tabelle 1 zeigt die freigegebenen Frequenzbereiche:

Region	Frequenzbereich in MHz
Europa	865-868/ 869
USA/ Kanada	902-928
Südamerika	915
Südafrika	865-868
Australien	916-926
Japan	916-921
China	920-925

Tabelle 1: Weltweit freigegebene RFID-Frequenzbänder (UHF)

Grundsätzlich sollten verwendete RFID-Transponder in allen Regionen genutzt werden können, um internationale Supply-Chain-Anwendungen zu ermöglichen. Gleichzeitig ist zu beachten, dass RFID-Transponder in der Regel für den Einsatz in bestimmten Frequenzbereichen optimiert sind, d. h., dass es beim Einsatz in abweichenden Frequenzbereichen zur Verringerung der Leistungsfähigkeit kommen kann.

2.3 **Aufbau und Größe der Speicherbereiche**

Passive RFID-Transponder nach ISO/IEC 18000-63/EPC Class1 Gen2 verfügen über vier logische Speicherbereiche/ Memory Banks (MB). Die Speicherbereiche sind wie folgt aufgebaut (vgl. Abbildung 3).

- **MB 00 „RESERVED“ – Kill- and Access-Password**
Passwort für den Zugriff sowie für das Deaktivieren (Kill) des RFID-Transponders. MB 00 kann lese- und schreibgeschützt werden.
- **MB 01 „EPC“ – Unique Item Identifier (UII)**
Bei Suchabfrage eines Readers (Inventory-Befehl) liefert der Transponder den Inhalt der MB 01. Alle anderen Speicherbänke müssen i.d.R. mit adressierten Befehlen vom Reader angefragt werden. In MB 01 wird die eindeutige Kennung des RFID-Transponders als Unique Item Identifier (UII) abgelegt. MB 01 kann gegen Schreibzugriff geschützt werden.
- **MB 10 „TID“ – Tag Identification**
Informationen über Typ, Hersteller, Modell des RFID-Chips. Sollte auch eine Seriennummer des Chipherstellers enthalten. MB 10 kann i.d.R. nicht verändert bzw. beschrieben werden.
- **MB 11 „USER“ – User Memory (UM)**
Speicherung zusätzlicher objekt- und anwendungsspezifischer Daten. MB 11 kann mit einem Schreibschutz versehen werden.

Die detaillierte Spezifizierung und Beschreibung der dargestellten Speicherbereiche ist der ISO/IEC 18000-63 zu entnehmen. Die Speichergröße von MB 01 beträgt zwischen 96 und 496 bit. Für die meisten automobilspezifischen Anwendungen sollte der Speicherbereich MB 01 einer Größe von 240 bit entsprechen. Die konkrete Größe der Speicherbereiche MB 01 und MB 11 hängt entscheidend vom jeweiligen Anwendungsfall ab und wird in den applikationsspezifischen VDA-Empfehlungen VDA 5501, 5509, 5510 und 5520 konkretisiert.

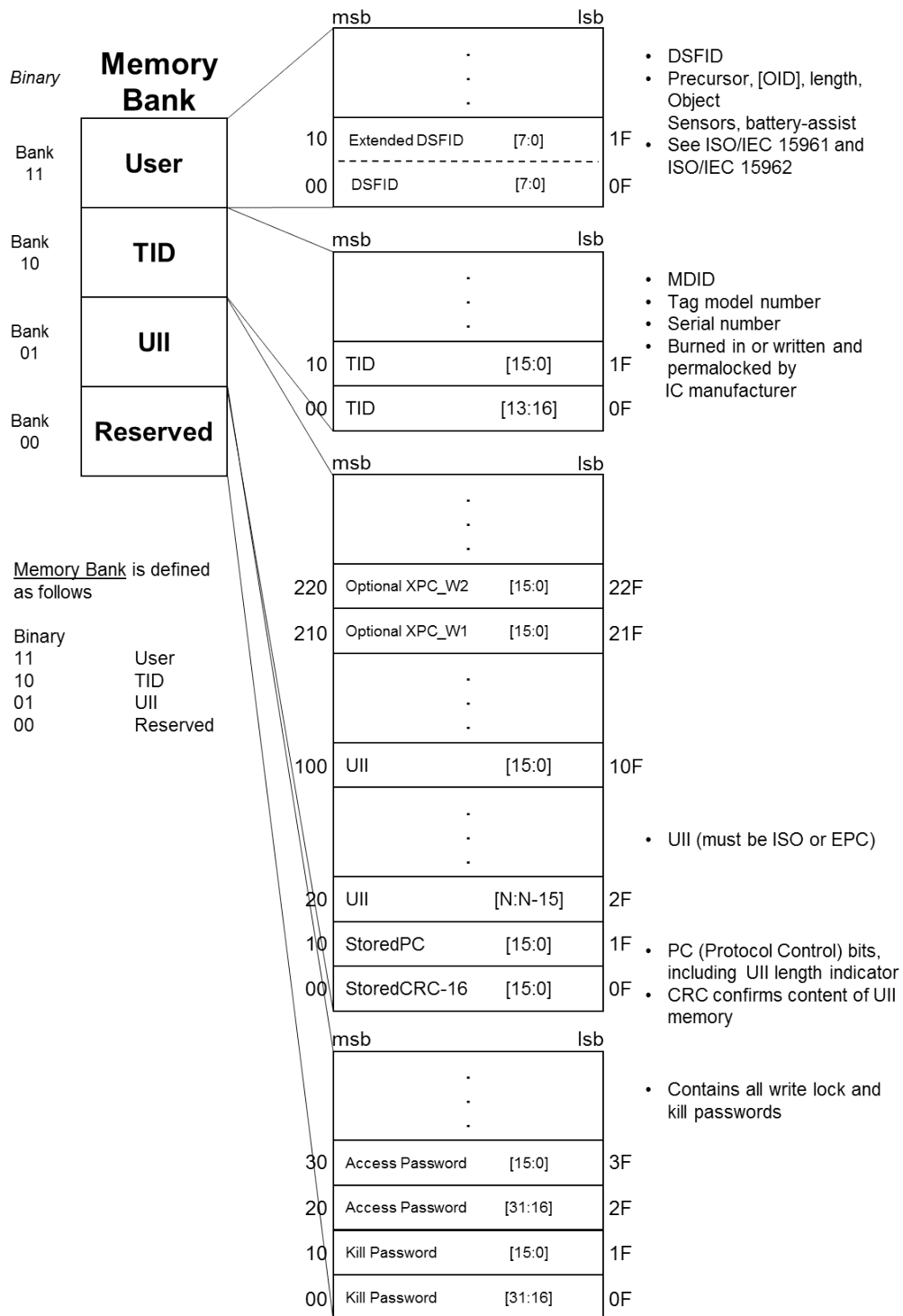


Abbildung 3: RFID-Speicherbereiche nach ISO/IEC 18000-63

2.4 Transponderauswahl, Positionierung und Befestigung

Die Auswahl von RFID-Transpondern, deren Positionierung, und die Art der Befestigung haben wesentlichen Einfluss auf die Leistungsfähigkeit passiver UHF-Systeme. Tabelle 2 zeigt verschiedene Transpondertypen und geeignete Oberflächenmaterialien auf:

Transpondertyp	Oberflächenmaterial	Anmerkung
Smart-Label (Papier o. ä.)	Kunststoffe, Stoffe, Glas (unbeschichtet)	Direktes Aufkleben von Labels. Nicht für Metall o. ä. geeignet.
Flag-Tag (Papier o. ä.)	Kunststoffe, Stoffe, Glas, Carbon, Metall	Smart-Label. Distanz zu Oberflächenmaterial wird durch Abknicken hergestellt. Auch für Metall o. ä. geeignet.
Hard-Tag (Kunststoff o. ä.)	Kunststoffe, Glas (beschichtet), Carbon, Metall	Abstand zur Oberfläche wird durch Bauform sichergestellt.
Embedded Transponder	Kunststoff, Stoffe, Glas	Transponder wird in das RFID-Objekt integriert.
Embedded RFID mit Schlitzantenne	Metall o. ä.	Transponder wird in das Objekt integriert. Objektoberflächenmaterial dient als Antenne.

Tabelle 2: Transpondertypen und geeignete Oberflächenmaterialien

Grundsätzlich steht eine Vielzahl von Befestigungsmöglichkeiten für RFID-Transponder zur Auswahl. Tabelle 3 stellt verbreitete Befestigungsarten und deren Vor- und Nachteile dar:

Befestigungsart	Vorteil	Nachteil
Kleben	Schnelles, kostengünstiges Abringen	Klebeverbindung muss Anforderungen an Bauteil entsprechen (Temperatur, Witterung, Lebensdauer etc.)
Einhängen	Flexibler Einsatz. Mehrfachverwendung möglich	Lediglich für temporäre Zuordnung von Transponder zu Objekt einsetzbar
Nieten	Besonders geeignet für Bleche, Leichtmetalle	Spezialwerkzeug erforderlich; Korrosionswahrscheinlichkeit
Schrauben	Permanente Verbindung. Einsatz von Standardwerkzeug	Bohrungen erforderlich; Korrosionswahrscheinlichkeit
Magnetisches Fixieren	Flexibler Einsatz. Mehrfachverwendung möglich	Magnetische Oberfläche erforderlich. Lediglich für temporäre Zuordnung von Transponder zu Objekt einsetzbar

Tabelle 3: Vor- und Nachteile von Befestigungsarten

Abbildung 4 zeigt exemplarische RFID-Anwendungen sowie entsprechende Transpondertypen und Befestigungsarten:



Abbildung 4: Exemplarische RFID-Anwendungen

Die Entscheidung für einen bestimmten Transpondertyp, dessen Positionierung und die jeweilige Befestigungsart hängt maßgeblich vom konkreten Anwendungsfall ab, und wird aus diesen Gründen in den anwendungsspezifischen VDA-Empfehlungen VDA 5501, 5509, 5510 und 5520 konkretisiert. Innerhalb der jeweiligen Anwendungsszenarien wird die Durchführung intensiver Praxistests empfohlen, um die Praxistauglichkeit der jeweiligen RFID-Applikation sicherzustellen. Folglich muss im Rahmen statischer und dynamischer Tests sichergestellt werden, dass die prozesssichere Erfassung ausgewählter Transponder unter Berücksichtigung der Positionierung und der Befestigungsart gewährleistet ist. Das schließt den applikationsspezifischen Aufbau und die Konfiguration von RFID-Erfassungspunkten (stationär, mobil) ein.

2.5 Rahmenbedingungen für den Transpondereinsatz

Innerhalb der Automobilindustrie kommen eine Reihe von Einflussfaktoren zum Tragen, die neben allgemeinen Faktoren (z. B. Schreib-/Lesegeschwindigkeit, Reichweite), die Leistungsfähigkeit von RFID-Systemen beeinflussen. Dazu zählen insbesondere:

- Reflektionen und Abschirmung durch Metall und Flüssigkeiten
- Absorbierende Oberflächen (z. B. Carbon)
- Resonanzverstimmende Oberflächen (z. B. Glas)
- Interferenzen durch andere Funksysteme (betrifft Fremdfunksender in gleichen bzw. in abweichenden Frequenzbändern)
- Elektrostatische Entladungen

Diese Rahmenbedingungen sind bei der Implementierung von RFID-Projekten und insbesondere bei der Transponderauswahl und –positionierung zu berücksichtigen.

2.6 *Zusätzliche Umwelteinflüsse und Lebensdauer*

Der Einsatz von RFID-Transpondern unterliegt, neben den in Abschnitt 2.5 aufgeführten Rahmenbedingungen, weiteren applikationsspezifischen Einflussfaktoren. Tabelle 4 zeigt einige dieser Umweltwelteinflüsse:

Umgebungseinfluss/Belastung	Ausprägung
Mechanische Belastungen	Stöße, Schwingungen, Druck, Reibung
Chemische Belastungen	Öle, Reinigungsmittel, Schmierstoffe, Säuren, Laugen, Alkohol, Tenside, Lösungsmittel etc.
Thermische Belastungen	Betriebs- und Lagertemperaturen
Witterungsbedingte Einflüsse	Schnee, Frost, Eis, Niederschlag, Nebel, Sonneneinstrahlung, salzige Seeluft etc.

Tabelle 4: Umwelteinflüsse und deren Ausprägungen

Aus diesem Grund empfiehlt sich für RFID-Transponder in den meisten Anwendungsfällen die Schutzklasse IP 54 (vgl. IEC 60529). Für diese Schutzklasse gelten folgende Eigenschaften:

- Vollständiger Berührungsschutz, Schutz gegen Staub im Inneren
- Geschützt gegen Sprühwasser

Im Rahmen gängiger RFID-Applikationen muss die dauerhafte Funktionalität bei Temperaturen von -40° bis +70° Celsius sichergestellt sein. Die jeweilige Befestigungsart sollte ebenfalls auf diesen Temperaturbereich ausgelegt sein. Je nach Anwendung kann es auch zu abweichenden Temperaturanforderungen kommen. Diese Abweichungen sind den applikationsspezifischen VDA-Empfehlungen 5501, 5509, 5510 und 5520 zu entnehmen.

Hinweis

Bzgl. der RFID-Transponder ist zwischen verschiedenen Temperaturangaben zu unterscheiden. Die Betriebstemperatur gibt an, bei welchen Temperaturen der RFID-Transponder beschrieben und ausgelesen werden kann. Die allgemeine Temperaturbeständigkeit gibt an, bis zu welchen Temperaturwerten die Haltbarkeit des RFID-Transponders gegeben ist - das heißt nicht, dass die RFID-Transponder bei den genannten Extremwerten tatsächlich auch beschrieben und ausgelesen werden können.

Die RFID-Transponder sollen im Allgemeinen eine Lebensdauer von 10 Jahren gewährleisten. Abweichende Anforderungen sind den VDA-Empfehlungen 5501, 5509, 5510 und 5520 zu entnehmen.

3 Allg. Grundsätze beim Aufbau von RFID-Datenstrukturen

3.1 Nutzung von Speicherbereichen

Nutzdaten werden in den beiden Speicherbereichen MB 01 und MB 11 hinterlegt. Dabei gelten folgende Prinzipien:

- Im Speicherbereich MB 01 wird der Header (Steuerinformation) und der Unique Item Identifier (UII) hinterlegt. Der UII repräsentiert eine exklusiv vergebene, eindeutige Referenz-ID, die das Objekt identifiziert. Die Referenz-ID wird normalerweise genutzt, um auf zusätzliche Informationen zu referenzieren, die in unterstützenden IT-Systemen hinterlegt sind. Der Speicherbereich MB 01 wird nach dem initialen Beschreiben vor weiterem Schreibzugriff geschützt (lock).
- Im Speicherbereich MB 11 befindet sich der User Memory (UM). Auf dem UM können zusätzliche Nutzdaten hinterlegt werden. Bei Nutzung des UM ist zu berücksichtigen, dass es bei größeren Datenmengen unter Umständen zu Leistungseinschränkungen (Dauer von Schreib-/Leseprozessen) kommen kann. Gleichzeitig liegen keine grundlegenden Vereinbarungen bzgl. des Aufbaus entsprechender Dateninhalte vor. Aus diesen Gründen unterliegt die Verwendung des UM der bilateralen Vereinbarung der Prozesspartner.

3.2 Auswahl von Datenstandards (ISO/IEC, GS1)

Bezüglich des Aufbaus von RFID-spezifischen Datenstrukturen haben sich in der Automobilindustrie zwei alternative Vorgehensweisen etabliert:

- Aufbau von Datenstrukturen nach ISO/IEC
- Aufbau von Datenstrukturen nach GS1

Für die Abwicklung von unternehmensübergreifenden RFID-Applikationen wird die Umsetzung von ISO/IEC-Standards empfohlen. Der Einsatz von GS1-Standards ist möglich – beschränkt sich jedoch auf unternehmensinterne Anwendungen und/oder zusätzliche, bilaterale Vereinbarungen. Die Umsetzung von GS1-Standards ist in den jeweils aktuellen GS1-Dokumenten beschrieben und wird an dieser Stelle nicht näher erläutert. Im Folgenden wird die ISO/IEC-Vorgehensweise beim Beschreiben der Speicherbereiche MB 01 und MB 11 konkretisiert.

3.3 Beschreiben des Speicherbereichs MB 01 (ISO/IEC)

Im Speicherbereich MB 01 werden der Header (Steuerinformation) und der eigentliche UII hinterlegt. Abbildung 5 zeigt den Aufbau des Speicherbereichs:

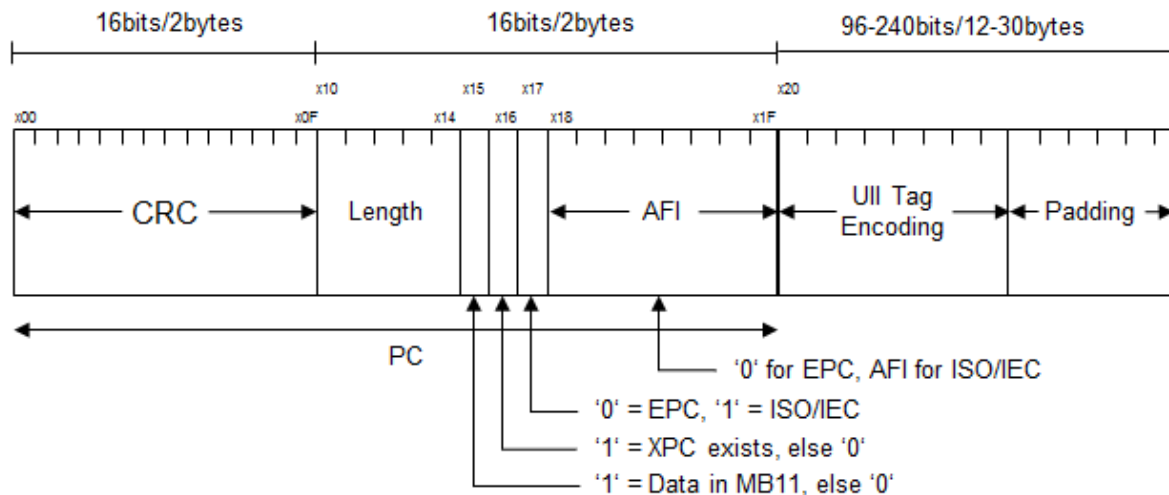


Abbildung 5: Aufbau der Speicherbank MB 01

Der **Header** beinhaltet folgende Steuerinformationen:

- Cyclic Redundancy Check (CRC)
- Wortlänge der Nutzdaten (16 bit words)
- Nutzung des Speicherbereichs MB 11 (Ja/Nein)
- Nutzung Extended PC word (Ja/Nein)
- Definition des Datenstandards nach ISO/IEC bzw. GS1 (Toggle Bit)
- Application Family Identifier (AFI)

Technische Details zum Aufbau und zur korrekten Anwendung der o. g. Steuerinformationen sind ISO/IEC 15961 zu entnehmen. An dieser Stelle wird insbesondere auf das Setzen des *Toggle Bits* und die Verwendung von Application Family Identifiers (AFI) eingegangen.

Mithilfe des **Toggle Bits** (17_{hex}) wird definiert, ob die Daten innerhalb der Speicherbank MB 01 nach ISO/IEC- oder nach GS1-Standard kodiert sind:

- GS1-Standard: Toggle-Bit auf 0
- ISO/IEC-Standard: Toggle-Bit auf 1

Im Rahmen der ISO/IEC-Codierung hat die Verwendung von Application Family Identifiers (AFI) eine besonders hohe Bedeutung. AFIs sind wichtige Primärfilter, mit deren Hilfe festgestellt werden kann, was für ein Objekt ausgelesen wird (z. B. Bauteil, Mehrwegbehälter). Auf diese Weise kann an spezifischen RFID-Lesepunkten zwischen applikationsrelevanten und nicht relevanten RFID-Objekten gefiltert werden. Darüber hinaus macht der verwendete AFI Angaben zu der Kodierung der RFID-Datenstrukturen (6-bit). Die AFIs werden in ISO/IEC 15961-2 Data Constructs Register aufgelistet. Die Ausprägung des AFI entspricht dabei dem jeweiligen Anwendungsfall (ISO 17363-17367) und wird in den applikationsspezifischen VDA-Empfehlungen benannt.

Der **UII** beinhaltet die eigentliche Referenz-ID des RFID-gekennzeichneten Objekts. Der Aufbau der Referenz-ID entspricht dabei ISO/IEC 15418/ANSI MH10.8.2 und ISO/IEC 15961-15962 sowie ISO 17363-17367. Die weitere industriespezifische Konkretisierung erfolgt in VDA 5501, 5509, 5510 sowie 5520.

Die Referenz-ID wird mithilfe von Data Identifiers (DI) gekennzeichnet. Der DI ist ein wichtiger Hinweis auf die Objektgruppe und Datenstruktur der nachfolgenden Daten. Deshalb kann er auch als Sekundärfilter genutzt werden, um festzustellen, was für ein Objekttyp ausgelesen wird (z. B. Behältertyp), d. h., der DI stellt im Verbund mit dem AFI ein stark differenzierendes Filterkriterium dar. Die Nutzung etablierter DI ermöglicht die Sicherstellung der Konformität und Kompatibilität mit bisherigen Barcode- und DataMatrix-Implementierungen.

Die Referenz-ID wird gemäß den Anwendungsstandards ISO 17363-17367 mit End of Transmission (<EoT>) abgeschlossen. Ziel dabei ist es, den RFID-Lesevorgang zu verbessern, indem lediglich relevante Daten eingelesen und der Lesevorgang anschließend abgebrochen werden kann. Wenn die Datenstruktur des UII den gesamten verfügbaren Speicherbereich belegt (MB 01), dann kann <EoT> entfallen. Die Länge der Referenz-ID inklusive DI und ggf. <EoT> bildet die UII und sollte insgesamt nicht die Länge von 40 alphanumerischen Zeichen überschreiten (240 bit), um den gängigen Speichergrößen verfügbarer RFID-Transponder gerecht zu werden. Nach Standard sind maximal 496 bit möglich.

Die Länge der RFID-Datenstruktur kann je nach Anwendung unterschiedlich sein. Im sogenannten Protocol Control (PC) - Speicherbereich (5-Bit Länge, direkt nach den 16-Bit CRC) erfolgt im MB 01 die Längenangabe des UII. Die Längenangabe beschreibt, wieviele 16-bit Wörter der UII umfasst. Zum Auffüllen auf jeweils volle 16-Bit-Worte werden Paddingbits angehängt. Gemäß ISO/IEC 15962 wird dazu eine festgelegte Bitfolge verwendet. Details sind Tabelle 5 zu entnehmen.

Hinweis

<EoT> und eventuelle Paddingbits innerhalb des UII (MB 01) und UM (MB 11) werden als Steuer- und Füllzeichen verwendet. Sie sind jedoch kein Bestandteil des eigentlichen Dateninhalts und werden deshalb beim Dekodieren entfernt und nicht an nachgelagerte IT-Anwendersysteme weitergegeben.

Die Dateninhalte des UII inklusive Referenz-ID werden 6-bit kodiert, d. h., es gilt die reguläre 6-bit Kodierung für die Darstellung von Buchstaben, Zahlen und Sonderzeichen. Folglich dürfen ausschließlich Großbuchstaben und eine eingeschränkte Menge von Sonderzeichen verwendet werden (siehe ISO/IEC 15962). Die Kodierungsvorschrift kann dem Anhang (Tabelle 17) entnommen werden.

Der vollständige Aufbau der MB 01 Datenstruktur inklusive der vorangestellten Protokoll-Kontrollbits (PC-Header) gestaltet sich wie folgt:

Bit Location (Hex)	Data Type	Value	Size	Description
MB 01: CRC + Protocol Control Word (Header)				
00 – 0F	CRC-16	Hardware assigned	16 bits	Cyclic Redundancy Check
10 – 14	Length	Variable	5 bits	Number of 16-bit words without Protocol Control information and AFI
15	PC bit 0x15	0b0 or 0b1	1 bit	0 = No valid User Data, or no MB 11 ₂ 1 = Valid User Data in MB 11 ₂
16	PC bit 0x16	0b0	1 bit	0 = "Extended PC word" not used
17	PC bit 0x17	0b1	1 bit	1 = Data interpretation rules based on ISO/IEC vs GS1
18 – 1F	AFI	z. B. 0xA1, 0xA2	8 bits	Application Family Identifier used according to ISO/IEC 15961/2 and ISO 17363-17367.
	Subtotal		32 bits	
MB 01: Unique Item Identifier (UII) with 6 bit encoding				
Start at location 20. Go to end of data /end of available memory	Referenz-ID (Platzhalter), Alphanumerisch (an)		n * 6 bits	Reference-ID including Data Identifier (DI)
	<EoT>	0b100001	6 bit	End of Transmission ISO 17363-17367
	Padding until the end of the last 16-bit word	0b10, 0b1000, 0b100000, 0b10000010, 0b1000001000, 0b100000100000, or 0b10000010000010	2, 4, 6, 8, 10, 12 or 14 bits	Bit Padding Schema according to ISO/IEC 15962 Chapter 13.1
	Subtotal Reference-ID		Variable	96 - 240 bit
	Total MB 01		Variable	Up to 272 bits

Tabelle 5: Kodierung des Speicherbereichs MB 01

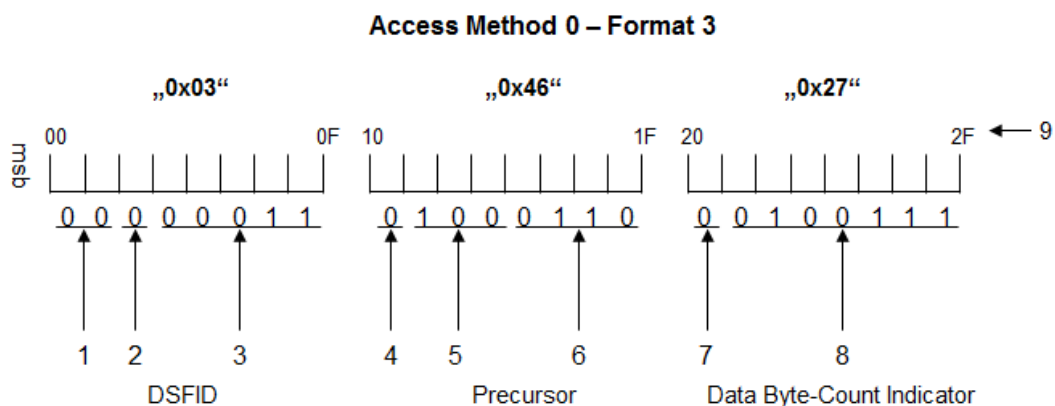
Im Anhang ist ein Kodierungsbeispiel beschrieben. Weitere Details und Kodierungsbeispiele sind den zugrundeliegenden ISO/IEC-Normen bzw. den jeweiligen anwendungsbezogenen VDA-Empfehlungen zu entnehmen.

3.4 Beschreiben des Speicherbereichs MB 11 (ISO/IEC)

Im Speicherbereich MB 11 können zusätzliche Objekt- und Anwenderdaten hinterlegt werden. Aus diesem Grund wird der Speicherbereich MB 11 auch User Memory (UM) genannt. Der Aufbau des UM mit 6-Bit-Code und DIs erfolgt ähnlich zum UII, d. h., neben den eigentlichen Nutzdaten werden auch Steuerinformationen abgelegt. Die Steuerinformationen wird in den ersten drei Bytes bzw. vier Bytes des Speicherbereichs MB 11 hinterlegt und sind wie folgt strukturiert:

- Data Structure Format Identifier (DSFID)
- Precursor (Compaction Code + Relative OID)
- Byte Count Indicator

Abbildung 6 zeigt den Aufbau der Steuerinformation:



- 1 Access Method: 0 (ISO/IEC 15962)
- 2 Extended Syntax: 0 (not required)
- 3 Data Format 3 (ISO/IEC 15434)
- 4 Extension Bit (not used)
- 5 Compaction Type (6 bit)
- 6 15434 Format Envelope `06`
- 7 Byte Count Indicator Switch (set to 0 indicating final byte of byte count)
- 8 Bit values for Byte Count Indicator (depends on length of data)
- 9 Physical memory addresses (00, 0F, 10, 1F, 20, 2F)

Abbildung 6: Aufbau von Steuerinformationen in MB 11

Der Data Structure Format Identifier (DSFID) beschreibt die Zugriffsmethode und das Datenformat. Verwendet wird die Zugriffsmethode 0, Format 3. Details sind ISO/IEC 15962 zu entnehmen. Der Precursor beschreibt die verwendete Kodierungsart (6-bit) und das Datenformat (Verwendung von Data Identifiers nach ISO/IEC 15434). Der

Byte Count Indicator beschreibt die Länge der im Speicherbereich MB 11 abgelegten Nutzdaten, also den kompletten 6-Bit kodierten nachfolgende Datensatz inklusive <EoT> und Paddingbits. Ist dieser Datensatz größer als 128 Byte (1024 Bit), so erfolgt die Längenangabe mit zwei Bytes, andernfalls nur mit einem Byte. Tabelle 6 und 7 verdeutlichen den Sachverhalt.

Die eigentlichen Objekt- und Anwenderdaten werden nach ISO/IEC 15418 mit Hilfe von DI identifiziert und mithilfe von Trennzeichen ($G_S = „^“$) getrennt. Die Identifizierung der einzelnen Datenelemente mit Hilfe von DI ist insofern besonders wichtig, als dass das Beschreiben von Dateninhalten innerhalb des UM bislang keiner unternehmensübergreifenden Vereinbarung unterliegt. Die ISO/IEC-konforme, eindeutige Identifizierung mit Hilfe von DI stellt sicher, dass die Dateninhalte auch ohne vorherige bilaterale Vereinbarung identifiziert werden können. Der UM wird mit <EoT> (!) abgeschlossen. Ziel dabei ist es, den RFID-Lesevorgang zu verbessern, indem lediglich relevante Objekt- und Anwenderinformation eingelesen und der Lesevorgang anschließend abgebrochen werden kann. Wenn die Daten den UM vollständig belegen, dann kann <EoT> folglich entfallen. Eventuell freie Bits im letzten verwendeten 16 bit Block (word) des UM werden mit Füllzeichen (Paddingbits) nach ISO/IEC 15962 Annex T 4.1 for MB 11 aufgefüllt.

Hinweis

<EoT> und eventuelle Paddingbits innerhalb des UII (MB 01) und UM (MB 11) werden als Steuer- und Füllzeichen beim Kodieren verwendet. Sie sind jedoch kein Bestandteil des eigentlichen Dateninhalts und werden deshalb beim Dekodieren entfernt und nicht an nachgelagerte IT-Anwendersysteme weitergegeben.

Die Dateninhalte werden 6-bit kodiert, d. h., es gilt die reguläre 6-bit Kodierung für die Darstellung von Buchstaben, Zahlen und Sonderzeichen. Folglich dürfen ausschließlich Ziffern, Großbuchstaben und eine eingeschränkte Menge von Sonderzeichen verwendet werden (siehe Anhang, Tabelle 17). Der Aufbau des User UM inklusive des vorangestellten Steuerinformation gestaltet sich bei einer Datengröße des MB 11 ≤ 1024 Bit wie folgt:

Position	Data Type	Value	Size	Description
MB 11: User Memory (UM): Steuerinformation (Header) für MB 11 ≤ 1024 Bit Nutzdaten				
1	DSFID	03 _(hex)	1 byte	Data Structure Format Identifier
2	Precursor	46 _(hex)	1 byte	Compaction Code + Relative OID)
3a	Byte Count Indicator Switch	0 ₍₂₎	1 bit	0 ₍₂₎ signalisiert, dass folgende 7 bits für die eigentliche Längenangabe der darauf folgenden Daten genutzt werden (Object Length ≤ 1024 bits). Keine Nutzung weiterer Bytes für Längenangabe.

3b	Byte Count Indicator Length	Variable	7 bit	Länge der folgenden Daten in Bytes (Object Length)
	Subtotal		24 bits	

Beträgt die Datengröße des MB 11 > 1024 Bit, dann gestaltet sich der Aufbau der Steuerinformation wie folgt:

MB 11: User Memory (UM): Objekt- und Anwenderdaten				
1	Data Identifier ₁	<DI ₁ >	6 ... 24 bit	DI Datenelement ₁
2	Datenelement ₁	alphanumerisch (an)	n * 6 bit	Datenelement ₁
3	Group Separator	<GS> („^“ in ASCII)	6 bit	Trennzeichen
4	Data Identifier ₂	<DI ₂ >	6 ... 24 bit	DI Datenelement ₂
5	Datenelement ₂	alphanumerisch (an)	n * 6 bit	Datenelement ₂
6
7	<EoT>	0b100001	6 bit	End of Transmission according to ISO 17363-17367
8	Padding	0b10, 0b1000, 0b100001, 0b10000110, 0b1000011000, 0b100001100001, or 0b10000110000110	2, 4, 6, 8, 10, 12 or 14 bits	Padding according to ISO/IEC 15962 Annex T 4.1 for MB 11
	Total MB 11		Variable	Up to chip limit

Tabelle 6: Kodierung des Speicherbereichs MB 11 ≤ 1024 Bit Nutzdaten

Position	Data Type	Value	Size	Description
MB 11: User Memory (UM): Steuerinformation (Header) für MB 11 > 1024 Bit Nutzdaten				
1	DSFID	03 _(hex)	1 byte	Data Structure Format Identifier
2	Precursor	46 _(hex)	1 byte	Compaction Code + Relative OID

3a	Byte Count Indicator Switch	$1_{(2)}$	1 bit	$1_{(2)}$ signalisiert, dass zusätzliches Byte für die Längenangabe genutzt wird. Nächsten 7 bits werden mit den entsprechenden 7 bits des Folge-Bytes für die Längenangabe der darauf folgenden Daten verkettet (Object Length > 1024 bits)
3b	Byte Count Indicator Length	Variable	7 bit	Erster Teil der Längenangabe mit Faktor 2^7 ($3b \cdot 128 + 4b$)
4a	Byte Count Indicator Switch	$0_{(2)}$	1 bit	$0_{(2)}$ signalisiert, dass nächste 7 bits für Längenangabe der darauf folgenden Daten genutzt werden. Keine weiteren Bytes für Längenangabe (Verkettungsende)
4b	Byte Count Indicator Length	Variable	7 bit	Zweiter Teil der Längenangabe ($3b \cdot 128 + 4b$) Bsp: 3b: 40000001 (128 Bytes) 4b: 00000010 (2 Bytes) Total Object Length: 130 Bytes
Subtotal			32 bits	

Tabelle 7: Aufbau der Steuerinformation für MB 11 > 1024 Bit Nutzdaten

Weitere Details und Kodierungsbeispiele sind den zugrundeliegenden ISO/IEC-Normen bzw. den jeweiligen anwendungsbezogenen VDA-Empfehlungen zu entnehmen.

3.5 Umsetzung des Schreib-/Leseschutzes und Kill-Befehl

Die RFID-Kennzeichnung von Objekten stellt für die Beteiligten eine finanzielle Investition dar. Viele RFID-gekennzeichnete Objekte zirkulieren in offenen Kreisläufen. Damit kann die beabsichtigte oder unbeabsichtigte Zweckentfremdung der angebrachten RFID-Transponder nicht immer zuverlässig sichergestellt werden. Um die Investition der Beteiligten zu schützen und die einsatzgebundene Verwendung der RFID-Transponder sicherzustellen, müssen die RFID-Transponder geschützt werden. Zu diesem Zweck wird der Schreib-/Leseschutz eingesetzt. Gleichzeitig wird der RFID-Transponder vor der Deaktivierung durch Dritte geschützt. Im Folgenden werden die technischen Rahmenbedingungen für den Schreib-/Leseschutz und das Vermeiden der Deaktivierung durch Dritte erläutert:

RFID-Transponder nach ISO/IEC 18000-63 verfügen über ein 32-bit *Access Password* (20_h to 3F_h) und ein *Kill Password* (00_h to 1F_h). Diese Passwörter werden in MB 00 hinterlegt.

Sobald ein Transponder angesprochen wird, wechselt der Transponder in einen der folgenden Zustände.

1. Open (öffentlicher Zustand)
2. Secured (abgesicherter Zustand)

Falls ein Access-Passwort in MB 00 vergeben ist (*Access Password* \neq „0“), ist die Angabe des Passworts erforderlich, um in den Zustand *Secured* zu wechseln. Wenn kein Access-Passwort in MB 00 vergeben ist (*Access Password* = „0“), geht der Transponder direkt in den Zustand *Secured* über. Abbildung 7 zeigt das *Tag State Diagram* nach ISO/IEC 18000-63.

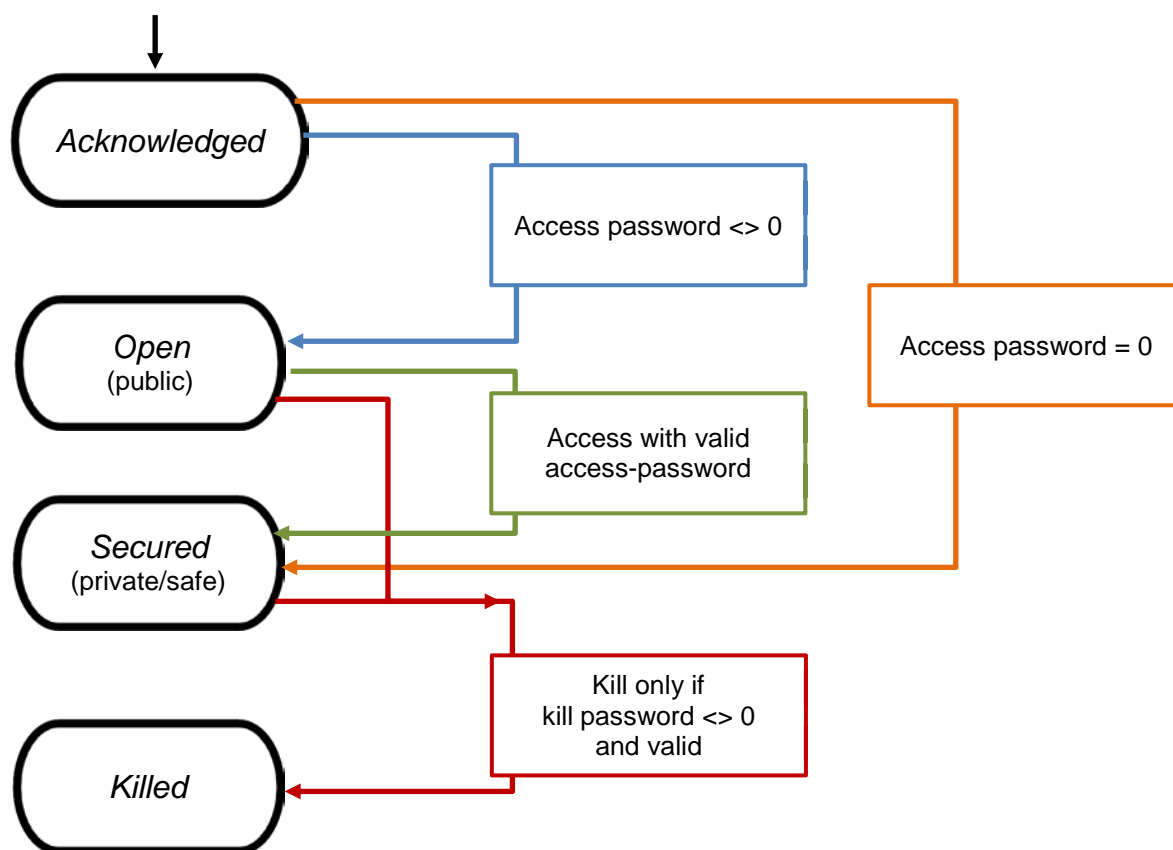


Abbildung 7: Transponderzustände gemäß ISO/IEC 18000-63

Im Zustand *Secured* können spezielle Lock-Befehle ausgeführt werden, um festzulegen, welche Speicherbereiche im Zustand *Open* lesbar bzw. beschreibbar sind.

Grundsätzlich können Speicherbereiche über vier Lock-Zustände verfügen. Der gewünschte Zustand wird dem Transponder mit dem Lock-Befehl mitgeteilt. Tabelle 8 zeigt die entsprechenden Lock-Optionen und deren Auswirkungen.

Lock-Optionen	Auswirkung auf Speicherbereiche MB 01 / MB 11
Unlocked	Der adressierte Speicherbereich ist in den Zuständen <i>Open</i> und <i>Secured</i> beschreibbar.
Perma-Unlocked	Der adressierte Speicherbereich ist in den Zuständen <i>Open</i> und <i>Secured</i> permanent beschreibbar und kann nicht gesperrt werden.
Locked	Der adressierte Speicherbereich ist im Zustand <i>Secured</i> beschreibbar, aber nicht im Zustand <i>Open</i> .
Perma-Locked	Der adressierte Speicherbereich ist in den Zuständen <i>Open</i> und <i>Secured</i> dauerhaft nicht beschreibbar.
Auswirkung auf Speicherbereich MB 00 (Passwörter)	
Unlocked	Der adressierte Passwortbereich in den Zuständen <i>Open</i> und <i>Secured</i> lesbar und beschreibbar.
Perma-Unlocked	Der adressierte Passwortbereich ist in den Zuständen <i>Open</i> and <i>Secured</i> permanent lesbar und beschreibbar und kann nicht gesperrt werden.
Locked	Der adressierte Passwortbereich ist nur im Zustand <i>Secured</i> lesbar und beschreibbar, aber nicht im Zustand <i>Open</i> .
Perma-Locked	Der adressierte Passwortbereich ist in den Zuständen <i>Open</i> und <i>Secured</i> dauerhaft weder lesbar noch beschreibbar.

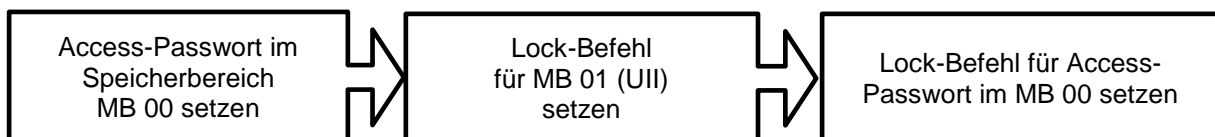
Tabelle 8: Lock-Optionen für RFID-Transponder gemäß ISO/IEC 18000-63

Der Passwort-Speicherbereich MB 00 kann sowohl gegen Lese- als auch Schreibzugriffe geschützt werden. Die Speicherbereiche MB 01 und MB 11 können lediglich gegen Schreibzugriffe geschützt werden.

RFID-Transponder können mithilfe des Kill-Befehls deaktiviert werden. Das Deaktivieren eines RFID-Transponders kann nicht rückgängig gemacht werden, d. h., der RFID-Transponder ist nicht mehr nutzbar. Um das Deaktivieren des RFID-Transponders dauerhaft zu verhindern, wird das Kill-Passwort im Speicherbereich MB 00 mit einem „Null“-Passwort versehen (siehe Abbildung 7).

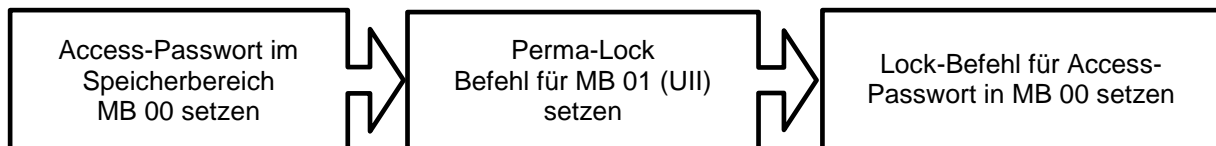
Im Folgenden wird die technische Umsetzung der o. g. Schutzmaßnahmen beschrieben:

Option 1: Schutz des UII (mit Access-Passwort veränderbar):



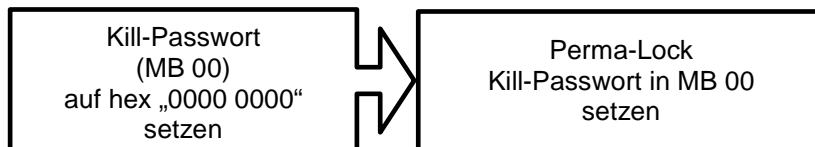
Der Lock-Befehl auf das Passwort in MB 00 sorgt dafür, dass das Passwort vor Lesezugriffen und damit vor Missbrauch geschützt ist.

Option 2: Permanenter Schutz des UII (unveränderbar):



Der Lock-Befehl auf das Passwort in MB 00 sorgt dafür, dass das Passwort vor Lesezugriffen und damit vor Missbrauch geschützt ist. Bei Verwendung des Perma-Locks für MB 01 kann dieser Schritt entfallen, da der Perma-Lock auch bei Angabe des korrekten Access-Passworts nicht zurückgenommen werden kann.

Unabhängig von der gewählten Option für den Schreib-/Leseschutz gilt, dass der RFID-Transponder dauerhaft gegen Deaktivierung (Kill-Befehl) geschützt wird:



Weiterführende Details zur Verwendung des Schreib-/Leseschutzes und des Kill-Befehls sind ISO/IEC 18000-63 zu entnehmen.

Hinweis:

Bei der Umsetzung von RFID-Projekten ist zu berücksichtigen, dass Hersteller von RFID-Schreib-/Lesegeräten oft spezifische Kommandos für die Realisierung des Schreib-/Leseschutzes und des Kill-Befehls verwenden. Darüber hinaus bieten einige Transponderhersteller weitere, proprietäre Schutzmechanismen und Kommandos an, um zusätzliche Lese- und Kopierschutzmöglichkeiten zu ermöglichen. VDA 5500 beschreibt lediglich den Umfang der Standardfunktionen, die in ISO/IEC 18000-63 spezifiziert sind. Darüber hinausgehende Funktionen sind den technischen Handbüchern der Hersteller und den jeweiligen APIs zu entnehmen.

4 Zusätzliche optische Kennzeichnung von Objekten

Ergänzend zur RFID-Kennzeichnung wird das zusätzliche Kennzeichnen mit Hilfe von optischen Identifizierungsmethoden wie Klarschrift und Barcode-/DataMatrix-Codes empfohlen. Hintergrund ist das geeignete Bereitstellen von *Backup*-Methoden sowie die Vermeidung technologiebedingter Medienbrüche. Diese Vorgehensweise stellt sicher, dass die Konformität und Kompatibilität der RFID-Kennzeichnung mit etablierten Barcode-/DataMatrix-Methoden gewährleistet, und damit die Koexistenz von Barcode-/DataMatrix sowie die schrittweise Migration von Barcode-/DataMatrix zu RFID ermöglicht wird.

4.1 Verwendung von Klarschrift und 1D/2D-Codes (ISO/IEC)

Das optische Kennzeichnen folgt den Prinzipien der RFID-Kennzeichnung. Dateninhalte werden grundsätzlich mit Hilfe von DI gekennzeichnet (vgl. ISO/IEC 15418). Bei Verwendung von 2D-Codes sind nach ISO/IEC 15434 zusätzlich die Startsequenz, der Format Indicator, ein Record Separator (R_S), Group Separator (G_S) und End of Transmission (E_{OT}) zu verwenden (*non-displayable characters*). Tabelle 9 zeigt exemplarisch die Formatierung von einem Code 128 (1D) und einem DataMatrix-Code (2D):

Beschreibung Dateninhalt	Code 128	DataMatrix
Startsequenz	*	[>
Record Separator	*	R_S
Format Indicator	*	06
Group Separator	*	G_S
Data Identifier ₁	<DI ₁ >	<DI ₁ >
Datenelement ₁	[..]	[..]
<i>Group Separator</i>	*	G_S
<i>Data Identifier₂</i>	*	<DI ₂ >
<i>Datenelement₂</i>	*	[..]
..
Record Separator	*	R_S
End of Transmission	*	E_{OT}

Tabelle 9: Exemplarische Codierung von 1D/2D-Codes

* keine Anwendung

Tabelle 10 zeigt den exemplarischen Aufbau der 1D/2D-Datenstrukturen:

1D/2D-Code	Exemplarischer Aufbau der Datenstruktur
Code 128	<DI>[Datenelement]
DataMatrix	[> ^R _S 06 ^G _S <DI ₁ >[Datenelement ₁] ^G _S <DI ₂ >[Datenelement ₂] ^R _S ^E O _T

Tabelle 10: Exemplarischer Aufbau von 1D/2D-Datenstrukturen

Im Gegensatz zum RFID-Prinzip werden die alphanumerischen Dateninhalte nicht 6-bit sondern 8-bit kodiert. Um die Synchronisierung von RFID- und 1D/2D-Datenstrukturen sicherzustellen, dürfen jedoch nur die in der 6-bit Kodierung üblichen Buchstaben, Zahlen und Sonderzeichen verwendet werden, d. h., es dürfen ausschließlich Großbuchstaben und eine eingeschränkte Menge von Sonderzeichen verwendet werden (siehe Anhang, Tabelle 17). Falls möglich, dann werden die codierten Daten zusätzlich als Klarschrift auf dem RFID-Transponder bzw. dem 1D/2D-Label dargestellt. Konkrete Beispiele und exemplarische 1D/2D-Codes sind den jeweiligen anwendungsbezogenen VDA-Empfehlungen zu entnehmen.

4.2 Verwendung des RFID-Symbols

Im Rahmen der RFID-Kennzeichnung wird empfohlen zur optischen Markierung das RFID-Emblem nach ISO/IEC 29160 zu verwenden (Abbildung 8).



Abbildung 8: RFID-Symbol

Die genaue Gestaltung des RFID-Emblems entspricht dem jeweiligen Anwendungsfall, d. h., es sind die jeweiligen anwendungsspezifischen Varianten des RFID-Emblems zu verwenden. Zusätzliche Hintergrundinformation zum RFID-Emblem sind unter <http://www.rfidemblem.eu/> zu finden.

5 Unternehmensexterner und -übergreifender Datenaustausch

Im Rahmen des RFID-spezifischen Datenaustauschs wird im Wesentlichen zwischen zwei Varianten unterschieden:

- Datenaustausch zwischen RFID-Geräten und IT-Systemen (unternehmensintern)
- Datenaustausch zwischen Geschäftspartnern (unternehmensübergreifend)

In den folgenden Abschnitten werden die beiden Varianten beschrieben.

5.1 Datenaustausch zwischen RFID-Geräten und IT-Systemen

Die *Electronic Product Code Information Services* (EPCIS) bieten ein geeignetes *Framework* für die Erfassung, den Austausch und die Abfrage von Ereignisdaten, die bspw. durch Auto-ID-Geräte (Barcode- oder RFID-Lesegeräte) erfasst wurden. Der EPCIS-Ansatz ist sowohl für die Abbildung von GS1 - als auch ISO/IEC-basierten Datenstrukturen geeignet (RFID, 1D/2D-Codes).

Abbildung 9 skizziert den Aufbau einer entsprechenden IT-Infrastruktur:

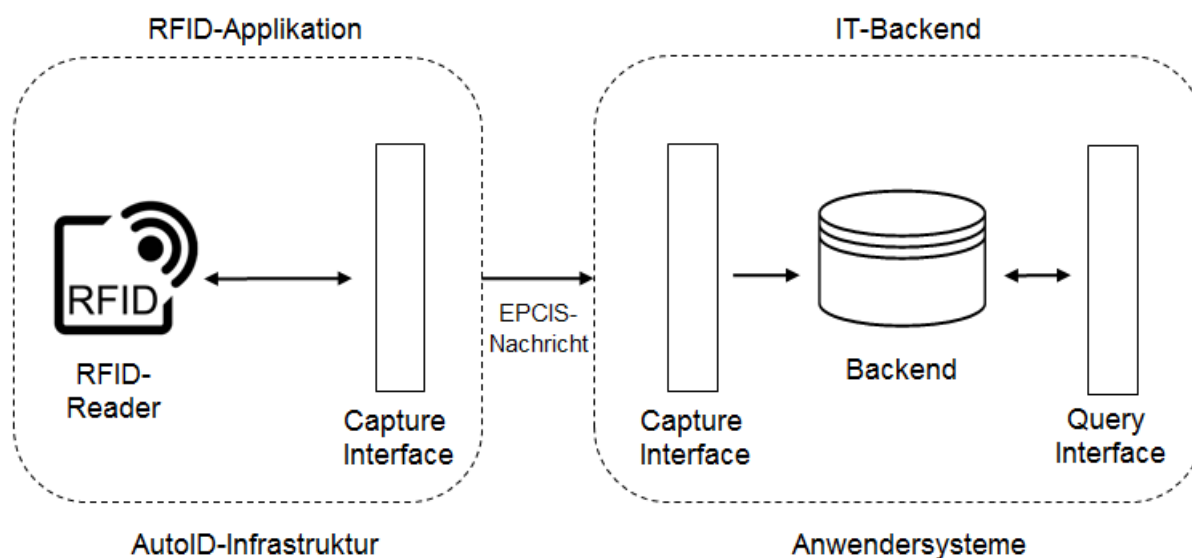


Abbildung 9: Datenübertragung von der RFID-Applikation an IT-Backends

Gekennzeichnete Objekte werden per RFID-Transponder bzw. 1D/2D-Codes erfasst und mit Hilfe dedizierter *Capturing Applications* in das EPCIS-Nachrichtenformat (XML) konvertiert. Die *Capturing Applications* setzen die EPCIS-Nachrichten bspw. per *http post* an das EPCIS Capture Interface ab (vgl. EPCIS Standard). Die erfassten Daten werden standardkonform an IT-Backend-Systeme versendet oder in einem *EPCIS-Repository* hinterlegt und können von dort bedarfsgerecht an Drittsysteme verschickt oder von Drittsystemen abgerufen werden.

Das EPCIS-Nachrichtenformat beinhaltet folgende Kerndaten:

Leseergebnisse (Was?)	Fahrzeug, Mehrwegbehälter..
Lesepunkt (Wo?)	Ort der RFID-Erfassung
Zeitstempel (Wann?)	Erfassungszeitpunkt
Kontext der Lesung (Warum?)	z. B. Wareneingang, Qualitätsprüfung

Tabelle 11: Grundlegende Informationen von AutoID-Ereignissen

Erfasste RFID-Objekte (**Was?**) werden im Rahmen des EPCIS-basierten Datenaustauschs in URI-Nomenklatur (*Uniform Resource Identifier*) dargestellt. Nach dem EPCIS-Framework ist die Übertragung und Ablage der sogenannten *Pure Identity* erforderlich, d. h., dass eindeutige Objektreferenzen abgebildet werden.

Tabelle 12 zeigt den exemplarischen Aufbau ISO/IEC- und GS1-konformer Nachrichteninhalte (vgl. CBV):

Standard	Uniform Resource Identifier (URI)	Exempl. Uniform Resource Name (URN)
ISO/IEC	urn:jaif:id:afi:[Pure Identity]	urn:jaif:id:A1:37SUN123456789 5Q1721095BK+123456789
GS1	urn:epc:id:sgln:[Pure Identity]	urn:epc:id:sgln:0614141.100734.400

Tabelle 12: URI-Nomenklatur von AutoID-Objekten

Im Rahmen der ISO/IEC-Repräsentation wird der RFID-typische AFI abgebildet (s. o.). In der Praxis kann es dazu kommen, dass der AFI entweder nicht oder fehlerhaft auf dem RFID-Transponder hinterlegt ist, sodass der AFI nicht korrekt ausgelesen und in die EPCIS-Nachricht eingetragen werden kann. In diesen Ausnahmefällen ist folgende generische Variante vorgesehen:

Standard	Uniform Resource Identifier (URI)	Exempl. Uniform Resource Name (URN)
ISO/IEC	urn:jaif:id:obj:[Pure Identity]	urn:jaif:id:obj:37SUN123456789 5Q1721095BK+123456789

Tabelle 13: URI-Nomenklatur von AutoID-Objekten (ISO/IEC, generisch)

1D/2D-Codes sehen im Gegensatz zu RFID-Datenstrukturen nicht die Abbildung der RFID-typischen AFIs vor. Dieser Fall wird ebenfalls durch die o. g. generische Variante abgedeckt, sodass die hybride Umsetzung von RFID und 1D/2D-Codes im Rahmen von EPCIS-Nachrichten gewährleistet ist.

Lesepunkte (RFID-Gates, mobile Handgeräte, Drucker etc.) werden auch *ReadPoints* genannt. *ReadPoints* werden analog zur beschriebenen Vorgehensweise nach URI-Nomenklatur abgebildet. Tabelle 14 zeigt entsprechende Beispiele für ISO/IEC- und GS1-basierte Datenstrukturen.

Standard	Uniform Resource Identifier (URI)	Beispiel
ISO/IEC	urn:jaif:id:obj:[Pure Identity]	urn:jaif:id:obj:25SUN123456789RFIDGate00001
GS1	urn:epc:id:sgln:[Pure Identity]	urn:epc:id:sgln:0614141.12345.0

Tabelle 14: Aufbau der URI-Nomenklatur von AutoID-Lesepunkten

Für die ISO/IEC-konforme Darstellung von *ReadPoints* wird die Verwendung der DIN 66277 empfohlen.

Der Ort, an dem eine RFID-Lesung stattfindet, wird auch als *bizLocation* (**Wo?**) bezeichnet (vgl. EPCIS Standard). Tabelle 15 zeigt exemplarische Datenstrukturen für ISO/IEC- und GS1-basierten Nachrichteninhalte.

Standard	Uniform Resource Identifier (URI)	Beispiel
ISO/IEC	urn:jaif:id:loc:[Pure Identity]	urn:jaif:id:loc:WOB.H55.1OG.Feld1
GS1	urn:epc:id:sgln:[Pure Identity]	urn:epc:id:sgln:0614141.54321.0

Tabelle 15: Aufbau der URI-Nomenklatur von AutoID-Leseorten

Die nähere Beschreibung des Lesevorgangs (**Warum?**) wird mit Hilfe sogenannter *BizSteps* dargestellt. Typische Beispiele sind Wareneingang, Warenausgang, Qualitätssicherung etc. Für die Beschreibung von Geschäftsvorgängen steht das sogenannte Core Business Vocabulary (CBV) und das ergänzende Automotive Business Vocabulary (ABV) zur Verfügung.

Die genauen Inhalte der EPCIS-Nachrichten und deren Aufbau hängen vom jeweiligen Anwendungsfall ab und werden deshalb innerhalb der applikations-spezifischen VDA-Empfehlungen VDA 5501, 5509, 5510 und VDA 5520 weitergehend spezifiziert.

5.2 Unternehmensübergreifender Datenaustausch

Der unternehmensübergreifende Datenaustausch wird innerhalb der Automobil-industrie klassischer Weise mithilfe von EDI-Nachrichten realisiert (z. B. EDIFACT). Alternativ können WebServices, wie z. B. der für die Datenübertragung innerhalb der Automobilindustrie entwickelte Webservice *auto-gration*, genutzt werden. Weitere Informationen unter <http://www.auto-gration.eu/>. Beide Methoden können auch für den Austausch von Referenzen auf eindeutig gekennzeichnete Objekte (RFID, 1D/2D-Codes) genutzt werden. Voraussetzung ist, dass die Nachrichtenformate über entsprechende Datenfelder verfügen.

Der Einsatz von RFID ermöglicht eine feingranulare Erfassung physikalischer Objektbewegungen. Zur Erfassung von objektbezogenen Ereignissen (Events) via RFID oder 1D/2D-Codes eignen sich beispielsweise EPCIS-Nachrichten. EPCIS-Nachrichten ersetzen dabei nicht die klassischen EDI-Nachrichtenformate, sondern ergänzen diese um Ereignisdaten. Dabei beschreiben sie den Kontext von Objektbewegungen. Damit ermöglichen EPCIS-Nachrichten die genauere Verfolgung physikalischer Objektbewegungen und erhöhen damit die Informationsqualität innerhalb der elektronischen Supply Chain. Beim Versenden von unternehmens-übergreifenden EPCIS-Nachrichten werden lediglich die erfassten Objekt-Referenzen (UII) und ein Kerndatensatz verschickt, der den Kontext der Objekterfassung beschreibt (vgl. Abschnitt 5.1). Die Inhalte des UM finden dabei keine Berücksichtigung.

Die weitere Konkretisierung des RFID-spezifischen Datenaustauschs hängt vom jeweiligen Anwendungsfall ab und werden daher applikationsspezifisch in VDA 5501, 5509, 5510 und 5520 beschrieben.

6 Referenzen

- GS1 Core Business Vocabulary (CBV)
- GS1 EPC Information Services (EPCIS) Standard
- GS1 Tag Data Standard (TDS)
- GS1 General Specification Version 14, January 2014:
http://www.gs1.org/docs/gsm/barcodes/GS1_General_Specifications.pdf
- IEC 60529 - Degrees of protection provided by enclosures (IP Code)
- ISO 3779 - Road vehicles - Vehicle identification number (VIN) - Content and structure
- ISO/IEC 15417 - Information Technology - Automatic Identification and Data Capture Techniques - Code 128 bar code symbology specification
- ISO/IEC 15418 - Information Technology - Automatic Identification and Data Capture Techniques - GS 1 Application Identifiers and ASC MH 10 Data Identifiers and Maintenance
- ISO/IEC 15434 - Information Technology - Syntax for High Capacity Automatic Data Capture (ADC) Media
- ISO/IEC 15961-1 Information Technology – Radio Frequency Identification (RFID) for Item Management - Data Protocol: Application Interface
- ISO/IEC 15961-2 Data Constructs Register
- ISO/IEC 15962 - Information Technology - Radio Frequency Identification (RFID) for Item Management - Data Protocol: Data Encoding Rules and Logical Memory Functions
- ISO/IEC 16022 - Information Technology - International Symbology Specification - Data Matrix
- ISO 17363 - Supply Chain Applications of RFID - Freight Containers
- ISO 17364 - Supply Chain Applications of RFID - Returnable Transport Items
- ISO 17365 - Supply Chain Applications of RFID - Transport Units
- ISO 17366 - Supply Chain Applications of RFID - Product Packaging
- ISO 17367 - Supply Chain Applications of RFID - Product Tagging
- ISO/IEC 18000-63 - Information Technology - Radio Frequency Identification for Item Management Part 6: Parameters for Air Interface Communications
- ISO/IEC 29160 - Information Technology - Radio Frequency Identification for Item Management - RFID Emblem
- VDA 5501 - RFID im Behältermanagement der Supply Chain
- VDA 5509 - AutoID/RFID-Einsatz und Datentransfer zur Verfolgung von Bauteilen und Komponenten in der Fahrzeugentwicklung
- VDA 5510 - RFID zur Verfolgung von Teilen und Baugruppen in der Automobilindustrie
- VDA 5520 - RFID in der Fahrzeugdistribution

7 Anhang

7.1 Application Family Identifiers (ISO/IEC)

AFI	Standards
A1	ISO 17367 – Supply chain applications of RFID – Product tagging
A2	ISO 17365 – Supply chain applications of RFID – Transport unit
A3	ISO 17364 – Supply chain applications of RFID – Returnable transport item
A4	ISO 17367 – Supply chain applications of RFID – Product tagging (HazMat)
A5	ISO 17366 – Supply chain applications of RFID – Product packaging
A6	ISO 17366 – Supply chain applications of RFID – Product packaging (HazMat)
A7	ISO 17365 – Supply chain applications of RFID – Transport unit (HazMat)
A8	ISO 17364 – Supply chain applications of RFID – Returnable transport item (HazMat)
A9	ISO 17363 – Supply chain applications of RFID – Freight container
AA	ISO 17363 – Supply chain applications of RFID – Freight container (HazMat)
90	Vehicle identified with the Vehicle Identification Number (VIN) as defined in ISO 3779

Tabelle 16: Application Family Identifiers (AFIs) nach ISO/IEC

7.2 Kodierungstabelle (6-bit Encoding)

Character	Binary Value	Character	Binary Value	Character	Binary Value	Character	Binary Value
Space	100000	0	110000	@	000000	P	010000
<EOT>	100001	1	110001	A	000001	Q	010001
<Reserved>	100010	2	110010	B	000010	R	010010
<FS>	100011	3	110011	C	000011	S	010011
<US>	100100	4	110100	D	000100	T	010100
<Reserved>	100101	5	110101	E	000101	U	010101
<Reserved>	100110	6	110110	F	000110	V	010110
<Reserved>	100111	7	110111	G	000111	W	010111
(101000	8	111000	H	001000	X	011000
)	101001	9	111001	I	001001	Y	011001
*	101010	:	111010	J	001010	Z	011010
+	101011	;	111011	K	001011	[011011
,	101100	<	111100	L	001100	\	011100
-	101101	=	111101	M	001101]	011101
.	101110	>	111110	N	001110	<GS>	011110
/	101111	?	111111	O	001111	<RS>	011111

Tabelle 17: ASCII-Character-to-6-Bit-Encoding nach ISO 17363-17367

7.3 Kodierungsbeispiel MB 01 (ISO 17367)

Reference-ID (plain text)

37SUN12345678999755512300FFFAS+123456

Compaction 6-bit code including <EoT>

110011	110111	010011	010101	001110	110001
110010	110011	110100	110101	110110	110111
111000	111001	111001	111001	110111	110101
110101	110101	110001	110010	110011	110000
110000	000110	000110	000110	000001	010011
101011	110001	110010	110011	110100	110101
110110	100001				

Complete data string including padding bits

1100111101110100	1101010100111011	0001110010110011
1101001101011101	1011011111100011	1001111001111001
1101111101011101	0111010111000111	0010110011110000
1100000001100001	1000011000000101	0011101011110001
1100101100111101	0011010111011010	0001 10000100000

Split into 8-bit fragments

11001111	01110100	11010101	00111011	00011100	10110011
11010011	01011101	10110111	11100011	10011110	01111001
11011111	01011101	01110101	11000111	00101100	11110000
11000000	01100001	10000110	00000101	00111010	11110001
11001011	00111101	00110101	11011010	00011000	00100000

Hex code representation

CF	74	D5	3B	1C	B3
D3	5D	B7	E3	9E	79
DF	5D	75	C7	2C	F0
C0	61	86	05	3A	F1
CB	3D	35	DA	18	20

PC data (cf. Section 3.3):

Ull-length in 16-bit words 0b **0111 1** (30 bytes → #15 words)
 Valid User Memory: 0b **0** (no user memory)
 XPC: 0b **0** (not used – reserved)
 EPC or ISO code: 0b **1** (ISO)

All PC bits: 0b **0111 1001** (hex 79)

Protocol Control (PC)	AFI
79	A1

Coded Ull content:

PC	AFI	Ull Reference																													
79	A1	CF	74	D5	3B	1C	B3	D3	5D	B7	E3	9E	79	DF	5D	75	C7	2C	F0	C0	61	86	05	3A	F1	CB	3D	35	DA	18	20