VDA Verband der Automobilindustrie

Empfehlung

Grundlagen zum AutoID-Einsatz in der Automobilindustrie

VDA 5500
Version 2.0, August 2026



Die vorliegende unverbindliche VDA-Empfehlung bietet einen Überblick über die Grundlagen des Einsatzes von AutoID-Technologien in der Automobilindustrie. Neben der Beschreibung und Standardisierung der technischen Anforderungen der einzelnen Technologien werden, sofern anwendbar, auch die zugrunde liegenden Datenstrukturen sowie deren Austausch betrachtet. Da die Auswahl der geeigneten Technologie vom jeweiligen Anwendungsfall abhängt, wird keine spezifische Technologie ausschließlich empfohlen. Ferner erhebt diese Empfehlung keinen Anspruch auf Vollständigkeit und wird bei Bedarf entsprechend dem Stand der Technik fortgeschrieben.

Haftungsausschluss

Die VDA-Empfehlungen sind Empfehlungen, die jedermann frei zur Anwendung stehen.
Wer sie anwendet, hat für die richtige Anwendung im konkreten Fall Sorge zu tragen.

Sie berücksichtigen den zum Zeitpunkt der jeweiligen Ausgabe herrschenden 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 VDA-Empfehlungen beteiligt sind, ist ausgeschlossen.

Jeder wird gebeten, wenn er bei der Anwendung der VDA-Empfehlungen auf Unrichtigkeiten oder die Möglichkeit einer unrichtigen Auslegung stößt, dies dem VDA umgehend mitzuteilen, damit etwaige Mängel beseitigt werden können.

Copyright 2026

Inhaltsangabe

1 Einleitung 5

2 Passive UHF Radio Frequency Identification (RFID) 7

2.1 Technische Anforderungen 7
2.2 Allgemeine Grundsätze beim Aufbau von RFID-Datenstrukturen 11
2.3 Verwendung des RFID-Symbols 21
2.4 Relevante Standards und Empfehlungen 22

3 Near Field Communication (NFC) 23

3.1 Technische Anforderungen 23
3.2 Relevante Standards und Empfehlungen 29

4 Bluetooth Low Energy (BLE) 30

4.1 Technische Anforderungen 30
4.2 Relevante Standards und Empfehlungen 37

5 Ultra Wideband (UWB) 37

6 Optische Identifikation von Objekten 37

6.1 Technische Anforderungen 37
6.2 Relevante Standards und Empfehlungen 39

7 Anhang 40

7.1 Empfehlungen und Standards 40
7.2 Application Family Identifiers (ISO/IEC) 42
7.3 Kodierungstabelle (6-bit Encoding) 43
7.4 Kodierungsbeispiel MB 01 (ISO 17360) 44

Copyright 2026

Versionsverlauf

Version	Veröffentlichung	Inhalte/Änderungen
1.0	Oktober 2014	Veröffentlichung zu Grundlagen zum RFID-Einsatz in der Automobilindustrie
1.1	April 2015	Präzisierungen der Speicherbereiche MB 01 & MB 11 sowie Ergänzung von Normreferenzen
1.2	Juni 2015	AFI 0x90 für die Identifizierung von Fahrzeugen ergänzt
2.0	August 2026	Vollständige Überarbeitung und Titeländerung der Empfehlung. Neben RFID sind Kapitel zu weiteren AutoID-Technologien wie NFC, BLE und UWB ergänzt

Copyright 2026

Abbildungsverzeichnis

Abbildung 1: AutoID-Potentiale in der Automobilindustrie 6
Abbildung 2: Aufbau eines RFID-Transponders 7
Abbildung 3: RFID-Speicherbereiche nach ISO/IEC 18000-63 10
Abbildung 4: Aufbau der Speicherbank MB 01 11
Abbildung 5: Aufbau von Steuerinformationen in MB 11 15
Abbildung 6: Transponderzustände gemäß ISO/IEC 18000-63 19
Abbildung 7: Generisches RFID-Symbol nach ISO/IEC 29160 21
Abbildung 8: Advertising-Kanäle innerhalb des 2,4-GHz-Frequenzbandes 32
Abbildung 9: Beispiel eines BLE Legacy Advertising Pakets 34
Abbildung 10: Beispiel eines BLE Diagnostic Advertising Pakets 35
Abbildung 11: Beispielhafte Modulgröße von Codesymbolen (x) 39

Tabellenverzeichnis

Tabelle 1: Kodierung des Speicherbereiches MB 01 14
Tabelle 2: Kodierung des Speicherbereichs MB 11 ≤ 1024 Bit Nutzdaten 17
Tabelle 3: Aufbau der Steuerinformation für MB 11 > 1024 Bit Nutzdaten 18
Tabelle 4: Lock-Optionen für RFID-Transponder gemäß ISO/IEC 18000-63 20
Tabelle 5: Übersicht der NFC-Tag Types 24
Tabelle 6: Übersicht der NDEF-Record Types 25
Tabelle 7: Struktur des Legacy Advertising Pakets 36
Tabelle 8: Struktur des Diagnostic Advertising Pakets 36
Tabelle 9: Exemplarische Codierung von 1D/2D-Codes 38
Tabelle 10: Exemplarischer Aufbau von 1D/2D-Datenstrukturen 38
Tabelle 11: Application Family Identifiers (AFIs) nach ISO/IEC 17360 (ehemals ISO/IEC 1736X) 42
Tabelle 12: ASCII-Character-to-6-Bit-Encoding nach ISO 17360, eingeschränkter Zeichensatz für Object Type + Serial Number 43

Abkürzungsverzeichnis

AFI ..... Application Family Identifiers
AoA ..... Angle of Arrival
BLE ..... Bluetooth Low Energy
CRC ..... Cyclic Redundancy Check
DI ..... Data Identifier
DMC ..... Data Matrix Code
DPP ..... Digital Product Passport
DSFID ..... Data Structure Format Identifier
eFTI ..... elektronische Frachtbeföderungsinformation
ELV ..... End-of-Life Vehicle
EoT ..... End of Transmission
FHSS ..... Frequency Hopping Spread Spectrum
GS ..... Group Seperator
GS1 ..... Global Standards One
IEC ..... International Electrotechnical Commission
IEEE ..... Institute of Electrical and Electronics Engineers
IoT ..... Internet of Things
ISO ..... International Organization for Standardization
ITU ..... International Telecommunications Union
MB ..... Memory Banks
NDEF ..... NFC Data Exchange Format
NFC ..... Near Field Communication
OID ..... Object Identifier

Copyright 2026

PC ..... Protocol Control
PPWR ..... Packaging and Packaging Waste Regulation
QR ..... Quick Response Code
RFID ..... Radio Frequency Identification
RS ..... Record Separator
RSSI ..... Received Signal Strength Indicator
SIG ..... Special Interest Group
UHF ..... Ultra High Frequency
UII ..... Unique Item Identifier
UM ..... User Memory
URI ..... Uniform Resource Identifier
URL ..... Uniform Resource Locator

Copyright 2026

1 Einleitung

AutoID-Technologien tragen zur Steigerung der Prozesseffektivität und -effizienz innerhalb der Automobilindustrie bei und werden seit vielen Jahren erfolgreich eingesetzt, sowohl in unternehmensinternen, geschlossenen (closed loop) als auch in unternehmensübergreifenden, offenen (open loop) Kreisläufen. Insbesondere unterstützen AutoID-Technologien papierlose Prozesse, regulatorische Anforderungen und den digitalen Zwilling. Die eindeutige Identifikation von Objekten (siehe VDA 5014) und ihre automatisierte Erfassung ermöglicht die Sammlung von Daten. Deren Auswertung und Verarbeitung kann dabei helfen, Probleme in Abläufen zu erkennen, zu lösen und Prozesse zu optimieren.

AutoID-Technologien ermöglichen eine nahtlose und effiziente Erfassung und Verarbeitung von Daten in Echtzeit. Dies reduziert den Bedarf an papierbasierten Dokumentationen erheblich und trägt zur Schaffung papierloser Prozesse unternehmensintern und -übergreifend bei. Durch die Automatisierung von Datenerfassungsprozessen können Fehler minimiert und die Effizienz gesteigert werden. Mitarbeiter haben jederzeit Zugriff auf aktuelle Informationen, was die Transparenz und Nachverfolgbarkeit erhöht.

Die Einhaltung regulatorischer Anforderungen, wie beispielsweise Packaging and Packaging Waste Regulation (PPWR), Digital Product Passport (DPP), elektronische Frachtbeföderungsinformation (eFTI), End-of-Life Vehicle (ELV) und weitere, sind auch in der Automobilindustrie von entscheidender Bedeutung. AutoID-Technologien unterstützen die lückenlose Dokumentation und Rückverfolgbarkeit von Produkten und Prozessen. Durch die automatische Erfassung und Speicherung von Daten können Unternehmen sicherstellen, dass alle relevanten Informationen jederzeit verfügbar und korrekt sind.

Der digitale Zwilling ist ein virtuelles Abbild eines physischen Objekts oder Systems, das dessen Zustand und Verhalten in Echtzeit widerspiegelt. AutoID-Technologien liefern die notwendigen Daten, um einen genauen und aktuellen digitalen Zwilling zu erstellen und zu pflegen. Durch die kontinuierliche Erfassung von Daten aus der realen Welt können Unternehmen den Zustand ihrer Lieferkette, der Logistik- und Produktionsprozesse in einem digitalen Abbild erfassen und überwachen. Dies ermöglicht eine genaue Analyse und kontinuierliche Optimierung der Geschäftsprozesse und führt zu einer verbesserten Entscheidungsfindung und einer höheren Betriebseffizienz.

Typische Anwendungsfälle sind hierbei die Steuerung und Verfolgung von Fahrzeugen, Bauteilen und (Mehrweg-)Behältern. Die vorliegende Empfehlung soll die technologieoffene Bewertung der Umsetzung von Anwendungsfällen mithilfe typischer AutoID-Technologien ermöglichen.

Auf konkrete Anwendungsfälle wird in folgenden VDA-Empfehlungen eingegangen:

- Behälterkennzeichnung (VDA 5501)
- Kennzeichnung von Prototypenteilen (VDA 5509)
- Teilekennzeichnung (VDA 5510)
- Fahrzeugidentifikation (VDA 5520)

Der Nachrichtenaustausch sowie regulatorische Anforderungen werden begleitend in der VDA 5530 bzw. 5540 beschrieben. Die VDA 5500 fasst Gemeinsamkeiten und grundsätzliche Anforderungen zusammen und fungiert damit als übergeordneter, allgemeiner Leitfaden zu den oben genannten, anwendungsspezifischen Industrieempfehlungen.

> **Hinweis**
> Die Empfehlung fokussiert sich auf AutoID-Technologien wie 1D-/2D-Code, Radio Frequency Identification (RFID), Near Field Communication (NFC), Bluetooth Low Energy (BLE) zur Identifikation von Objekten. Ortungstechnologien wie z.B. Ultra Wideband (UWB) werden aktuell nicht näher betrachtet.

Copyright 2026

Die Abbildung 1 zeigt die Potentiale von AutoID in der Automobilindustrie in verschiedenen Bereichen und Prozessen auf.

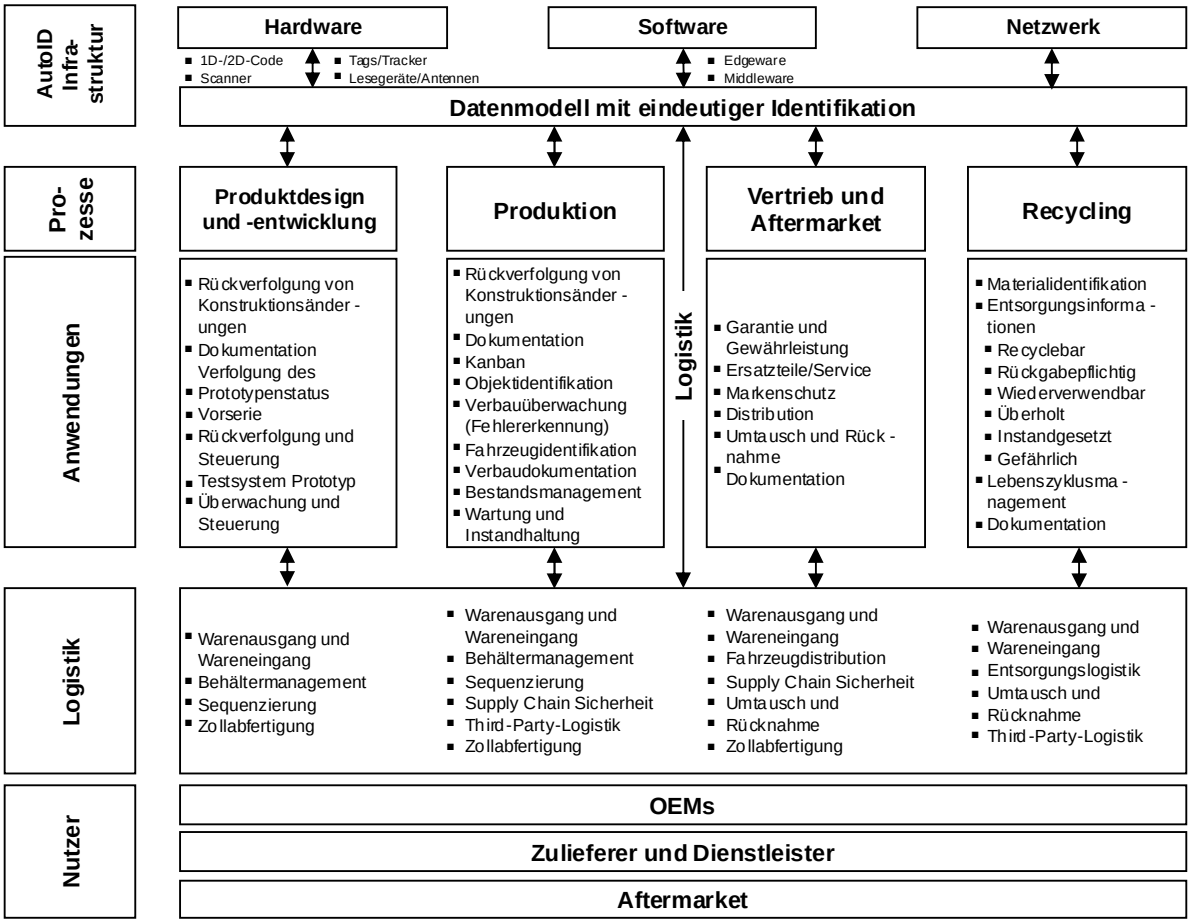


Abbildung 1: AutoID-Potentiale in der Automobilindustrie

In den folgenden Kapiteln werden jeweils verschiedene AutoID-Technologien, die in der Automobilindustrie Einzug finden, dargelegt und Empfehlungen zu deren Einsatz beschrieben. Anwendungsbeispiele, applikationsspezifische Anforderungen und die Gestaltung des Datenaustauschs werden in Abhängigkeit von den jeweiligen Anwendungsfällen in den zuvor genannten VDA-Empfehlungen konkretisiert.

Ziel der vorliegenden Empfehlung ist es, Abhängigkeiten und Lock-in-Effekte zu vermeiden und dafür größtmögliche Flexibilität und Skalierbarkeit zu fördern. Dabei wird eine langfristige Nutzungsdauer bei gleichzeitig optimierten Betriebskosten berücksichtigt. Ein weiterer zentraler Aspekt dieser Empfehlung ist die Förderung des Wettbewerbs.

Copyright 2026

2 Passive UHF Radio Frequency Identification (RFID)

RFID wird seit vielen Jahren erfolgreich in der Automobilindustrie eingesetzt. Bislang 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).

Allgemein wird zwischen aktiven und passiven RFID unterschieden, wobei erstere tendenziell selten in Logistikprozessen der Automobilindustrie eingesetzt werden. Aus diesem Grund wird in der VDA 5500 nur auf passive RFID näher eingegangen.

2.1 Technische Anforderungen

2.1.1 Funktionsweise passiver RFID-Systeme

Passive RFID-Systeme bestehen aus folgenden Komponenten:

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

Die RFID-Transponder bestehen aus einem Mikrochip und einer Antenne (siehe Abbildung 2). Die passiven RFID-Transponder werden mithilfe von Funkwellen durch die RFID-Schreib-/Leseeinheiten 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 wenigen Zentimetern bis zu über 10 m. Hohe Variabilität, Reichweite und Kostenvorteile ermöglichen ein großes Anwendungsspektrum innerhalb der Automobilindustrie.

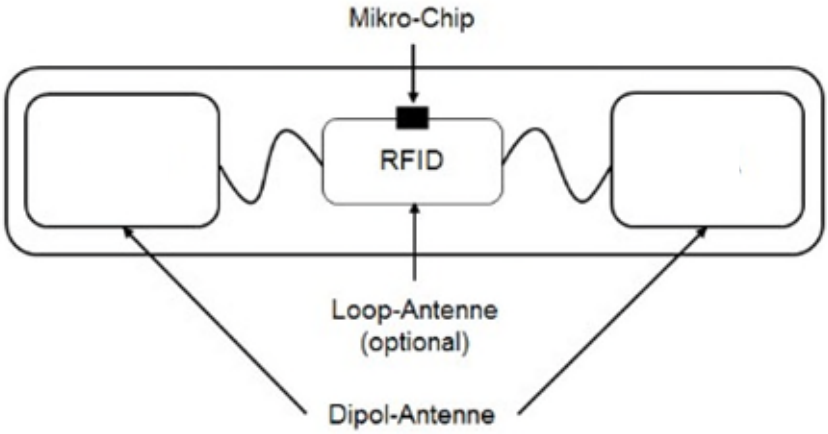


Abbildung 2: Aufbau eines RFID-Transponders

Copyright 2026

Hinweis
Standardtransponder besitzen üblicherweise eine Kombination zweier Antennentypen (Hybridantenne). Im Nahfeld, also wenige Zentimeter zwischen Sendeantenne und Transponderantenne, wird eine Loop-Antenne eingesetzt (siehe Abbildung 2). Durch induktive Kopplung können dadurch sehr nah beieinander platzierte Transponder separiert mit Energie versorgt und programmiert werden (z. B. RFID-Drucker). Eine Dipol-Antenne im Transponder übernimmt die Kommunikation im normalen Anwendungsfall (Fernfeld). Dabei ist zu beachten, dass es verschiedene Polarisationstypen gibt: Sind die Antennen eines Transponders horizontal ausgerichtet (siehe Abbildung 2), dann wird von horizontaler Polarisation gesprochen. Wird die linear polarisierte Antenne der RFID-Schreib-/Leseeinheit ebenfalls horizontal ausgerichtet, so können mit wenig Sendeleistung große Distanzen erreicht werden. Werden die Antennen um 90° gedreht, dann wird von vertikaler Polarisation gesprochen. Häufig werden Antennen mit drehender Polarisation (zirkulare Polarisation) eingesetzt, sodass die Polarisation 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).

2.1.2 Luftschnittstelle und Frequenzbereiche

Die Luftschnittstelle der passiven RFID-Transponder entspricht den Vorgaben der ISO/IEC 18000-63/EPC Class1 Gen2. Bei der Wahl der RFID-Hardware sind die unterschiedlichen von der International Telecommunications Union (ITU) festgelegten Frequenzbereiche für UHF-Kommunikation (860-930 MHz) zu berücksichtigen. Es dürfen ausschließlich Lesegeräte eingesetzt werden, die im jeweiligen Land für die entsprechenden Frequenzbänder behördlich zugelassen sind. Dies ist bereits im Rahmen der Beschaffung zu berücksichtigen.
Grundsätzlich sollte die verwendete RFID-Transponder in allen Regionen genutzt werden können, um internationale Supply-Chain-Anwendungen zu ermöglichen. Gleichzeitig ist zu beachten, dass RFID-Transponder, vor allem On-Metal-Transponder für den Einsatz in bestimmten Frequenzbereichen optimiert sein können, d.h., dass es beim Einsatz in abweichenden Frequenzbereichen zur Verringerung der Leistungsfähigkeit kommen kann.

2.1.3 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 (siehe 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.

Copyright 2026

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 benötigte Größe der Speicherbereiche MB 01 und MB 11 und damit die Auswahl des konkreten Chips hängt entscheidend vom jeweiligen Anwendungsfall ab.

Copyright 2026

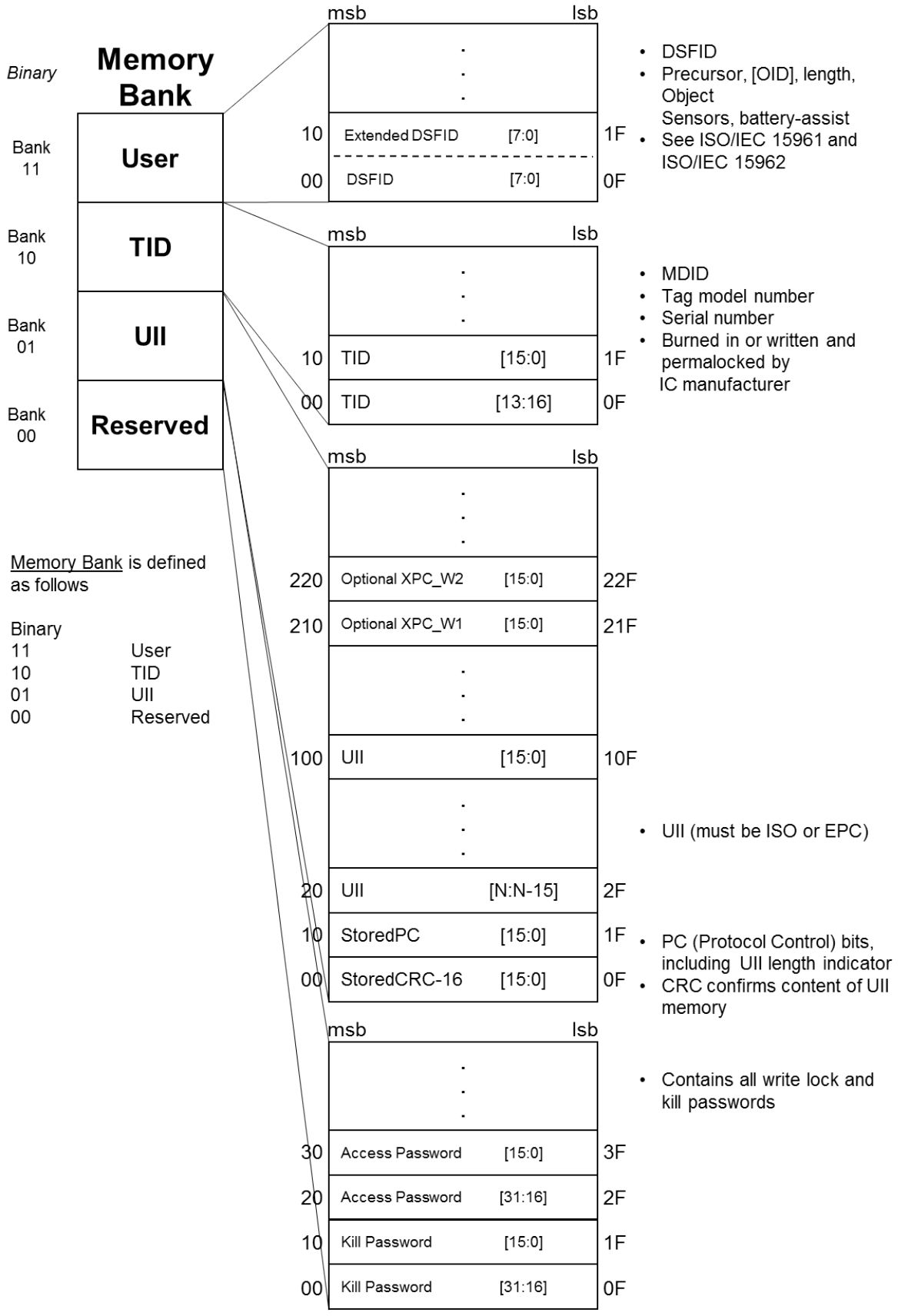


Abbildung 3: RFID-Speicherbereiche nach ISO/IEC 18000-63

Copyright 2026

2.2 Allgemeine Grundsätze beim Aufbau von RFID-Datenstrukturen

2.2.1 Nutzung von Speicherbereichen

Nutzdaten werden in den beiden Speicherbereichen MB 01 und MB 11 hinterlegt (siehe Abbildung 4). 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. 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.

2.2.2 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 gewinnt zunehmend an Bedeutung. Er sollte dabei mit allen beteiligten Parteien abgestimmt werden. 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.

2.2.3 Beschreiben des Speicherbereichs MB 01 (ISO/IEC)

Im Speicherbereich MB 01 werden der Header (Steuerinformation) und der eigentliche UII hinterlegt. Abbildung 4 zeigt den Aufbau des Speicherbereichs:

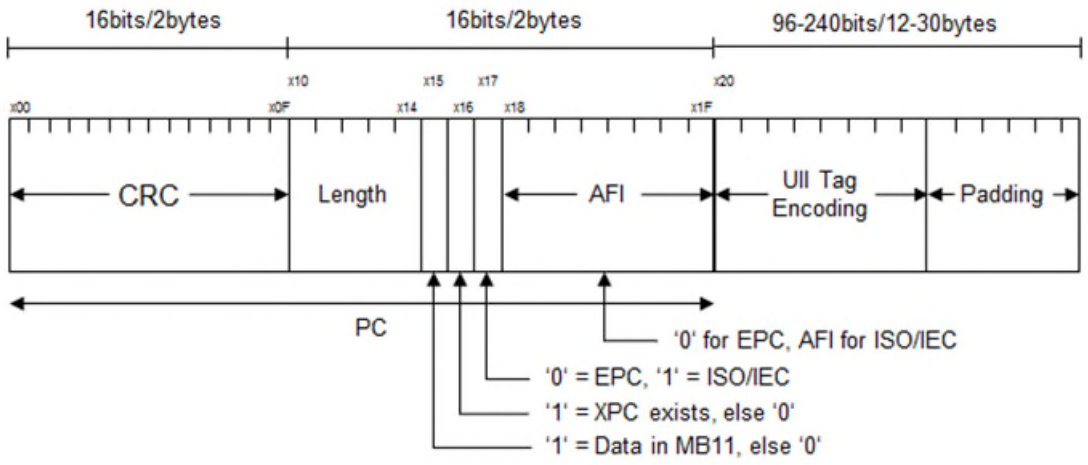


Abbildung 4: Aufbau der Speicherbank MB 01

Copyright 2026

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

Anmerkung: Es existieren Chips auf dem Markt, dessen Toggle-Bit (17_{hex}) herstellerseitig fest auf „0“ codiert sind und somit nicht für ISO/IEC Datenstrukturen nutzbar sind.

Im Rahmen der ISO/IEC-Codierung hat die Verwendung von 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 die verwendeten AFI-Angaben zu der Kodierung der RFID-Datenstrukturen (6-bit oder 8-bit). Die AFIs werden in ISO/IEC 15961-2 Data Constructs Register aufgelistet. Die Ausprägung des AFI entspricht dabei dem jeweiligen Anwendungsfall (ISO/IEC 17360) 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/IEC 17360. Die weitere industriespezifische Konkretisierung erfolgt in den anwendungsspezifischen VDA-Empfehlungen.

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 Data Matrix-Implementierungen.

Die Referenz-ID wird gemäß den Anwendungsstandards ISO/IEC 17360 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, wie viele 16-bit Wörter der UII umfasst. Zum Auffüllen auf

Copyright 2026

jeweils volle 16-Bit-Worte werden Paddingbits angehängt. Gemäß ISO/IEC 15962 wird dazu eine festgelegte Bitfolge verwendet. Details sind der Tabelle 1 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 gemäß dem verwendeten AFI codiert. In VDA Automotive Anwendung wird in der Regel 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 12 entnommen werden.

Der vollständige Aufbau der MB 01 Datenstruktur inklusive der vorangestellten Protokoll-Kontrollbits (PC-Header) ist in der Tabelle 1 dargestellt.

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

Copyright 2026

Tabelle 1: Kodierung des Speicherbereiches MB 01

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/IEC 17360
	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***
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/IEC 17360
	Subtotal		***32 bits***	
*Es ist zu beachten, dass es Chip-Hersteller gibt, bei denen das Bit 0x15 bei Vorhandensein eines User Memories standardmäßig auf 1 gesetzt ist. Dies sollte bei der Umsetzung in Projekten berücksichtigt werden.				

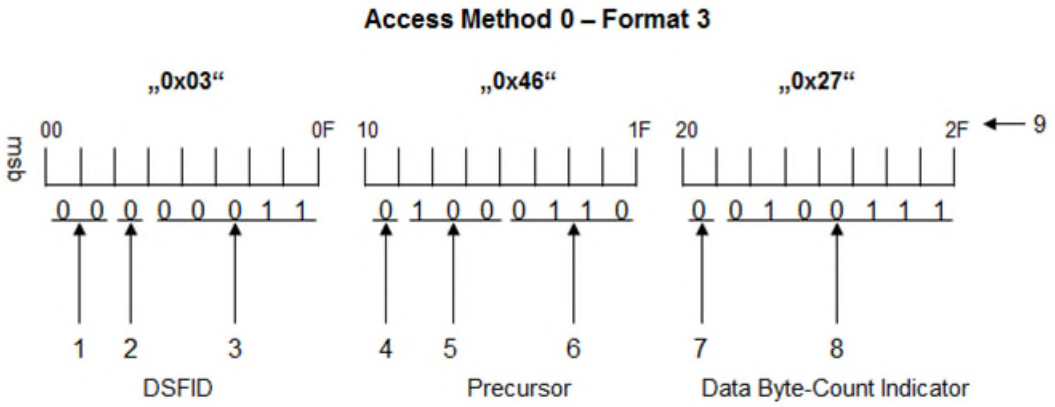
Copyright 2026

2.2.4 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 genannt. 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

Anschließend folgen die Daten, bestehend aus DI und Nutzdaten, die gemäß der zu Beginn gewählten AFI mit 6- oder 8-Bit codiert sind. Die Abbildung 5 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 5: Aufbau von Steuerinformationen in MB 11

Der DSFID beschreibt die Zugriffsmethode und das Datenformat. Verwendet wird die Zugriffsmethode 0, Format 3. Details sind der 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 nachfolgenden 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 2 und 3 verdeutlichen den Sachverhalt.

Die eigentlichen Objekt- und Anwenderdaten werden nach ISO/IEC 15418 mit Hilfe von DI identifiziert und mithilfe von Trennzeichen (GS = „^“) 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

Copyright 2026

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.

Wie auch beim MB 01, werden die Dateninhalte in Abhängigkeit des AFI in der Regel 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 12). Bei einer Datengröße des MB 11 ≤ 1024 Bit ist der User Memory, inklusive der vorangestellten Steuerinformation, wie in der Tabelle 2 aufgebaut.

Copyright 2026

Tabelle 2: 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 Nutzendaten				
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/IEC 17360
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***

Copyright 2026

Tabelle 3: Aufbau der Steuerinformation für 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 Längen-angabe 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*128 + 4b)
4a	Byte Count Indicator Switch	*0(2)*	1 bit	*0(2)* signalisiert, dass nächste 7 bits für Längenangabe der darauffolgenden Daten genutzt werden. Keine weiteren Bytes für Längenangabe (Verkettungsende)
4b	Byte Count Indicator Length	Variable	7 bit	Zweiter Teil der Längenangabe (3b*128 + 4b) Bsp: 3b: ~~1~~0000001 (128 Bytes) 4b: ~~0~~0000010 (2 Bytes) Total Object Length: 130 Bytes
	Subtotal		***32 bits***	

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

2.2.5 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 beabsichtige 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.

Copyright 2026

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* <> „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 6 zeigt das Tag State Diagram nach ISO/IEC 18000-63.

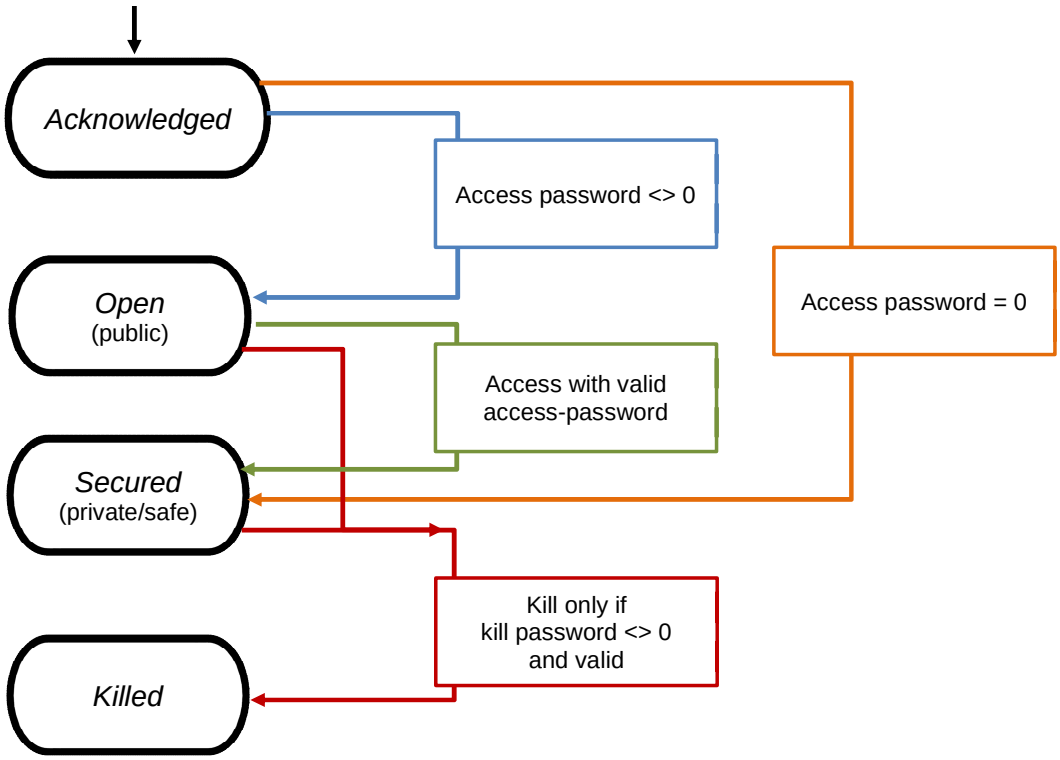


Abbildung 6: Transponderzustände gemäß ISO/IEC 18000-63

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. Die Tabelle 4 zeigt die entsprechenden Lock-Optionen und deren Auswirkungen.

Copyright 2026

Tabelle 4: Lock-Optionen für RFID-Transponder gemäß ISO/IEC 18000-63

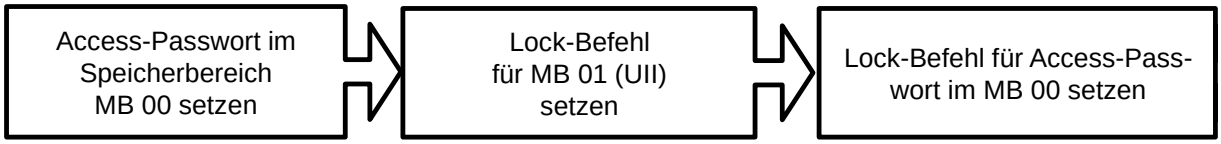
Lock-Optionen	**Auswirkung auf Speicherbereiche MB 01 / MB 11**
Unlocked	Der adressierte Speicherbereich ist in den Zuständen *Open* und *Secured* beschreibbar.
Perma-Unlocked	Der adressierte Speicherbereich ist in den Zuständen *Open* und *Secured* permanent beschreibbar und kann nicht gesperrt werden.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

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 6).

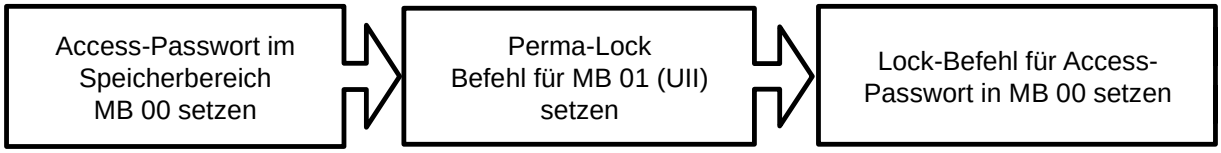
Im Folgenden wird die technische Umsetzung der o.g. Schutzmaßnahmen beschrieben:

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.

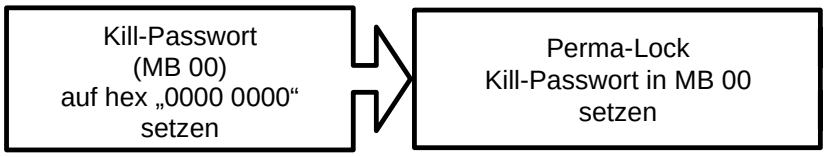
Option 2: Permanenter Schutz des UII (unveränderbar):



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.

Copyright 2026

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. 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.

2.3 Verwendung des RFID-Symbols

Im Rahmen der RFID-Kennzeichnung wird empfohlen zur optischen Markierung das RFID-Emblem nach ISO/IEC 29160 zu verwenden (siehe Abbildung 7).



Abbildung 7: Generisches RFID-Symbol nach ISO/IEC 29160

Darüber hinaus existieren anwendungsspezifische Varianten des RFID-Emblems, die ebenfalls näher in der ISO/IEC 29160 beschrieben sind. Deren Verwendung sollte anwendungsspezifisch abgestimmt werden.

Copyright 2026

2.4 Relevante Standards und Empfehlungen

ISO/IEC	
ISO/IEC 15961-1	Information Technology – Radio Frequency Identification (RFID) for Item Management - Data Protocol: Application Interface
ISO/IEC 15962	Information Technology - Radio Frequency Identification (RFID) for Item Management - Data Protocol: Data Encoding Rules and Logical Memory Functions
ISO/IEC 17360	Automatic identification and data capture techniques - Supply chain applications of RFID - Product tagging, product packaging, transport units, returnable transport units and returnable packaging items
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
Odette	
B21/LR05	RFID Item Level Standard
LR02	RFID in Vehicle Distribution Processes
LR03	RFID for Tracking of Parts and Assemblies
LR07	Implementing RFID in the Automotive Supply Chain
VDA	
5501	RFID-Einsatz im Behältermanagement
5509	RFID-Einsatz und Datentransfer zur Verfolgung von Bauteilen und Komponenten in der Fahrzeugentwicklung
5510	RFID zur Verfolgung von Teilen und Baugruppen in der Automobilindustrie
5520	RFID-Einsatz in der Fahrzeugdistribution
5540	Zulassungsbedingungen für RFID-Transponder

Copyright 2026

3 Near Field Communication (NFC)

NFC ist eine RFID-Technologie zur drahtlosen Datenübertragung über kurze Distanzen (typisch <10 cm) im Frequenzbereich von 13,56 MHz. Sie basiert auf dem ISO/IEC 14443 Standard und ermöglicht den Austausch von Daten zwischen einem NFC-Tag (passives Medium) und einem NFC-Lesegerät (aktives Medium).

NFC wird vor allem im Bereich der Bezahlsysteme verwendet. In industriellen Anwendungen wird NFC zunehmend zur eindeutigen Kennzeichnung von Objekten eingesetzt. Die Vorteile liegen in der einfachen Handhabung, kontaktlosen Auslesbarkeit, Beständigkeit gegen Verschmutzung sowie der Möglichkeit zur Speicherung strukturierter Daten in standardisierter Form mit dem NFC Data Exchange Format (NDEF).

NFC kann zur Kennzeichnung von Objekten verwendet werden, und kann in Koexistenz mit anderen Kennzeichnungsverfahren wie Ultra High Frequency (UHF) RFID oder optischer Kennzeichnungen verwendet werden. Ziel ist es, die Möglichkeit der Verwendung von NFC zur Kennzeichnung von Objekten im Automotive-Umfeld aufzuzeigen, ohne auf die vielfältigen Möglichkeiten und Anwendungsfälle der NFC-Technologie im Detail einzugehen. Dazu wird auf einschlägige Literatur, Dokumente und Standards des NFC-Forums verwiesen.

3.1 Technische Anforderungen

3.1.1 NFC-Tag Types

Es gibt fünf verschiedene Tag Types, die in der Tabelle 5 aufgelistet sind. Deren Verwendung stellt die Interoperabilität der NFC-Devices sicher. Die Types unterscheiden sich hinsichtlich Speicherkapazität, Übertragungsgeschwindigkeit und Kompatibilität. Die Auswahl des geeigneten Tag Types erfolgt in Abhängigkeit von der Anwendung, der benötigten Speichermenge und den Umgebungsbedingungen.

Für die Verwendung im Automotive-Umfeld bzgl. Objektkennzeichnung sind vor allem die Tag Types 2 und 5 etabliert. Durch die Einführung des Tag Types 2 ist der Type 1 überholt. Dieser findet jedoch in Einzelfällen noch Anwendungen.

Für die Auswahl des Tags ist die Applikation maßgeblich.

- Wird NFC zur Kennzeichnung von Objekten verwendet, können die Tag Typen (1), 2 und 5 empfohlen werden. Hier können Objektnummern analog zur optischen Kennzeichnung (1D, 2D-Codes) eingesetzt werden. Starke Verschlüsselungen und Sicherheitsmaßnahmen werden in der Regel nicht benötigt. Zudem gibt es hier eine Vielzahl geeigneter Tags und Labels.
- Bei Zutrittssystemen (z.B. Digital Key Cards) sind starke Verschlüsselungen notwendig. Hier können Tags aus der Kategorie Tag Type 4 empfohlen werden.

Copyright 2026

Tabelle 5: Übersicht der NFC-Tag Types

Tag Type	Standard	Speicher	Datenübertragungsrate	Features
1	ISO/IEC 14443 kompatibel	Von 96 Byte bis 2 KByte	Bis zu 106 kbit/s	Mehrfach beschreibbar Schreibschutz
2	Wie Typ 1, ISO/IEC 14443 kompatibel	Von 48 Byte bis 2 KByte	Bis zu 106 kbit/s	Mehrfach beschreibbar Schreibschutz Geringe Kosten Weit verbreitet
3	JIS X 6319-4 FeliCa	9 kb(bis theor. 1MB)	Bis zu 212 kbit/s	Tags sind vorkonfiguriert als mehrfach beschreibbar oder read only Hoche Speicherkapazität und Übertragungsraten
4	ISO/IEC 14443	Theoretische Größe bis zu 32 kb	Bis zu 424 kbit/s	Vorkonfiguriert als mehrfach beschreibbar oder read only Security und Verschlüsse-lung Authentifizierung Flexible Datenstrukturen
5	ISO/IEC 15693	Unterschiedliche Speichergrößen	-Typisch: ~26kbit/s Optional: ~53 kbit/s	User-Memory wird verwen-det Blockweise Locking Weitere Lesedistanz Geringe Datenraten

Verbreitete Typen in der Objektkennzeichnung

Copyright 2026

3.1.2 NDEF-Record Types

Die Tabelle 6 zeigt, die vom NFC-Forum definierten NDEF-Record Types.

Tabelle 6: Übersicht der NDEF-Record Types

Record Type	Beschreibung	Vollständige URN	Spezifikation
Di	Device Information	urn:nfc:wkt:Di	Device Information Record Type Definition
Gc	Generic Control (zurückgezogen)	urn:nfc:wkt:Gc	Generic Control Record Type Definition (withdrawn)
Hc	Handover Carrier	urn:nfc:wkt:Hc	Connection Handover
Hi	Handover Initiate	urn:nfc:wkt:Hi	Connection Handover
Hm	Handover Mediation	urn:nfc:wkt:Hm	Connection Handover
Hr	Handover Request	urn:nfc:wkt:Hr	Connection Handover
Hs	Handover Select	urn:nfc:wkt:Hs	Connection Handover
Mr	Money Transfer Response	urn:nfc:wkt:Mr	NFC Money Transfer
Mt	Money Transfer Request	urn:nfc:wkt:Mt	NFC Money Transfer
PHD	Personal Health Device	urn:nfc:wkt:PHD	Personal Health Device Communication
Sig	Signature	urn:nfc:wkt:Sig	Signature Record Type Definition
Sp	Smart Poster	urn:nfc:wkt:Sp	Smart Poster Record Type Definition
T	Text	urn:nfc:wkt:T	Text Record Type Definition
Te	TNEP Status	urn:nfc:wkt:Te	Tag NDEF Exchange Protocol
Tp	Service Parameter	urn:nfc:wkt:Tp	Tag NDEF Exchange Protocol
Ts	Service Select	urn:nfc:wkt:Ts	Tag NDEF Exchange Protocol
U	URI	urn:nfc:wkt:U	URI Record Type Definition
V	Verb	urn:nfc:wkt:V	Verb Record Type Definition
WLCCAP	WLC Capability	urn:nfc:wkt:WLCCAP	Wireless Charging
WLCCTL	WLC Listen Control	urn:nfc:wkt:WLCCTL	Wireless Charging
WLCFOD	WLC JiFOD	urn:nfc:wkt:WLCFOD	Wireless Charging
WLCINF	WLC Poll Information	urn:nfc:wkt:WLCINF	Wireless Charging

Zur Objektkennzeichnung geeignete Typen

3.1.3 Verwendung von NDEF-Records zur Objektkennzeichnung

3.1.3.1 Text Record

Der Text Record dient zur Ablage von reinen Textinformationen. Die Nutzdaten enthalten:

- Sprachkennung (z.B. "de" für Deutsch)
- Textinhalt (UTF-8-kodiert)

Zur Objektkennzeichnung kann der Text Record genutzt werden, um die gleiche Datenstruktur wie im Data Matrix Code gemäß Kapitel 6 zu speichern.

Copyright 2026

3.1.3.2 URI Record

Der Uniform Resource Identifier (URI) Record ermöglicht die Ablage einer Uniform Resource Locator (URL). Diese kann genutzt werden, um auf eine webbasierte Datenquelle zu verweisen, in der die Identifikations- oder Objektdaten hinterlegt sind.

Beispielhafte URL:
https://Beispiel.com/Wartungsplan.pdf

Diese Variante ist insbesondere für Anwendungen geeignet, in denen eine Online-Datenbank zur Objektrückverfolgung existiert (bspw. DPP). Hierzu gibt es aktuell keine standardisierte Form und ist somit individuell vom Anbieter abhängig.

Hinweis
Die Verwendung von NFC-Tags zur Objektkennzeichnung bietet eine standardisierte, robuste und zukunftssichere Lösung. Durch die Nutzung des NDEF-Formats können die im Data Matrix Code definierten Datenstrukturen direkt übernommen werden. Die Unterstützung von Text- und URI-Records ermöglicht eine flexible Integration in bestehende Prozesse und Systeme.

Copyright 2026

3.1.4 Aufbau von NFC-Chips und Nutzung von Speicherbereichen

Die Speicherkonfiguration wird im NXP Data Sheet anhand des NFC-Chips NTAG213 dargestellt:

Datenblock			**Inhalt**				**Beschreibung**
DB	0		Int	Int	Int	Int	UID
DB	1		Int	Int	Int	Int	UID
DB	2		Int	Int	Lock 0	Lock 1	UID / internal
DB	3		CC	10	12	00	Capability Container
DB	4		SD	SD	SD	SD	Static Memory
DB	5		SD	SD	SD	SD	Static Memory
DB	6		SD	SD	SD	SD	Static Memory
DB	7		SD	SD	SD	SD	Static Memory
DB	8		SD	SD	SD	SD	Static Memory
DB	9		SD	SD	SD	SD	Static Memory
DB	10		SD	SD	SD	SD	Static Memory
DB	11		SD	SD	SD	SD	Static Memory
DB	12		SD	SD	SD	SD	Static Memory
DB	13		SD	SD	SD	SD	Static Memory
DB	14		SD	SD	SD	SD	Static Memory
DB	15		SD	SD	SD	SD	Static Memory
DB	16		DD	DD	DD	DD	Dynamic Memory
DB	17		DD	DD	DD	DD	Dynamic Memory
DB	18		DD	DD	DD	DD	Dynamic Memory
DB	19		DD	DD	DD	DD	Dynamic Memory
DB	20		DD	DD	DD	DD	Dynamic Memory
DB	21		DD	DD	DD	DD	Dynamic Memory
DB	22		DD	DD	DD	DD	Dynamic Memory
DB	23		DD	DD	DD	DD	Dynamic Memory
DB	24		DD	DD	DD	DD	Dynamic Memory
DB	25		DD	DD	DD	DD	Dynamic Memory
DB	26		DD	DD	DD	DD	Dynamic Memory
DB	27		DD	DD	DD	DD	Dynamic Memory
DB	28		DD	DD	DD	DD	Dynamic Memory
DB	29		DD	DD	DD	DD	Dynamic Memory
DB	30		DD	DD	DD	DD	Dynamic Memory
DB	31		DD	DD	DD	DD	Dynamic Memory
DB	32		DD	DD	DD	DD	Dynamic Memory
DB	33		DD	DD	DD	DD	Dynamic Memory
DB	34		DD	DD	DD	DD	Dynamic Memory
DB	35		DD	DD	DD	DD	Dynamic Memory
DB	36		DD	DD	DD	DD	Dynamic Memory
DB	37		DD	DD	DD	DD	Dynamic Memory
DB	38		DD	DD	DD	DD	Dynamic Memory
DB	39		DD	DD	DD	DD	Dynamic Memory
DB	40		LL	LL	LL	LL	Dynamic Lock

Copyright 2026

Folgendes Bedatungsbeispiel zeigt den Speicherinhalt in 8-bit ASCII für einen Type-2 Tag für die Teilenummer gem. VDA 5509.

[)><RS>06<GS>37SUN123456789 5Q1721095BK+123456789<RS><EOT>

Hier wird der Speicher ab Datenblock „3“ beschrieben. In den Blöcken „0“ bis „2“ sind UID und Systemdaten gespeichert.

Datenblock	Inhalt (hexadezimal)	Inhalt (ASCII)
[03]	E1 10 12 00	|····|
[04]	03 34 D1 01	|·4··|
[05]	30 54 02 64	|0T·d|
[06]	65 5B 29 3E	|e[)>|
[07]	1E 30 36 1D	|·06·|
[08]	33 37 53 55	|37SU|
[09]	4E 31 32 33	|N123|
[0A]	34 35 36 37	|4567|
[0B]	38 39 20 35	|89 5|
[0C]	51 31 37 32	|Q172|
[0D]	31 30 39 35	|1095|
[0E]	42 4B 2B 31	|BK+1|
[0F]	32 33 34 35	|2345|
[10]	36 37 38 39	|6789|
[11]	1E 04 FE 00	|····|

Folgendes Bedatungsbeispiel zeigt den Speicherinhalt in 8-bit ASCII für einen Type-5 Tag für die Teilenummer gem. VDA 5509. Hier wird das Usermemory ab Datenblock “0” beschrieben.

Datenblock	Inhalt (hexadezimal)	Inhalt (ASCII)
[00]	E1 10 12 00	|····|
[01]	03 34 D1 01	|·4··|
[02]	30 54 02 64	|0T·d|
[03]	65 5B 29 3E	|e[)>|
[04]	1E 30 36 1D	|·06·|
[05]	33 37 53 55	|37SU|
[06]	4E 31 32 33	|N123|
[07]	34 35 36 37	|4567|
[08]	38 39 20 35	|89 5|
[09]	51 31 37 32	|Q172|
[0A]	31 30 39 35	|1095|
[0B]	42 4B 2B 31	|BK+1|
[0C]	32 33 34 35	|2345|
[1D]	36 37 38 39	|6789|
[1E]	1E 04 FE 00	|····|

Copyright 2026

3.2 Relevante Standards und Empfehlungen

Im Folgenden ist eine Übersicht über themenverwandte und -relevante Empfehlungen und Standards hinsichtlich NFC aufgeführt.

ISO/IEC	
ISO/IEC 14443, 1-4	Cards and security devices for personal identification — Contactless proximity objects
ISO/IEC 15693	Cards and security devices for personal identification — Contactless vicinity objects
ISO/IEC 18092	Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol 1 (NFCIP-1) Grundlegendes • Frequenz: 13,56 MHz (wie bei ISO/IEC 14443) • Reichweite: wenige Zentimeter (typisch 0–5 cm, max. ca. 10 cm) • Datenraten: 106, 212 und 424 kbit/s • Kommunikationsarten: ▪ Aktiv: Beide Geräte erzeugen ihr eigenes RF-Feld ▪ Passiv: Nur ein Gerät (Initiator) erzeugt das RF-Feld, das andere (Target) nutzt dieses Feld zur Antwort Typische Betriebsarten nach ISO/IEC 18092 • Reader/Writer-Mode: NFC-Gerät liest oder beschreibt NFC-Tags (z. B. Werbeposter mit NFC-Tag) • Card Emulation Mode: NFC-Gerät verhält sich wie eine kontaktlose Smartcard (z. B. Smartphone als Kreditkarte im Payment) • Peer-to-Peer Mode: Zwei NFC-Geräte tauschen Daten direkt aus (z. B. Dateiübertragung, Bluetooth-Pairing)
NFC Forum	Release Candidate Specification DPP Text Record Type Definition Technical Specification
NFC Data Exchange Format (NDEF)	Technical Specification, NFC Forum, Revision 1.0, July 24, 2006
NFC Record Type Definition (RTD)	Technical Specification, NFC Forum, RTD 1.0, July 24, 2006
Text Record Type Definition	Technical Specification, NFC Forum, RTD-Text 1.0, July 24, 2006
URI Record Type Definition	Technical Specification, NFC Forum, RTD-URI 1.0, July 24, 2006

Type 1 Tag Operation Specification, July 9, 2007

Type 2 Tag Operation Specification, July 9, 2007

Type 3 Tag Operation Specification, August 16, 2007

Type 4 Tag Operation Specification, March 13, 2007

Type 5 Technical Specification, April 27, 2018

Copyright 2026

4 Bluetooth Low Energy (BLE)

Das folgende Kapitel setzt sich mit der Nutzung von BLE-Beacons auseinander. In der Technologie-Landschaft haben sich Big Tech Anbieter auf unterschiedliche Vorgehensweisen bei der Nutzung dieser Technologie spezialisiert. Dies birgt jedoch das Risiko von Lock-in-Effekten, die die Flexibilität und Anpassungsfähigkeit der Anwender erheblich einschränken können.

Neben der technischen Beschreibung der relevanten Datenpakete werden auch die physikalischen Anforderungen behandelt, die insbesondere im Einsatz in der Automobilbranche unabdingbar sind. Diese Anforderungen sind essenziell, um eine reibungslose Integration und einen zuverlässigen Betrieb der Systeme sicherzustellen.

Es gilt zu beachten, dass die Nutzungsempfehlungen einzelner proprietärer Anbieter durchaus spezifische Vorteile bieten können. Diese potenziellen Vorteile müssen jedoch im jeweiligen Projektkontext individuell bewertet und entschieden werden. Im Rahmen dieser allgemeinen Empfehlung werden solche spezifischen Vergleiche bewusst nicht näher betrachtet.

4.1 Technische Anforderungen

4.1.1 Funktionsweise von BLE-Systemen/-Beacons

BLE-Beacons sind kompakte, batteriebetriebene Geräte, die in regelmäßigen Abständen drahtlose Signale aussenden. Diese Signale enthalten eine eindeutige ID sowie zusätzliche Informationen wie die Sendeleistung. Die Beacons werden häufig zur Lokalisierung von Objekten wie Behältern eingesetzt und ermöglichen eine präzise Standortbestimmung in unterschiedlichsten Umgebungen.

BLE-Beacons senden kontinuierlich Signale (Advertising Pakete) aus, die von Empfängern wie Smartphones, Tablets oder speziellen Gateways erfasst werden können. Diese Empfänger messen die Signalstärke (RSSI – Received Signal Strength Indicator), um die ungefähre Entfernung zum Beacon zu bestimmen. Die Signalstärke nimmt ab, je weiter der Empfänger vom Beacon entfernt ist.

Zur Lokalisierung von Behältern werden in der Regel stationäre Gateways in einem definierten Bereich platziert. Mithilfe verschiedener Methoden kann die Position eines Behälters ermittelt werden. Dabei reicht die Genauigkeit von der einfachen Erfassung der Anwesenheit bis zur auf bis zu wenigen Metern genauen Erfassung der Position.

4.1.1.1 Anwendung in der Behälterlokalisierung

BLE-Beacons werden in verschiedenen Szenarien eingesetzt, um Behälter effizient zu lokalisieren. Folgend sind einige Beispiele genannt.

- Lagerumgebungen:
  Beacons können in großen Lagerhallen verwendet werden, um Behälter zu identifizieren und ihren Standort zu überwachen. Dies erleichtert die Navigation und Bestandsverwaltung.

- Transportketten:
  Während des Transports können Beacons den Standort eines Behälters kontinuierlich überwachen, indem sie mit mobilen Empfängern oder fest installierten Gateways entlang der Route kommunizieren.

- Produktionsumgebungen:
  In Fertigungsanlagen ermöglichen Beacons die Verfolgung von Behältern innerhalb von Produktionslinien, wodurch Prozesse besser koordiniert werden können.

Copyright 2026

4.1.1.2 Lokalisierungsmethoden und Planungsaspekte

Die Wahl der Lokalisierungsmethoden muss, neben der Platzierung der Beacons am zu lokalisierenden Objekt, bereits bei der Planung eines BLE-basierten Lokalisierungssystems berücksichtigt werden, da sie entscheidend für die Effizienz und Genauigkeit des Systems ist:

- Proximity Detection (Present Detection):
  Diese Methode erkennt, ob ein Behälter sich in der Nähe eines bestimmten Gateways befindet. Es muss sichergestellt werden, dass die Gateways strategisch platziert werden, um ein ausreichendes Abdeckungsgebiet zu gewährleisten.

- Trilateration:
  Diese Methode nutzt die Signalstärke mehrerer Gateways, um den Standort zu berechnen. Für eine präzise Lokalisierung ist eine durchdachte Platzierung und Dichte der Gateways erforderlich. Hindernisse wie Wände oder Metallstrukturen sollten bei der Planung berücksichtigt werden.

- Triangulation, Angle of Arrival (AoA):
  Hierbei wird die Position eines Behälters durch Winkelmessungen von idealerweise mehr als zwei Gateways bestimmt. Diese Methode erfordert, dass die Gateways an bekannten, festen Positionen angebracht werden. Eine sorgfältige Planung der Gateway-Standorte ist notwendig, um präzise Winkelmessungen und damit eine möglichst genaue Lokalisierung sicherzustellen.

4.1.1.3 Erfassung mehrerer Beacons

Ein signifikanter Vorteil von BLE-Beacons ist die Möglichkeit, innerhalb kurzer Zeit viele Beacons gleichzeitig zu erfassen. Aufgrund der geringen Energiekosten der BLE-Technologie können Empfänger schnell und effizient Signale von mehreren Beacons in der Umgebung scannen. Dies ist besonders nützlich in dynamischen Umgebungen wie Lagerräumen oder bei der Verfolgung von Behältern, bei denen sich viele Objekte gleichzeitig bewegen. Die Fähigkeit, eine große Anzahl von Beacons gleichzeitig zu erfassen, ermöglicht eine schnelle und präzise Positionierung, was zu einer verbesserten Effizienz und einer optimierten Bestandsverwaltung führt.

BLE-Beacons sind somit eine leistungsfähige Technologie, um Behälter in Lagerhäusern, Produktionsstätten oder während des Transports zu lokalisieren. Eine fundierte Planung, die die gewählten Lokalisierungsmethoden berücksichtigt, ist entscheidend für die Effizienz des Systems und ermöglicht eine präzise Standortbestimmung, die individuell auf die jeweilige Umgebung und Anwendung abgestimmt werden kann.

4.1.2 Luftschnittstelle und Frequenzbereiche

BLE-Beacons nutzen die 2,4-GHz ISM-Band-Luftschnittstelle (Industrial, Scientific, and Medical Band) zur drahtlosen Kommunikation. Dieses Band ist weltweit lizenzfrei und eignet sich ideal für kurze bis mittlere Distanzen sowie energieeffiziente Anwendungen. Wie bereits angeführt, basiert BLE auf dem Low Energy-Standard der SIG[1], der speziell für geringe Energieanforderungen bei gleichzeitig zuverlässiger Signalübertragung entwickelt wurde.

4.1.2.1 Luftschnittstelle

Die Luftschnittstelle beschreibt, wie Signale zwischen Sender (Beacon) und Empfänger übertragen werden. BLE-Beacons senden sogenannte Advertising-Pakete, die kleine Datenmengen wie die Beacon-ID, Sendeleistung und Statusinformationen enthalten. Diese Pakete werden in regelmäßigen Intervallen ausgesendet, die angepasst werden können, um entweder Energie zu sparen oder die Sichtbarkeit zu erhöhen. Die Übertragung erfolgt auf spezifischen Kanälen innerhalb des 2,4-GHz-Bands, um eine stabile und effiziente Kommunikation zu gewährleisten. Technisch basiert BLE auf der Bluetooth Core Specification, die sicherstellt, dass die Kommunikation zwischen Geräten interoperabel und zuverlässig ist. Zudem halten

[1] Bluetooth Technology Website - Specifications and documents (Stand 18.05.2026)

Copyright 2026

BLE-Beacons die in der IEEE 802.15.1 festgelegten Standards ein, welche die grundlegenden Anforderungen für die Funkübertragung und Frequenznutzung definieren.

4.1.2.2 Kanalbelegung und Frequenzbereiche

Das 2,4-GHz-Band ist bei BLE in insgesamt 40 Kanäle mit einer Bandbreite von je 2 MHz unterteilt. Diese Kanäle sind in zwei Gruppen aufgeteilt.

- Advertising-Kanäle:
  Die Kanäle 37, 38 und 39 werden speziell für das Senden der oben genannten Advertising-Pakete genutzt. Diese Kanäle sind essenziell für die initiale Erkennung von Beacons durch Empfänger.

- Datenkanäle:
  Die Kanäle 0 bis 36 werden für die Übertragung von Daten nach dem Aufbau einer Verbindung verwendet. Sie ermöglichen die Kommunikation zwischen einem Beacon und einem Empfänger, wenn etwa zusätzliche Informationen ausgetauscht werden sollen.

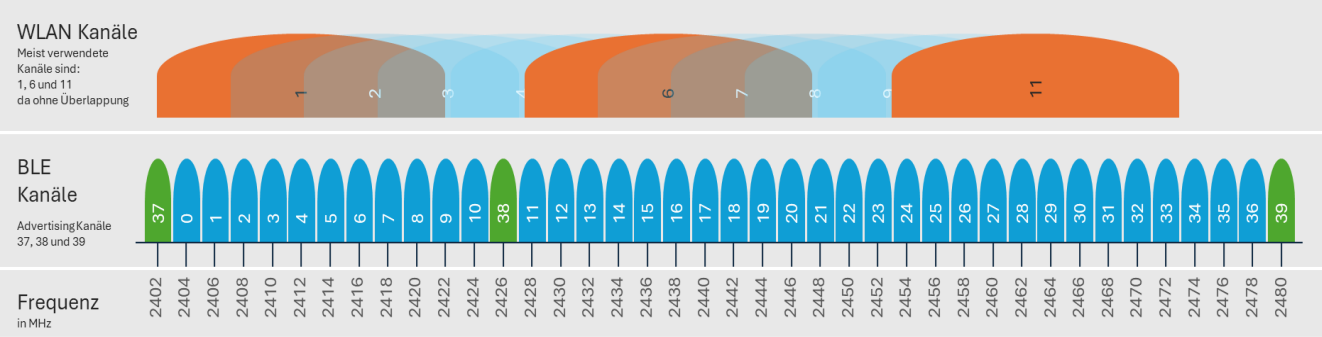


Abbildung 8: Advertising-Kanäle innerhalb des 2,4-GHz-Frequenzbandes

Die Abbildung 8 zeigt, dass die Advertising-Kanäle strategisch innerhalb des 2,4-GHz-Bands verteilt sind, um Störungen durch andere drahtlose Technologien wie bspw. WLAN zu minimieren. BLE verwendet zudem eine Frequenzsprungtechnik (Frequency Hopping Spread Spectrum, FHSS), bei der das Signal zwischen verschiedenen Kanälen wechselt. Dies verbessert die Signalqualität und reduziert Interferenzen in Umgebungen mit vielen Funksignalen.
Durch die kontinuierliche Weiterentwicklung der BLE-Versionen wird die Technologie immer leistungsfähiger und vielseitiger, was BLE-Beacons zu einer geeigneten Lösung für innovative und energieeffiziente Lokalisierungssysteme macht.

4.1.3 Definition des Advertising Type

Der Advertising Type im BLE-Standard definiert die Art und Weise, wie ein Gerät Werbepakete Advertising-Pakete sendet und wie es mit anderen Geräten interagiert. Er bestimmt, ob und wie ein Gerät von anderen gefunden, gescannt oder verbunden werden kann. Der Advertising Type umfasst dabei folgende Hauptaufgaben:

Bestimmung der Verbindungsfähigkeit
Der Advertising Type legt fest, ob das Gerät Verbindungen zu anderen BLE-Geräten zulässt oder nur Daten übermittelt.

Connectable Advertising:
Das Gerät erlaubt Verbindungen.

Non-Connectable Advertising:
Verbindungen werden nicht akzeptiert.

Steuerung des Werbeverhaltens
Der Advertising Type bestimmt, ob das Gerät nur Broadcasts sendet oder auch auf Scan-Anfragen von Scannern reagiert.

Copyright 2026

Scannable Advertising: Das Gerät kann auf Anfragen antworten und zusätzliche Informationen im Scan Response bereitstellen.	Non-Scannable Advertising: Es werden nur die Werbepakete gesendet (keine Antworten auf Scan-Anfragen).

Festlegung der Zielausrichtung
Der Advertising Type definiert, ob die Werbepakete an ein spezifisches Gerät gerichtet sind oder an alle Geräte in Reichweite.

Directed Advertising: Pakete sind für ein bestimmtes Gerät bestimmt (z. B. für schnelles Re-Pairing).	Undirected Advertising: Pakete werden an alle Geräte in der Umgebung gesendet.

Optimierung von Energieverbrauch und Performance
Unterschiedliche Advertising Types sind so konzipiert, dass sie je nach Anwendung Energie sparen können (z. B. Non-Connectable Advertising für Beacons). Dies ist relevant für batteriebetriebene Geräte.

Unterstützung spezifischer Anwendungsfälle
Der Advertising Type ermöglicht die Anpassung an verschiedene Szenarien, Beispiele sind:
- Beacons senden Standortdaten im Non-Connectable Modus
- Fitness-Tracker erlauben Verbindungen im Connectable Modus
- Geräte Re-Pairing nutzen Directed Advertising für schnelle Wiederverbindungen.

4.1.3.1Aufbau und Größe der Advertising Pakete

Ein BLE Advertising Paket besteht aus mehreren Komponenten, die in einer festgelegten Reihenfolge angeordnet sind. Diese sind wie folgt:

1. Preamble (1 Byte)
   Die Präambel dient der Synchronisation zwischen Sender und Empfänger. Sie ermöglicht es dem Empfänger, sich auf das Signal des Beacons einzustellen.

2. Access Address (4 Byte)
   Diese Adresse ist für Advertising-Pakete fest auf `0x8E89BED6` gesetzt und dient der Identifikation des Kanals für die Übertragung. Sie stellt sicher, dass das Paket als BLE-Advertising-Paket erkannt wird.

3. Advertising Header (2 Byte)
   Der Header enthält grundlegende Informationen über das Paket:
   - PDU Type (4 Bit): Gibt den Pakettyp an, z. B. `ADV_IND` (Connectable Advertising Packet) oder `ADV_NONCONN_IND` (Non-Connectable Advertising Packet).
   - TX Add (1 Bit): Gibt an, ob die Adresse des Senders (TX Address) eine öffentliche oder zufällige Adresse ist. Ein Wert von `0` bedeutet, dass es sich um eine öffentliche Adresse handelt, während `1` eine zufällige Adresse angibt.
   - RX Add (1 Bit): Gibt an, ob die Adresse des Empfängers (RX Address) ebenfalls öffentlich oder zufällig ist. Ebenso bedeutet ein Wert von `0` eine öffentliche Adresse und ein Wert von `1` eine zufällige Adresse.
   - RFU (Reserviert für spätere Erweiterungen, 2 Bit):
   - Length (6 Bit): Gibt die Länge des folgenden Payloads an (0 bis 37 Byte).

Copyright 2026

4. Payload (0–37 Byte)
   Der Payload ist der zentrale Teil des Advertising-Pakets und enthält die eigentlichen Daten, darunter die Beacon-ID. Der Payload kann verschiedene Felder enthalten, abhängig von den Anforderungen des Beacons:
   - MAC-Adresse (6 Byte):
     Die ersten 6 Byte des Payloads repräsentieren die MAC-Adresse des Beacons, die eine eindeutige Identifikation im Netzwerk ermöglicht. Diese Adresse kann als öffentliche oder zufällige Adresse kodiert werden, je nach Typ des Beacons.
   - Manufacturer Specific Data (bis zu 31 Byte):
     Dieser Bereich des Payloads ist flexibel und für herstellerspezifische Daten vorgesehen. Er umfasst:
     - AD Length (1 Byte):
       Gibt die Länge der nachfolgenden Daten in Byte an, die in diesem Feld enthalten sind, und informiert den Empfänger über die erwartete Datenmenge.
     - Advertising Type (1 Byte):
       Dieses Feld gibt an, welche Art von Daten im Bereich der Manufacturer Specific Data enthalten ist. Der Advertising Type kann beispielsweise angeben, ob es sich um Beacon-Informationen, Telemetriedaten, Sensordaten oder andere herstellerspezifische Inhalte handelt. Bestimmte Werte können verwendet werden, um den Typ der Daten weiter zu spezifizieren, wodurch der Empfänger die Informationen korrekt verarbeiten kann.
     - Kundenindividuelle Daten:
       Hier können herstellerspezifische und anwendungsspezifische Informationen eingefügt werden, die je nach Bedarf des Unternehmens variieren können. Dies ermöglicht eine flexible Anpassung und Erweiterung der Funktionalität der Beacons nach individuellen Anforderungen.

5. CRC (Cyclic Redundancy Check, 3 Byte)
   Der CRC-Wert wird verwendet, um die Integrität des Pakets zu überprüfen. Er hilft festzustellen, ob das Paket während der Übertragung beschädigt wurde.

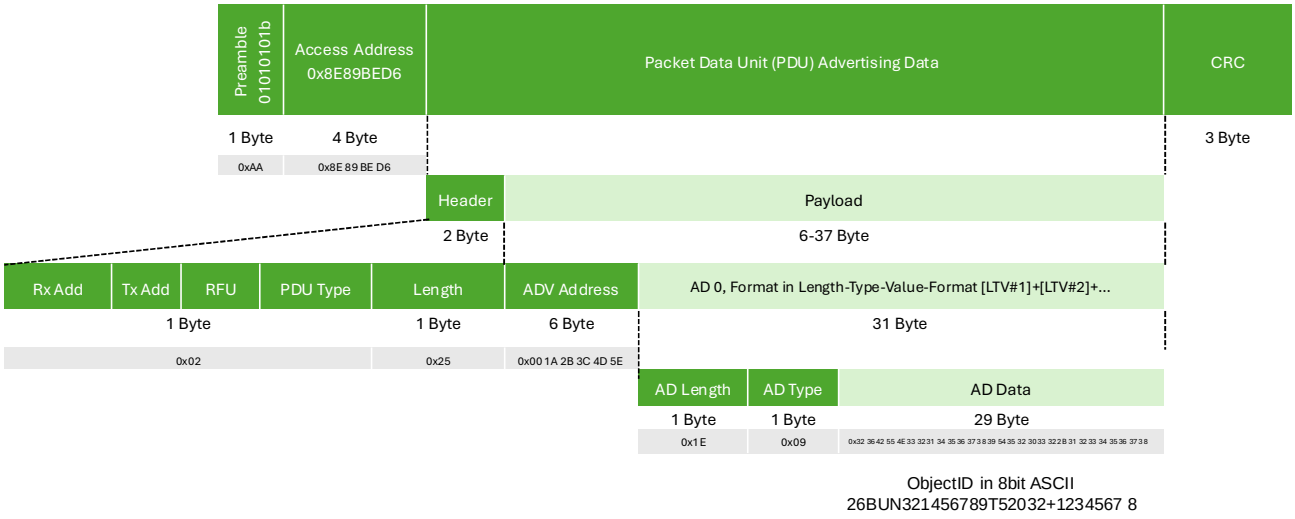


Abbildung 9: Beispiel eines BLE Legacy Advertising Pakets

Die Abbildung 9 zeigt beispielhaft, wie ein BLE Advertising Paket aufgebaut ist. Dieses ist speziell darauf ausgelegt, kleine Datenmengen wie die Beacon-ID effizient zu übertragen. Es besteht aus einer festen Struktur, die Synchronisation (Preamble), Kanalzuordnung (Access Address), Paketinformationen (Header), Daten (Payload) und Fehlerprüfung (CRC) umfasst. Der Bereich für Manufacturer Specific Data bietet Flexibilität und ermöglicht es Unternehmen, kunden- oder anwendungsspezifische Informationen in das Paket zu integrieren. Dies macht BLE-Beacons zu einer vielseitigen Lösung für unterschiedlichste Anwendungsfälle.

Copyright 2026

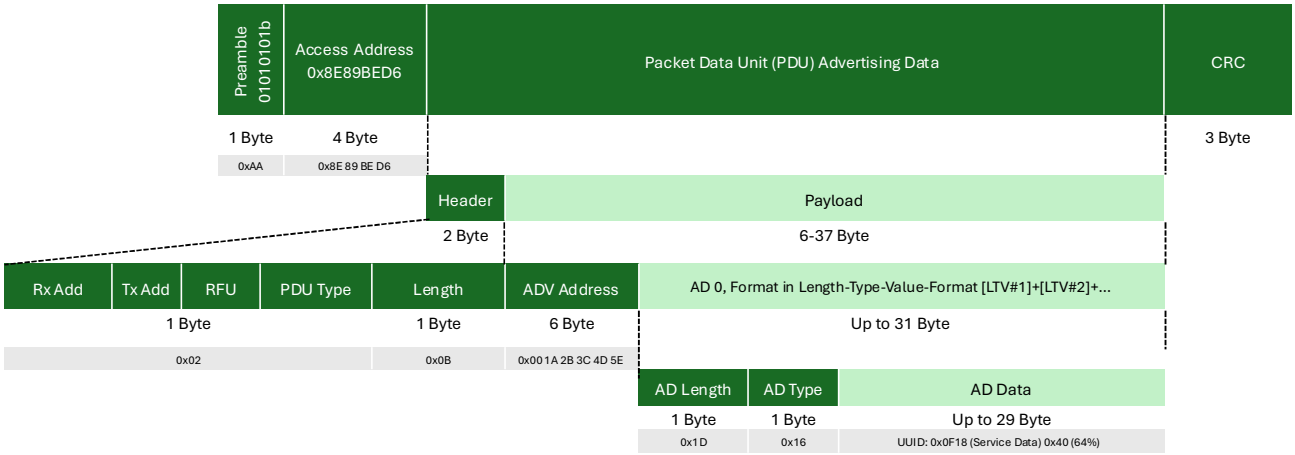


Abbildung 10: Beispiel eines BLE Diagnostic Advertising Pakets

Die Abbildung 10 zeigt beispielhaft den Aufbau eines BLE Advertising Pakets zur Übertragung von Service Data. Über den AD Type 0x16 werden die nachfolgenden Daten als Service Data gekennzeichnet. Der Bereich AD Data ermöglicht anschließend die Übertragung einer UUID sowie zugehöriger anwendungsspezifischer Daten. Dadurch können BLE-Beacons standardisierte Services eindeutig kennzeichnen und gleichzeitig spezifische Informationen innerhalb des Advertising Pakets übertragen.

4.1.4 Beschreibung der Advertising Pakete

Bei der Planung ist es essenziell, die maximale Energieeffizienz zu gewährleisten. Da BLE-Beacons für ihren geringen Energieverbrauch bekannt sind, ist es wichtig, Übertragungsintervalle und die Menge der gesendeten Daten so zu optimieren, dass der Energieverbrauch minimiert wird, ohne die Funktionalität zu beeinträchtigen. Das bedeutet, dass nur die wirklich benötigten Daten in den definierten Intervallen übertragen werden sollten. Für die Lokalisierung von Objekten wie Ladungsträgern empfiehlt der VDA deshalb die Verwendung von zwei unterschiedlichen Advertising-Paketen. Diese lauten wie folgt:

1. **Legacy Advertising**
   Das Legacy-Advertising-Paket enthält die Object-ID gemäß der VDA-Empfehlung 5014

2. **Diagnostic Advertising**
   Das Diagnostic-Advertising-Paket enthält Informationen wie die aktuelle Batteriespannung, den Hersteller und Typ des Beacons sowie Sensordaten wie Temperatur und möglicherweise andere Messdaten

Der Aufbau der Advertising-Pakete folgt den Spezifikationen der SIG. Es wird der Advertising-Typ 0x02 – „Non Scannable Undirected Advertising“ (ADV_NONCONN_IND) verwendet. Dieser Typ ermöglicht es, dass die Werbepakete von allen Geräten empfangen werden können, während er gleichzeitig einen optimalen Energieverbrauch bietet.

4.1.4.1 Legacy Advertising

Die Tabelle 7 zeigt wie das Legacy Advertising Paket strukturiert ist. Per Grundeinstellung wird dies alle 5 Sekunden wiederholt.

Copyright 2026

Tabelle 7: Struktur des Legacy Advertising Pakets

Komponente	Beschreibung	Länge	Beispiel
Preamble	Startsequenz (fest vorgegeben)	1 Byte	0xAA
Access Address	Access Address (fest vorgegeben)	4 Byte	0x8E 89 BE D6
Header			
PDU Type	PDU Type “non-connectable undirect advertising”	4 Bit	0b00 10
RFU	Reserviert für künftige Anwendungen	2 Bit	0b00
TX Add	TX Address (öffentliche Adresse)	1 Bit	0b0
RX Add	RX Address (nicht relevant)	1 Bit	0b0
Payload Length	Payload Länge ab diesem Byte	1 Byte	0x25
ADV Address	MAC Adresse des Beacons	6 Byte	0x00 00 00 00 00
AD Length	Länge AD Type und Daten ab diesem Byte	1 Byte	0x1D
AD Typ	Typ: Complete Local Name	1 Byte	0x09
AD Daten	Advertising Daten (ObjectID nach VDA5014)	29 Byte (max)	0x32 36 42 55 4E 33…
CRC	24-Bit CRC mit dem Polynom 0x00065B	3 Byte	0x00 00 00

4.1.4.2 Diagnostic Advertising

Die Tabelle 8 zeigt wie das Diagnostic Advertising Paket strukturiert ist. Per Grundeinstellung wird dies alle 120 Minuten wiederholt.

Tabelle 8: Struktur des Diagnostic Advertising Pakets

Komponente	Beschreibung	Länge	Beispiel
Preamble	Startsequenz (fest vorgegeben)	1 Byte	0xAA
Access Address	Access Address (fest vorgegeben)	4 Byte	0x8E 89 BE D6
Header			
PDU Type	PDU Type “non-connectable undirect advertising”	4 Bit	0b00 10
RFU	Reserviert für künftige Anwendungen	2 Bit	0b00
TX Add	TX Address (öffentliche Adresse)	1 Bit	0b0
RX Add	RX Address (nicht relevant)	1 Bit	0b0
Payload Length	Payload Länge ab diesem Byte	1 Byte	0x25
ADV Address	MAC Adresse des Beacons	6 Byte	0x00 00 00 00 00
AD Length	Länge AD Type und Daten ab diesem Byte	1 Byte	0x04 (4 Byte)
AD Typ	Typ: Service Data	1 Byte	0x16
AD Daten	Standard-GATT-Service x180F + Batteriestand in %	3 Byte	0x0F1840 (0x40 = 64%)
CRC	24-Bit CRC mit dem Polynom 0x00065B	3 Byte	0x00 00 00

4.1.4.3 Constant Tone Extension

Im Falle eine AoA-Anwendung wird einem Advertising Paket um eine so sogenannte Constant Tone Extension (CTE) ergänzt. Diese erzeugt eine kontinuierliches Trägersignal, das präzise Messungen hinsichtlich Abstand und Richtung zum Sender ermöglicht.

Copyright 2026

4.1.5 BLE Versionen

Die verschiedenen Versionen von Bluetooth Low Energy bringen jeweils signifikante Verbesserungen mit sich, die die Leistung und Flexibilität von BLE-Beacons erhöhen. BLE 4.x führte die Technologie ein und ermöglichte energieeffiziente Verbindungen, die sich vor allem für tragbare Geräte eigneten. BLE 5.x brachte erhebliche Erweiterungen, darunter eine deutlich größere Reichweite (bis zu 200 Meter), eine höhere Datenrate (bis zu 2 Mbit/s) und verbesserte Robustheit in schwierigen Umgebungen. BLE 6.x fokussiert sich auf eine verbesserte Energieeffizienz, optimierte Kanalnutzung und erweiterte Möglichkeiten zur gleichzeitigen Interaktion mit mehreren Geräten. Dies macht BLE 6.x besonders attraktiv für Internet-of-Things-Anwendungen (IoT) und komplexe Lokalisierungssysteme, wie sie bei BLE-Beacons zum Einsatz kommen.

4.2 Relevante Standards und Empfehlungen

Die dargestellten Inhalte basieren auf den Empfehlungen und Spezifikationen der Bluetooth Special Interest Group (SIG). Diese Non-Profit-Organisation ist verantwortlich für die Entwicklung und Pflege der globalen Quasi-Standards im Bereich der Bluetooth-Technologie. Die Einhaltung der SIG-Richtlinien stellt sicher, dass die beschriebenen Systeme und Technologien den aktuellen Best Practices entsprechen und eine nahtlose Integration mit anderen Bluetooth-Geräten und -Anwendungen ermöglichen. Alle weiteren Informationen sind der offiziellen Webseite der SIG zu entnehmen.

5 Ultra Wideband (UWB)

Die UWB-Technologie zur Lokalisierung von Objekten zeichnet sich durch ein breites Frequenzspektrum aus. Dabei basiert sie auf Messung der Signallaufzeit breitbandiger Funkimpulse. Aufgrund ihrer hohen zeitlichen Auflösung ermöglicht UWB eine präzise Bestimmung von Entfernungen und Positionen.
Zum Stand der Ausarbeitung der VDA-Empfehlung bestehen derzeit keine verbreiteten und anerkannten Standards, weshalb auf die Technologie hier nicht näher eingegangen wird. Sobald die Rahmenbedingungen eine detailliertere Betrachtung und Empfehlung durch den VDA ermöglichen, wird das vorliegende Dokument um UWB als Ortungstechnologie erweitert.

6 Optische Identifikation von Objekten

Ergänzend zu den vorangegangen Kennzeichnungen wird das zusätzliche Kennzeichnen mit Hilfe von optischen Identifizierungsmethoden empfohlen wie:

1D
- Klarschrift
- Barcode

2D
- Data Matrix Code (DMC)
- Quick Response Code (QR)

Hintergrund ist das geeignete Bereitstellen von Backup-Methoden sowie die Vermeidung technologiebedingter Medienbrüche. Diese Vorgehensweise stellt sicher, dass die Konformität und Kompatibilität der AutoID-Kennzeichnungen mit etablierten 1D/2D-Code-Methoden gewährleistet wird, und damit die Koexistenz von Bar-/DMC-/QR-Code sowie eine schrittweise Migration von Bar-/DMC/QR-Code zu weiteren AutoID Technologien ermöglicht wird.

6.1 Technische Anforderungen

6.1.1 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-Codesa, also QR-

Copyright 2026

Code und Data Matrix Code sind nach ISO/IEC 15434 zusätzlich die Startsequenz, der Format Indicator, ein Record Separators (RS), Group Separators (GS) und End of Transmission (EoT) zu verwenden (non-displayable characters). Tabelle 9 zeigt exemplarisch die Formatierung von einem Code 128 (1D) und einem 2D Code.

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

Beschreibung Dateninhalt	Code 128	2D Code	DOT Syntax
Startsequenz	*	[]>	.
Record Separator	*	$^{R}_{S}$	
Format Indicator	*	06	
Group Separator	*	$^{G}_{S}$	
Data Identifier$_1$	<DI$_1$>	<DI$_1$>	<DI$_1$>
Datenelement$_1$	[..]	[..]	[..]
Group Separator	*	$^{G}_{S}$	^
Data Identifier$_2$	*	*<DI$_2$>*	*<DI$_2$>*
Datenelement$_2$	*	*[..]*	*[..]*
..	..	..	..
Record Separator	*	$^{R}_{S}$	*
End of Transmission	*	$^{E}O_{T}$	*

* Keine Anwendung

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

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

1D/2D-Code	Exemplarischer Aufbau der Datenstruktur
Code 128	<DI>[Datenelement]
2D-Code	[]>$^{R}_{S}$06$^{G}_{S}$<DI$_1$>[Datenelement$_1$]$^{G}_{S}$<DI$_2$>[Datenelement$_2$]$^{R}_{S}{}^{E}O_{T}$
DOT Syntax	.<DI$_1$>[Datenelement$_1$]^<DI$_2$>[Datenelement$_2$]

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

Copyright 2026

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 12). 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.

Die Gestaltung des Data Matrix Codes entspricht dabei DataMatrix ECC 200 (vgl. ISO/IEC 16022). Hier werden u.a. die Abmessungen, Mindestgröße, Qualitätsklasse sowie Druckauflösung definiert. Die Abbildung 11stellt dies exemplarisch dar. Die Anforderungen für die Objektkennzeichnung in der Automobilindustrie sind jedoch abhängig vom Anwendungsfall und können in der Praxis variieren. Die Spezifikationen des konkreten Codes sollten daher projektbezogen abgestimmt werden.

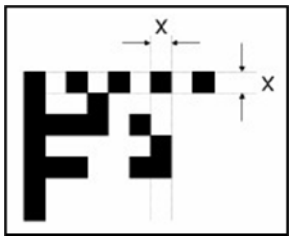


Abbildung 11: Beispielhafte Modulgröße von Codesymbolen (x)

6.2 Relevante Standards und Empfehlungen

Im Folgenden ist eine Übersicht über themenverwandte und -relevante Empfehlungen und Standards hinsichtlich optischer Identifikation von Objekten aufgeführt.

ISO/IEC	
ISO 15394	Packaging - Bar code and two-dimensional symbols for shipping, transport and receiving labels
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 16022	Information Technology - International Symbology Specification - Data Matrix

Copyright 2026

7 Anhang

7.1 Empfehlungen und Standards

Im Folgenden ist eine Gesamtübersicht über themenverwandte und -relevante Empfehlungen und Standards aufgeführt.

GS1	
GS1	Core Business Vocabulary (CBV)
GS1	EPC Information Services (EPCIS) Standard
GS1	Tag Data Standard (TDS)
GS1	General Specification
ISO/IEC	
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/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
ISO 15394	Packaging - Bar code and two-dimensional symbols for shipping, transport and receiving labels
ISO/IEC 15459-2	Information technology - Automatic identification and data capture techniques - Unique identification, Part 2: Registration procedures
ISO/IEC 17360	Automatic identification and data capture techniques - Supply chain applications of RFID - Product tagging, product packaging, transport units, returnable transport units and returnable packaging items
ISO/IEC 25910	Syntax keyboard and Web compatible encoding of data elements in machine readable symbols applied with ASC Data Identifiers
ISO/IEC 6523	Information technology - Structure for the identification of organizations and organization parts
JAIF	
JA01	Data Identifiers for Use in AutoID
Odette	
B21/LR05	RFID Item Level Standard
LR02	RFID in Vehicle Distribution Processes
LR03	RFID for Tracking of Parts and Assemblies
LR06	Capturing Supply Chain Events with auto-ID
LR07	Implementing RFID in the Automotive Supply Chain
RC-6/LR04	Returnable Transport Items Identification

Copyright 2026

VDA	
5014	Objektidentifikation in der Automobilindustrie
5501	RFID-Einsatz im Behältermanagement
5509	RFID-Einsatz und Datentransfer zur Verfolgung von Bauteilen und Komponenten in der Fahrzeugentwicklung
5510	RFID zur Verfolgung von Teilen und Baugruppen in der Automobilindustrie
5520	RFID-Einsatz in der Fahrzeugdistribution
5530	Automotive Business Vocabulary (ABV) gem. ISO 19987 (EPCIS)
5540	Zulassungsbedingungen für RFID-Transponder

Copyright 2026

7.2 Application Family Identifiers (ISO/IEC)

Tabelle 11: Application Family Identifiers (AFIs) nach ISO/IEC 17360 (ehemals ISO/IEC 1736X)

AFI	Bezeichnung/Einsatzbereich	Status
A1	Product tagging	Aktuell
A2	Transport unit	Aktuell
A3	Returnable transport item (RTI)	Aktuell
A5	Product packaging	Aktuell
AD	Returnable packaging item (RPI)	Aktuell
90	Vehicle identified with the Vehicle Identification Number (VIN) ISO 3779	Aktuell
A4	Product tagging – Hazardous Materials (HazMat) ISO 17367	Historisch, nicht für neue Anwendungen
A6	Product packaging – HazMat ISO 17366	Historisch, nicht für neue Anwendungen
A7	Transport unit – HazMat ISO 17365	Historisch, nicht für neue Anwendungen
A8	Returnable transport item – HazMat ISO 17364	Historisch, nicht für neue Anwendungen
A9	Freight container ISO 17363	
AA	Freight container (HazMat) ISO 17363	Historisch, nicht für neue Anwendungen

Copyright 2026

7.3 Kodierungstabelle (6-bit Encoding)

Tabelle 12: ASCII-Character-to-6-Bit-Encoding nach ISO 17360, eingeschränkter Zeichensatz für Object Type + Serial Number

Character	Binary Value	Character	Binary Value	Character	Binary Value	Charac-ter	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

Nur die in der Tabelle 12 grün markierten Zeichen sollten für die Abbildung von Dateninhalten innerhalb des UIIs verwendet werden:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z. Zusätzliche Verwendung von „ “ (Leerzeichen), + (Plus), - (Minus), . (Punkt), <EOT>, <RS>, <GS> gemäß Spezifikation. Alle anderen Zeichen könnten von IT-Systemen nicht als Nutzdaten interpretiert werden. Beispielsweise wird „*“ häufig als „Wildcard“ interpretiert.

Copyright 2026

7.4 Kodierungsbeispiel MB 01 (ISO 17360)

Reference-ID (plain text)
37SUN123456789975551230OFFFAS+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**100000100000**

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

Copyright 2026

PC data (cf. 2.2.3):

UII-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 UII content:

PC	AFI	UII 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

Copyright 2026

Der Verband der Automobilindustrie (VDA) vereint rund 620 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote.

Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen.

Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 780.000 Menschen sind direkt in der deutschen Automobilindustrie beschäftigt.

Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber	Verband der Automobilindustrie e.V. (VDA) Behrenstraße 35, 10117 Berlin www.vda.de Deutscher Bundestag Lobbyregister-Nr.: R001243 EU-Transparenz-Register-Nr.: 9557 4664 768-90

Copyright	Verband der Automobilindustrie e.V. (VDA) Nachdruck und jede sonstige Form der Vervielfältigung ist nur mit Angabe der Quelle gestattet.

Version	Version 2.0, August 2026