VDA	Basic Principles for RFID Application in the Automotive Industry	5500

This non-binding recommendation by the German Association of the Automotive Industry (VDA) has the following objectives:

- Standardization of technical requirements for RFID transponders
- Standardization of RFID-specific data structures
- Definition of requirements for application und usage of RFID transponders
- Standardized electronic data transfer for exchanging RFID information

Version 1.2 dated June 2015
(substitutes Version 1.1 dated April 2015)

AutoID Project Group

Publisher: Verband der Automobilindustrie
Behrenstrasse 35
10117 Berlin
Phone +49(0)30/897842-0
Telefax +49(0)30/897842-606
Internet: www.vda.de

VDA | Verband der Automobilindustrie

Disclaimer

VDA recommendations are freely available for general use. The user is responsible for ensuring correct application for the specific case.

They represent the latest technology available at the time of issue. Application of VDA recommendations does not relieve the user from responsibility for his own actions. In this regard, all users act at their own risk. VDA and those involved with VDA recommendations do not accept any liability.

Anyone applying VDA recommendations who identifies inaccuracies or possible incorrect interpretations is invited to inform VDA immediately and any errors can thus be rectified.

Document Maintenance Summary

Date	Action	Description
2015-06-15	Addition	Added AFI 0x90 for vehicle identification (Section 7.1)

Table of Contents

Figures

Tables

Abbreviations

AFI	Application Family Identifier
an	alphanumeric
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	Harzardous Materials
IEC	International Electronical 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	German Association of the Automotive Industry
VIN	Vehicle Identification Number
XML	Extensible Markup Language

1 Introduction

Radio Frequency Identification (RFID) improves process effectiveness and efficiency in the automotive industry. This particularly applies for Ultra High Frequency technology (UHF). Typical use cases are the Tracking & Tracing of vehicles, parts and (returnable) transport items (RTI). RFID has been successfully applied in the automotive industry for many years. So far the automotive industry mainly implemented RFID in closed loop applications. Recently, the automotive industry focuses on RFID applications in open loop environments.

The application of RFID in the automotive supply chain enables realizing several economic potentials:

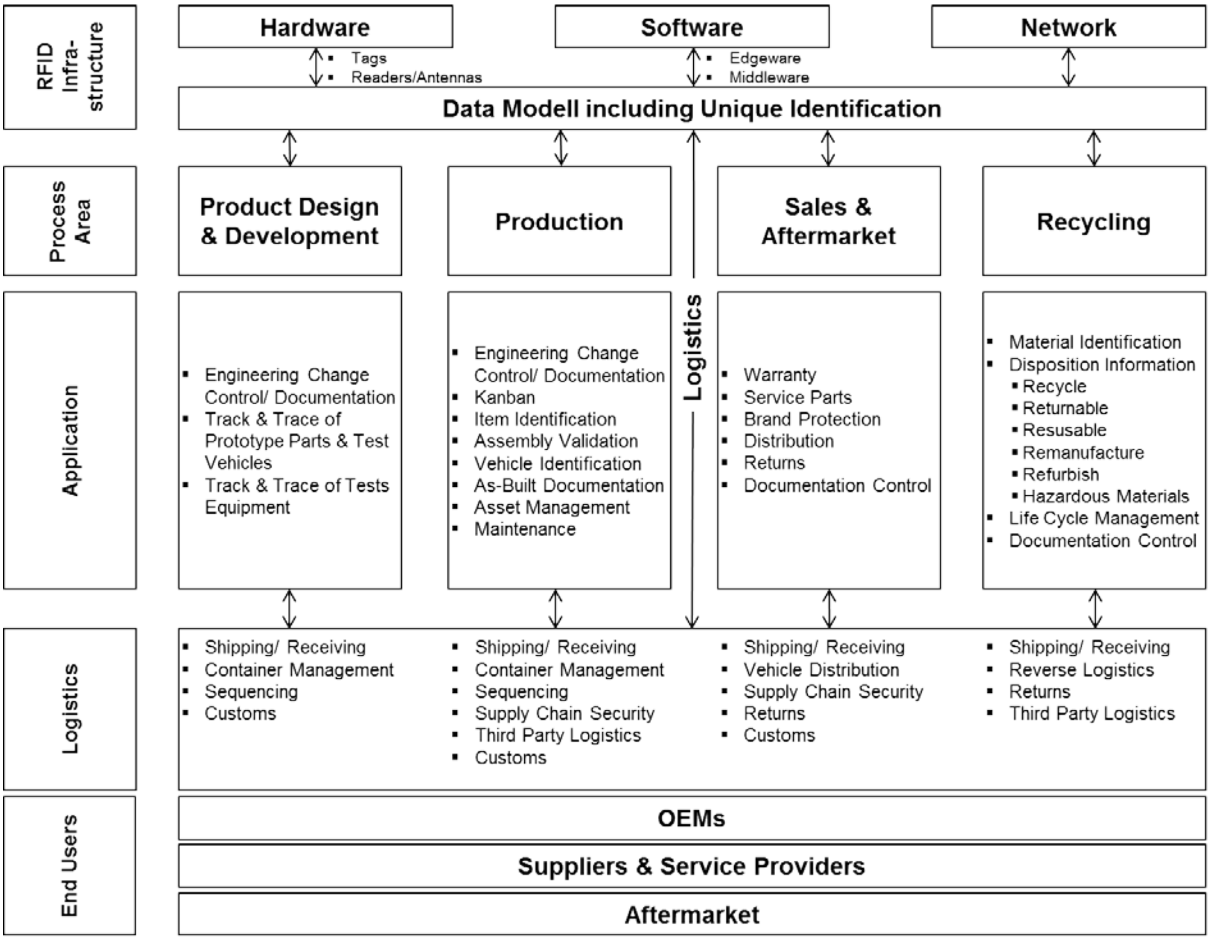


Figure 1: RFID Potentials in the Automotive Industry

Such cross-company RFID-applications require standards and recommendations to provide for industry-wide implementation. In the past few years, the German Association of the Automotive Industry (VDA) has published four industry-specific recommendations for implementing RFID technology:

- VDA 5501 - RFID for Container Management in the Supply Chain
- VDA 5509 - AutoID/RFID-Application and Data Transfer for Tracking Parts and Components in the Vehicle Development Process
- VDA 5510 - RFID for Tracking Parts and Components in the Automotive Industry
- VDA 5520 - RFID in Vehicle Distribution

These recommendations highlight some of the most significant and well-known use cases for cross-company RFID implementation.

VDA 5500 serves as a master document and summarizes general requirements for cross-company RFID applications as described in VDA 5501, 5509, 5510 and 5520. This document is organized as follows: Section 2 contains technical requirements for RFID transponders. Section 3 describes basic principles for setting up RFID-specific data structures. Section 4 covers the complementary application of optical identification such as 1D/2D codes. Section 5 addresses RFID-specific data exchange.

2 Technical Requirements for RFID Transponders

2.1 About Passive RFID Systems

Passive RFID systems include the following components:

- Stationary or mobile RFID reader and antenna(s)
- RFID transponders that are applied to objects

RFID transponders consist of microchips and antennas (Figure 2). The RFID reader transmits continuous waves, which are rectified at the transponder and used for power supply. Once the RFID transponders are activated, the RFID reader and the RFID transponders communicate via backscatter modulation. Passive RFID systems typically achieve operating ranges between 1-10 m. The RFID transponders vary in shape and size. They do not depend on additional power sources (e.g. batteries), which facilitates low cost production and operation (e.g. maintenance). Due to high operating ranges, flexibility and costs benefits passive RFID systems are particularly well-suited for industrial application.

Comment:
Conventional RFID transponders typically combine two different antenna types: Loop antennas and dipole antennas (Figure 2). Loop antennas and the dipole antennas are used for near field and far field communication respectively. The polarization of the RFID antennas strongly affects the performance of passive RFID transponders: Horizontally polarized (linear) antennas have their electric field parallel to the Earth's surface. An antenna is said to be vertically polarized (linear) when its electric field is perpendicular to the Earth's surface. A circular polarized antenna radiates in both the horizontal and vertical direction. RFID transponders perform best when the polarization of the transmitting RFID antennas and the polarization of the receiving antennas are aligned.

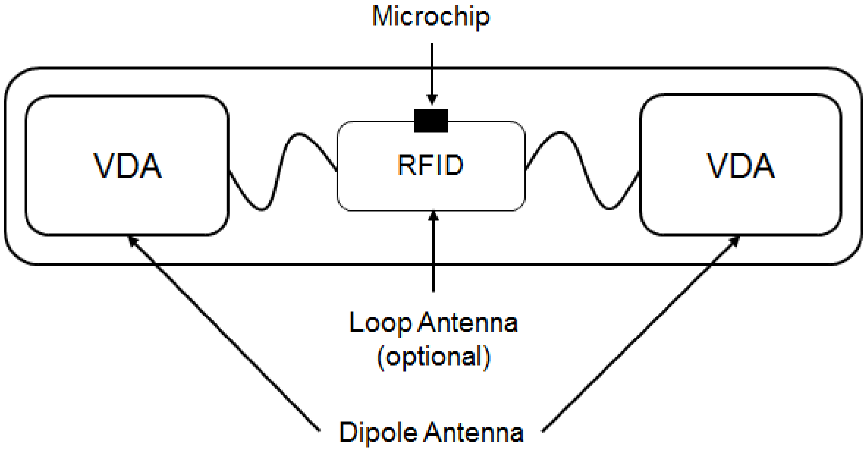


Figure 2: Design of passive RFID Transponders

2.2 Air Interface and Band Widths

Applied RFID transponders are compliant with ISO/IEC 18000-63/ EPC Class 1 Gen 2 (Air Interface). Applicable band widths differ and are defined by the International Telecommunications Union (ITU) as shown in Table 1:

Region	Frequency Ranges (MHz)
Europe	865-868/ 869
USA/ Canada	902-928
South America	915
South Africa	865-868
Australia	916-926
Japan	916-921
China	920-925

Table 1: Approved Frequency Ranges

RFID transponders shall provide for global application. However, conventional RFID transponders are usually optimized for regional operation, which may negatively affect the transponder performance in other regions.

2.3 Structure and Size of Memory Banks

Appropriate RFID transponders contain four different memory banks (MB):

- **MB 00 \`RESERVED´ – Kill- and Access-Password**
  Password for accessing and deactivating the RFID transponder. Maybe protected against read and write access.
- **MB 01 \`EPC´ – Unique Item Identifier (UII)**
  Unique Reference-ID for object identification. The content of MB 01 is read by default (inventory command) and does not require dedicated read/write commands such as other memory banks. It may be protected against write access.
- **MB 10 \`TID´ – Tag Identification**
  Manufacturer, type and model of the RFID chip. Shall also include a unique serial number issued by the transponder manufacturer. The content of MB 10 is usually protected against write access (lock).
- **MB 11 \`USER´ – User Memory (UM)**
  Additional object and application data. May be protected against write access.

Figure 2 shows the structure and content of the different memory banks:

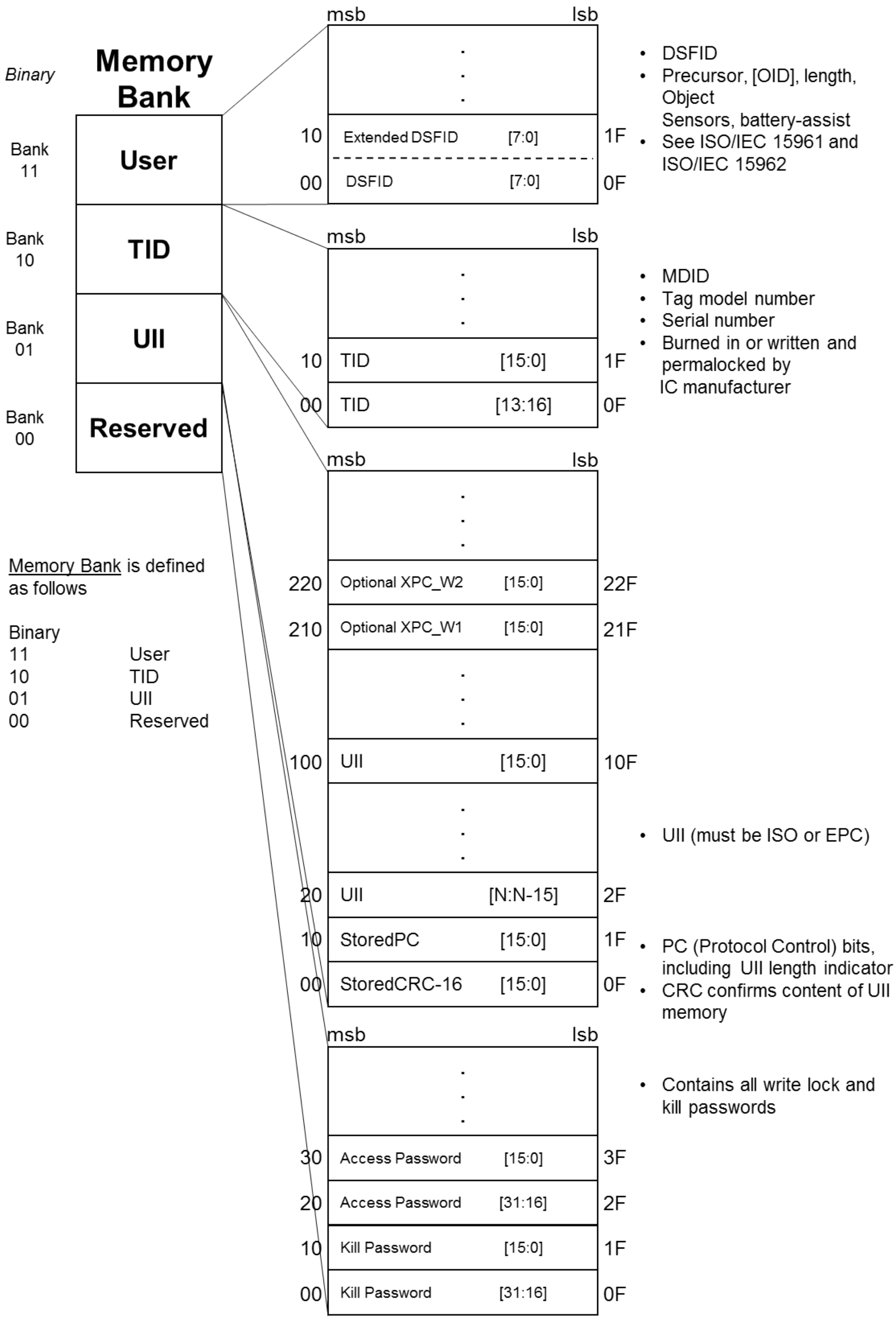


Figure 3: Structure of the Memory Banks (ISO/IEC 18000-63)

MB 01 has a memory size of 96-496 bit. Most automotive RFID applications require a memory size of 240 bits. The particular size of MB 01 and MB 11 depends on application-specific requirements which are specified in VDA 5501, 5509, 5510 and 5520 in more detail.

2.4 Transponder Types, Positioning and Mounting

The type, the positioning and the mounting of RFID transponders strongly affect the performance of RFID systems. Table 2 shows different transponder types and suitable materials they may be attached to:

Transponder Type	Object Type	Comment
Smart-Label (e.g. paper)	Plastics, textiles, glass (uncoated).	Not appropriate for metal application.
Flag-Tag (e.g. paper)	Plastics, textiles, glass, carbon fiber, metal.	Special type of Smart-Label. Also suitable for metal or similar.
Hard-Tag (e.g. plastics)	Plastics, glass (coated), carbon fiber, metal.	Distinguish between onMetal and nonMetal applications.
Embedded Transponder	Plastics, textiles, glass.	Transponder is integrated into the object.
Embedded RFID with slot antenna	Metal or similar.	Transponder is integrated into the object. Surface of the object serves as antenna.

Table 2: Transponder Types and Suitable Object Types

Table 3 shows several mounting methods and their particular advantages and disadvantages:

Mounting	Characteristics	Comments
Adhesive bondings	Fast, inexpensive application.	Must meet the same requirements as the object itself (temperature, weather conditions, durability etc.).
Clips	Flexible, re-usable.	Temporary appliances only.
Rivets	Especially suited for metal sheets and light alloy.	Special tools and corrosion protection required.
Screws	Suitable for permanent application. No special tools required.	Requires borings and corrosion protection.
Magnets	Flexible, re-usable.	Requires metal surfaces. Temporary appliances only.

Table 3: Mounting Methods

Figure 4 shows several RFID applications and suitable transponder types and fixing methods:

Containers (Volkswagen AG)

Automotive Parts (Robert Bosch GmbH)

Toll Application (Mexico)

Vehicle Distribution (SEAT S.A.)

Figure 4: Exemplary RFID Applications

The choice for specific transponder types, the positioning and the mounting depends on individual application scenarios and is therefore specified in VDA 5501, 5509, 5510 and 5520. Before actually implementing an RFID solution the RFID transponders shall be tested under real-life test conditions (static, dynamic). This also includes the installation, deployment and configuration of RFID readers and antennas (stationary, mobile).

2.5 Determining Factors for RFID Application

RFID applications in the automotive industry have to deal with multiple factors that influence the overall performance of RFID transponders (e.g. read rates, operating range). This includes:

- Reflections and shielding effects (metal, liquids)
- Absorbing materials (e.g. carbon fiber)
- Materials that manipulate radio signals (e.g. glass)
- Electromagnetic interferences caused by third party radio systems
- Electrostatic discharges

2.6 Environmental Influences and Durability

Apart from the determining factors for RFID application within the automotive industry (Section 2.5) there are several environmental influences that affect the performance of passive RFID systems and the durability of RFID transponders (Table 4).

Environmental Factors	**Comments**
Mechanical forces	Hits, vibrations, pressure, friction
Chemicals	Oil, cleansers, lubricants, acids, leaches, alcohol, tensides, solvents, salt
Temperature	Operating temperature, sun etc.
Weather conditions	Snow, rain, frost, ice, fog etc.

Table 4: Environmental Influences

Hence, in most automotive applications RFID transponders shall meet the requirements of IP 54 (cf. IEC 60529). This includes:

- Protection against contact and dust deposit
- Protection from splashed water

Typically, the RFID transponders shall resist temperatures between -40° and +70° Celsius. This also includes the mounting (e.g. adhesive bondings). The particular requirements vary and depend on the application context. Please review VDA 5501, 5509, 5510 and 5520 for further details.

Comment

The technical specifications of RFID transponders usually distinguish between temperature resistance and operation temperature. The temperature resistance specifies the minimum and maximum temperatures the RFID transponders are able to deal with. The operation temperature indicates the temperature range in which the RFID transponders may actually be operated (read/write).

RFID transponders shall last for approximately 10 years. Please review VDA 5510, 5509, 5510 and 5520 for deviant, application-specific requirements.

3 Data Structures for RFID Application

3.1 Principles for Storing Data to RFID Transponders

Application-specific data is stored to the Memory Banks 01 and 11. The following principles apply:

- MB 01 contains control information and the Unique Item Identifier (UII). The UII contains a reference-ID which is used to uniquely identify objects and typically is used to reference additional data that is stored in supporting IT-systems. MB 01 is to be protected against write access (lock).
- MB 11 contains additional object and application data (User Memory). Storing extensive data to MB 11 may lead to constraints regarding the performance of read/write processes. At the same time the automotive industry has not agreed on binding application standards yet. Hence, the usage of MB 11 is subject to bilateral agreements.

3.2 Alternative Data Standards (ISO/IEC, GS1)

In the automotive industry two alternative standards for structuring the data contents of RFID transponders have been established:

- Data structures according to ISO/IEC principles
- Data structures according to GS1 principles

The VDA recommends the implementation of ISO/IEC standards for cross-company RFID applications. However, GS1 standards may be used for intra-company RFID applications. Using GS1 standards in cross-company scenarios requires additional bilateral agreements between the affected supply chain partners.

In the following, we describe appropriate ISO/IEC-methods for structuring data in MB 01 and MB 11. GS1 standards are not described in this document. Please review the latest GS1 standards for technical documentation.

3.3 Storing Data to Memory Bank 01 (ISO/IEC)

Memory Bank 01 contains control information and the actual reference-ID (UII) that uniquely identifies objects. Figure 5 shows the structure of MB 01.

The control information contains the following details:

- Cyclic Redundancy Check (CRC)
- Length of Application Data (16 bit Words)
- Usage of Memory Bank 11 (Yes/No)
- Usage of the Extended PC Word (Yes/No)
- Applicable Data Standard ISO/IEC vs GS1 (*Toggle Bit*)
- Application Family Identifier (AFI)

In the following, we explain how to use the *Toggle Bit* and *Application Family Identifiers* (AFI). Please review ISO/IEC 15961 for further details.

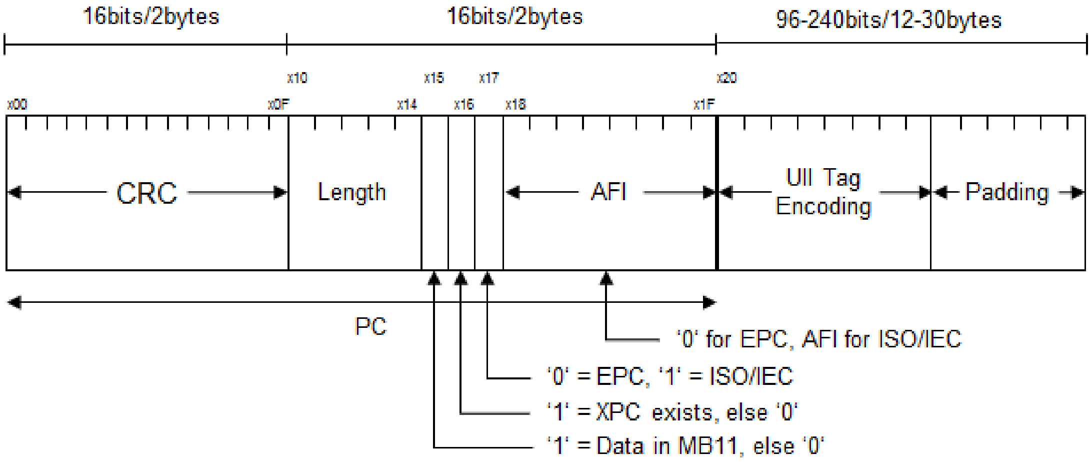


Figure 5: Structure of Memory Bank MB 01

The *Toggle Bit* (17_{hex}) defines whether the following data is structured according to ISO/IEC or GS1 principles:

- GS1-Standard: Set *Toggle Bit* to 0
- ISO/IEC-Standard: Set *Toggle Bit* to 1

Regarding the application of ISO/IEC-standards the AFI is particularly important. The AFI servers as primary filter that supports in distinguishing what kind of object has been read by the RFID application (e.g. automotive part, container). That way, the AFI supports in filtering relevant from irrelevant data. Additionally the AFI defines which kind of coding has been applied (6-bit). Available, standardized AFIs are listed in ISO/IEC 15961-2 Data Constructs Register and specified in ISO 17363-17367. Please review VDA 5501, 5509, 5510 and 5520 for choosing the right application-specific AFI.

MB 01 also contains the actual reference-ID (UII) that uniquely identifies objects. The format of the reference-ID is compliant with ISO/IEC 15418/ANSI MH10.8.2, ISO/IEC 15961-15962 and ISO 17363-17367. Please review VDA 5501, 5509, 5510 and 5520 for further application-specific details.

The reference-ID contains Data Identifiers (DI), which identify and structure the application-specific data contents. DIs complement AFIs and serve as secondary, more specified data filters, that support in identifying what kind of object has been identified by the RFID application (e.g. container type). Applying proper DIs makes sure that the RFID data structures are compliant with established 1D and 2D solutions.

The reference-ID shall end with End of Transmission (<EoT>) according to Application Standards ISO 17363-17367, which supports in abbreviating the decoding procedure. In case the reference-ID fills the complete capacity of the UII, the <EoT> may be omitted. The total length the reference-ID including DIs and <EoT> shall not succeed 240 bits (alphanumeric) to cope with commercially available low-cost transponders. Current standards permit up to 496 bits. The actual length of the data structure depends on the application-specific context and is defined within the Protocol Control (PC) area of the memory (5-bit length, following the 16-bit CRC declaration). The UII length defines how many 16-bit words are used. Incomplete 16-bit words must be filled with padding bits (monomorphic) as described in ISO/IEC 15962. Please review Table 5 for further details. The UII is 6-bit encoded; i.e. only capital letters, numeric values and a limited set of special characters may be applied (cf. Attachments, Table 17).

Comment

<EoT> and padding bits are used for control purposes and padding. They are not part of the reference-ID in the UII (MB 01) and the data that is stored to the UM (MB 11), i.e. both <EoT> and the padding bits are removed when decoding the data and sending it to IT backend systems.

Table 5 indicates how to code and decode a complete ISO/IEC-compliant data structure:

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	e.g. 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	**Reference-ID (alphanumeric)**		n * 6 bits	Reference-ID including Data Identifier (DI)
	<EoT>	0b100001	6 bit	End of Transmission according to 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*

Table 5: ISO/IEC-Encoding of MB 01

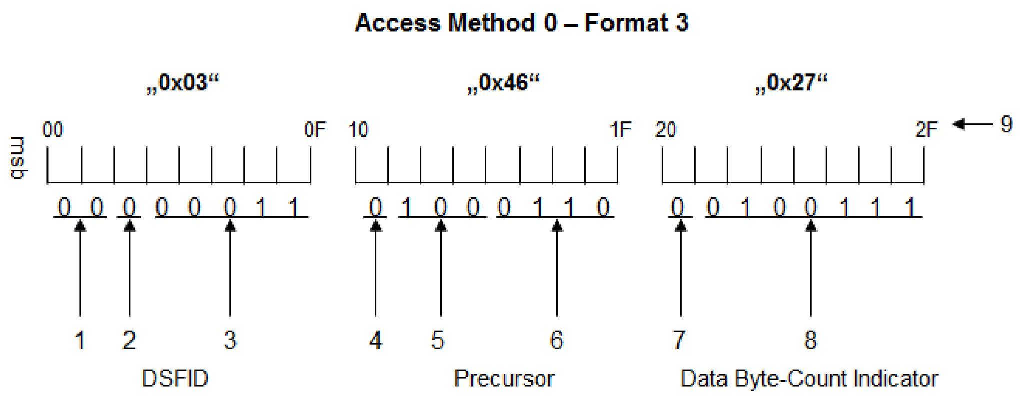
The attachments contain an example that shows how to appropriately code/encode ISO/IEC compliant data structures. Please review the referenced ISO/IEC standards and applicable VDA recommendations (5501, 5509, 5510 and 5520) for more technical and application-specific details.

3.4 Storing Data to Memory Bank 11 (ISO/IEC)

Memory Bank 11 contains object- and application-relevant data that complements the information of MB 01. That is why MB 11 is also called User Memory (UM). The format of MB 11 is aligned with MB 01; i.e. MB 11 contains both control and application data. The control information is stored to the first three bytes or four bytes of MB 11 and contains the following details:

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

Figure 6 shows the format of the control information that is stored to MB 11:



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)

Figure 6: Control Information in MB 11

The *Data Structure Format Identifier* (DSFID) specifies the access method and data format according to ISO/IEC 15962 (access method 0, format 3). The *Precursor* defines the coding type (6-bit) and the application of ISO/IEC 15434 compliant Data Identifiers (DI). The *Byte Count Indicator* contains the length of the application data stored to MB 11 including <EoT> and applicable Padding bits. The length of the *Byte*

Count Indicator varies between 1 byte or 2 bytes depending on whether the MB contains up to 1024 bits (≤ 128 bytes) or more (> 128 bytes). Please review Table 6 and Table 7 for more details.

The actual application data in MB 11 is structured with DIs according to ISO/IEC 15418. MB 11 may contain several data elements. Each data element is identified with appropriate DIs and separated using applicable *Separators* ($^{G}{}_{S}$ = „^“). The application of appropriate DIs is particular important because so far there are no cross-company standards regarding MB 11 application. Using standardized DI assures that the data can be interpreted.

The UM data content shall end with End of Transmission (<EoT>), which supports in abbreviating the decoding procedure. Remaining bits of the last 16 bit block (word) are filled with padding according to ISO/IEC 15962 Annex T 4.1 for MB 11. In case the UM data including DIs fills the complete capacity of the UM, the <EoT>may be omitted.

Comment

<EoT> and padding bits are used for control purposes and padding. They are not part of the reference-ID in the UII (MB 01) and the data that is stored to the UM (MB 11), i.e. both <EoT> and the padding bits are removed when decoding the data and sending it to IT backend systems.

Data contents are 6-bit encoded, i.e. only capital letters, numeric values and a limited set of special characters may be applied (cf. Attachments, Table 17). Table 6 indicates the control information in case the application data (*Object Length*) stored to MB 11 is ≤ 1024 bits:

Position	Data Type	Value	Size	Description
MB 11: User Memory (UM): Control Information (Header) for MB 11 ≤ 1024 bits				
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	$0_{(2)}$ declares that the next 7 bits are used to define the length of the following application data (object length ≤ 1024 bits). No additional bytes used for indicating the object length.
3b	Byte Count Indicator Length	Variable	7 bit	Object Length in Bytes
	Subtotal		***24 bits***	

MB 11: User Memory (UM): User- and Application Data				
1	Data Identifier$_1$	<DI$_1$>	6 … 24 bit	DI Data Element$_1$
2	Datenelement$_1$	alphanumerisch (an)	n * 6 bit	Data Element$_1$
3	Group Separator	<GS> ("^" in ASCII)	6 bit	Separator
4	Data Identifier$_2$	<DI$_2$>	6 … 24 bit	DI Data Element$_2$
5	Datenelement$_2$	alphanumerisch (an)	n * 6 bit	Data Element$_2$
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***

Table 6: ISO/IEC-Encoding of MB 11 (Object Length ≤ 1024 bits):

As mentioned above, the content of the control section in MB 11 depends on the size of the data that is stored into MB 11. Table 7 shows the control information in case the application data (*object length*) in MB 11 is > 1024 bits:

Position	Data Type	Value	Size	Description
MB 11: User Memory (UM): Control Information (Header) for MB 11 > 1024 bits				
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	$1_{(2)}$ declares that an additional byte is used to define the application data length (object length). The next 7 bits and the relevant 7 bits of the additional, following byte are concatenated to indicate extended application data (object length > 1024 bits)
3b	Byte Count Indicator Length	Variable	7 bit	First part of the length declaration. Applicable factor is 2^7 (3b*128 + 4b)
4a	Byte Count Indicator Switch	$0_{(2)}$	1 bit	$0_{(2)}$ declares that the next 7 bits are used to indicate the application data length. It also declares that no further bytes are applied for object length indication (no further concatenating).
4b	Byte Count Indicator Length	Variable	7 bit	Second part of the length declaration (3b*128 + 4b) Example: 3b: ~~1~~0000001 (128 bytes) 4b: ~~0~~0000010 (2 bytes) Total Object Length: 130 byte
	Subtotal		***32 bits***	

Table 7: ISO/IEC-Encoding of MB 11 (Object Length > 1024 bits):

Please review the referenced ISO/IEC standards and the application-specific industry recommendations VDA 5501, 5509, 5510 and 5520 for more details.

3.5 Read/Write Protection and Kill-Command

RFID-equipped objects often circulate in open-loop environments which implies that the RFID transponders are subject to potential misuse and therefore require protection. This particularly applies to MB 01 which contains the unique reference-ID. Corrupting the unique reference-ID may cause severe application and handling errors. Therefore, we recommend protecting MB 01 against write access.

Additionally, the RFID transponder shall be protected against deactivation. In the following, we describe applicable safety measures that prevent potential misuse:

Transponders that are compliant with ISO/IEC 18000-63 have two different passwords: an *Access Password* and a *Kill Password* (32 bit each). The passwords are stored to MB 00.

As soon as an RFID transponder is being addressed, it enters into one of two different states:

1. Open (factory default)
2. Secured (restricted access)

In case the RFID transponder does not contain an access password in MB 00 (*Access Password* = „0“), the transponder directly switches to the *Secure* state. Otherwise the appropriate password is required (*Access Password* <> „0“). Figure 7 indicates the password requirements for switching from one state to the other.

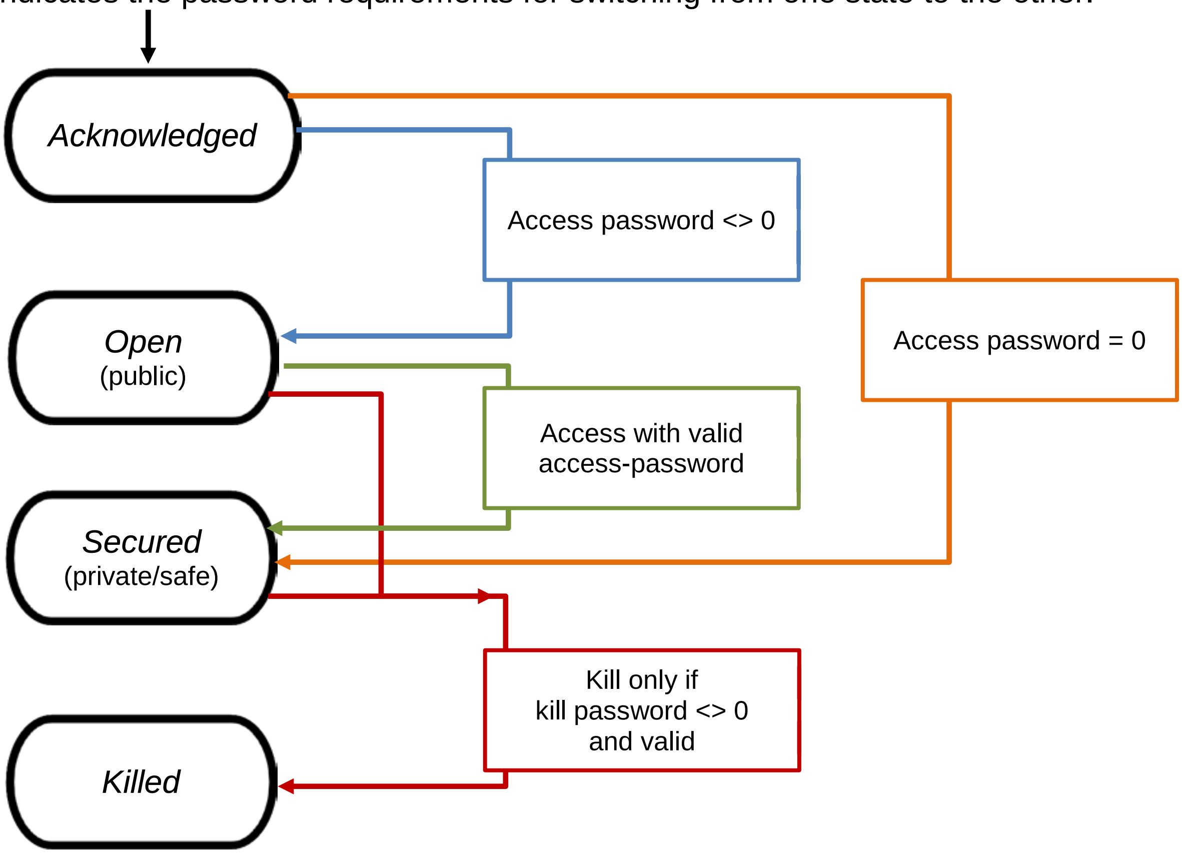


Figure 7: Tag State Diagram according to ISO/IEC 18000-63

The *Secure* state allows executing lock commands, which control the read/write access to the RFID transponder. This implies that each of the relevant memory banks of the RFID transponder is controlled separately. According to ISO/IEC 18000-63, RFID transponders provide for the following locking options:

Options	**UII (MB 01) / UM (MB 11)**
Unlocked	Associated memory bank is writeable from either the *Open* or *Secured* states.
Perma-Unlocked	Associated memory bank is permanently writeable from either the *Open* or *Secured* states and cannot be locked.
Locked	Associated memory bank is writeable from the *Secured* state but not from the *Open* states.
Perma-Locked	Associated memory bank is permanently not writeable from either the *Open* or *Secured* states.
	Passwords (MB 00)
Unlocked	Associated password location is readable and writeable from either the *Open* or *Secured* states.
Perma-Unlocked	Associated memory bank is permanently writeable from either the *Open* or *Secured* states and can't be locked.
Locked	Associated password location is readable and writeable from the *Secured* state but not from the *Open* state.
Perma-Locked	Associated password location is not readable or writeable from either the *Open* or *Secured* states.

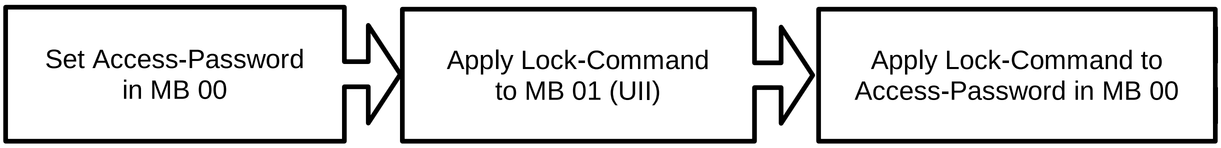
Table 8: Look Options according to ISO/IEC 18000-63

MB 00 (Passwords) may be protected against read and write access. MB 01 (UII) and MB 11 (UM) may be protected against write access only.

The kill command allows deactivating RFID transponders. Deactivating RFID transponders is irreversible. Therefore, we highly recommend protecting RFID transponders against deactivation by setting the access password in MB 00 to “Null” (cf. Figure 7).

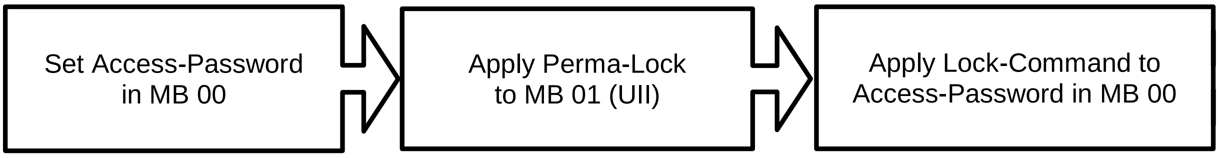
In the following, we show how to apply the read/write protection and prevent the RFID transponder from being deactivated:

Option 1: Protect UII against write access (reversible, password required):



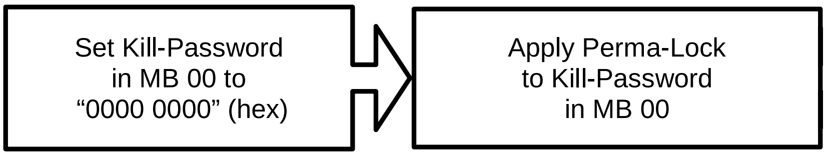
Locking the Access-Password in MB 00 protects the password against read access and potential misuse.

Option 2: Permanently protect UII against write access (irreversible):



Locking the Access-Password in MB 00 protects the password against read access and potential misuse. This step may be omitted when applying a perma-lock to MB 01 due to the fact that the perma-lock is irreversible and permanently protects the UII against write access even if the correct access-password is been provided.

After the write access to MB 01 has been restricted, protect the RFID transponder from being deactivated by disabling the kill-command:



Please review ISO/IEC 18000-63 for further details on read/write protection and the kill-command.

Comment
VDA 5500 exclusively addresses standardized read/write methods which are specified in ISO/IEC 18000-63. Note that several RFID equipment manufacturers implement proprietary commands for read/write protection. These commands may provide enhanced read/write options. Please review the manufacturer´s technical specifications and the applicable APIs for further information on hardware-specific read/write functionalities.

4 Additional Optical Object Identification

RFID applications shall imply optical object identification such as 1D/2D codes. The compatibility and interoperability of established 1D/2D codes and RFID technology supports automotive manufacturers in managing the coexistence of 1D/2D codes and RFID and in achieving gradual migration. Beyond that 1D/2D codes provide for appropriate *Backup*.

4.1 Application of 1D/2D Labels (ISO/IEC)

RFID identification and 1D/2D codes follow the same principles. Data elements are identified using Data Identifiers (DI) as described in ISO/IEC 15418. 2D codes additionally implement a Start Sequence, a Format Indicator, Group Separators ($^{G}{}_{S}$), Record Separators ($^{R}{}_{S}$) and End of Transmission ($^{E}O_{T}$) as specified in ISO/IEC 15434. Table 9 shows the format of appropriate 1D and 2D codes:

Data Contents	Code 128	DataMatrix
Start Sequence	*	[)>
Record Separator	*	$^{R}{}_{S}$
Format Indicator	*	06
Group Separator	*	$^{G}{}_{S}$
Data Identifier$_1$	<DI$_1$>	<DI$_1$>
Data Element$_1$	[..]	[..]
Group Separator	*	$^{G}{}_{S}$
Data Identifier$_2$	*	*<DI$_2$>*
Data Element$_2$	*	*[..]*
..	..	..
Record Separator	*	$^{R}{}_{S}$
End of Transmission	*	$^{E}O_{T}$

Table 9: Appropriate Formats for 1D/2D Codes

* not applicable

Table 10 shows exemplary 1D/2D codes:

1D/2D Code	Data Contents
Code 128	<DI>[Data Element]
DataMatrix	[)>$^{R}{}_{S}$06$^{G}{}_{S}$<DI$_1$>[Data Element$_1$]$^{G}{}_{S}$<DI$_2$>[Data Element$_2$]$^{R}{}_{S}$$^{E}O_{T}$

Table 10: Exemplary 1D/2D Codes

Unlike RFID data structures 1D/2D do not implement 6-bit but 8-bit encoding. However, VDA 5500 aims for consistency of RFID and 1D/2D data contents (hybrid application). Therefore, only 6-bit characters shall be used, i.e. capital letters, numeric values and a limited set of special characters (cf. Attachments, Table 17). If possible RFID-equipped objects shall also be identified using plain writing. VDA 5501, 5509, 5510 and VDA 5520 contain application-specific examples for appropriate optical object identification.

4.2 Application of the RFID Emblem

RFID-equipped objects shall be marked using the RFID emblem as described in ISO/IEC 29160 (Figure 8):

Figure 8: RFID Emblem

ISO/IEC 29160 provides for several, application-specific RFID emblems. Please review http://www.rfidemblem.eu/ for further details.

5 RFID-Specific Data Exchange

The RFID-specific data exchange primarily involves to two different scenarios:

- Intra-Company data exchange between RFID devices and IT Systems
- Cross-Company data Exchange between business partners

The following sections address these scenarios in more detail:

5.1 Intra-Company Applications

EPC Information Services (EPCIS) provide for an appropriate framework to communicate captured RFID data from RFID devices to IT backend systems. The EPCIS framework is suitable for both ISO/IEC- and GS1-based data structures and includes both RFID and 1D/2D approaches.

Figure 9 visualizes the EPCIS communication between RFID applications and IT backend systems.

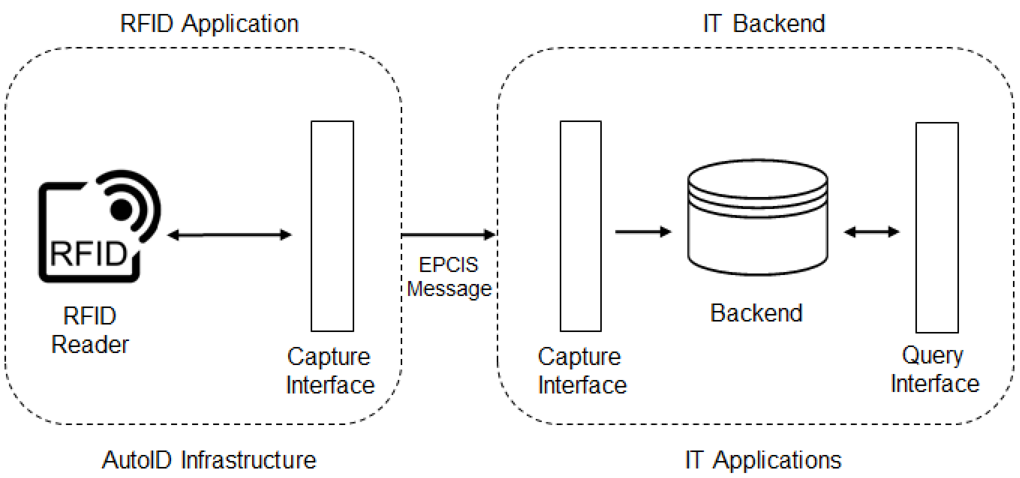


Figure 9: Data Exchange between RFID Applications and IT Backend Systems

The RFID transponders are read with stationary or mobile RFID devices which run dedicated *Capturing Applications*. The captured data is processed and converted into EPCIS messages (XML). The EPCIS messages are sent to *EPCIS Capturing Interfaces* via *http post* and are either sent to IT backend systems and/or EPCIS repositories.

EPCIS messages contain the following information:

Read Events (What?)	RFID-equipped objects
Read Locations (Where?)	Location where the RFID event takes place
Time Stamp (When?)	Capturing date and time
Context Information (Why?)	Goods receipt, quality inspection etc.

Table 11: Basic Event Information in EPCIS Messages

RFID Objects are described by applying Uniform Resource Identifiers (URI). In EPCIS, objects are represented using the so called *EPC Pure Identity*, i.e. the EPCIS Message contains the actual object references only and abandons additional control information.

Table 12 shows sample URIs for ISO/IEC and GS1-compliant data structures (CBV):

Standard	Uniform Resource Identifier (URI)	Sample 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

Table 12: URI Notation for Object References (ISO/IEC, GS1)

ISO/IEC-based data structures include the Application Family Identifier (AFI). In some cases the AFI may not be available. Hence the AFI may not be read and copied to the EPCIS messages. In these cases the following generic approach applies:

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

Table 13: URI Notation for Object References (ISO/IEC, generic)

1D/2D codes do not implement AFI at all. The generic approach also covers 1D/2D solutions, thus enables hybrid EPCIS approaches that account for both RFID and 1D/2D codes.

The URI representation also applies for RFID gates, mobile devices, printers etc. (ReadPoints):

Standard	Uniform Resource Identifier (URI)	Sample
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

Table 14: URI Notation for Read Points (ISO/IEC, GS1)

The *Pure Identity* of *ReadPoints* (ISO/IEC) shall be structured according to DIN 66277.

The location where an AutoID event takes place (*bizLocation*) is described as follows:

Standard	Uniform Resource Identifier (URI)	Sample
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

Table 15: URI Notation for Locations

The context of RFID events is described by *bizSteps*, e.g. goods receipt, quality inspection. Applicable *bizSteps* are specified in the Core Business Vocabulary (CBV) and the Automotive Business Vocabulary (ABV).

The particular contents of EPCIS messages vary and depend on the specific application context. Please review VDA 5501, 5509, 5510 and 5520 for further details.

5.2 Cross-Company Applications

In the automobile industry cross-company data exchange is typically based on the established EDI messaging formats (e.g. EDIFACT). Alternatively, business partners may choose to implement the *auto-gration* WebService, which was developed to meet the needs of the automotive industry. Please check http://www.auto-gration.eu/ for further details. Both methods are suitable for exchanging object information (RFID, 1D/2D codes) as long as the chosen messaging format provides for appropriate data contents.

RFID applications enable business partners to capture and exchange more object-related information than they used to in the past. The EPCIS messaging format is one of several approaches that is suitable for coping with these requirements and was specifically designed to exchange object related data (RFID, 1D/2D codes).

However, EPCIS messages do not replace but complement existing messaging formats. They contain additional information on objects and logistic procedures, thus support business partners in capturing and exchanging object-relevant data and in improving supply chain processes. EPCIS messages follow the so called *onNetwork* approach, i.e. EPCIS messages contain the actual object references which are stored to the UII of RFID transponders and a basic set of context information as described in Section 5.1. EPCIS messages are not intended to exchange object data and related information which is stored to the UM of RFID transponders.

The general conditions for RFID-specific data exchange and the actual content of the EPCIS messages vary and depend on specific implementation scenarios. VDA 5501, 5509, 5510 and 5520 specify relevant application requirements in more detail.

6 References

- 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/gsmp/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 for Container Management in the Supply Chain
- VDA 5509 - AutoID/RFID-Application and Data Transfer for Tracking Parts and Components in the Vehicle Development Process
- VDA 5510 - RFID for Tracking Parts and Components in the Automotive Industry
- VDA 5520 - RFID in Vehicle Distribution Processes

7 Attachments

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

Table 16: Application Family Identifiers (AFI) according to ISO/IEC

7.2 Coding Table (6 bit)

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

Table 17: ASCII-Character-to-6-Bit-Encoding (ISO 17363-17367)

7.3 Coding Example MB 01 (ISO 17367)

Reference-ID (plain text)
37SUN12345678999755512300FFFAS+123456

Compaction 6-bit code in binary code add <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

PC data (cf. Section 3.3):

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