

**VDA**

**RFID for Tracking Parts and Components  
in the Automotive Industry**

**5510**

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
- Complementary optical identification with DataMatrix Code

**Version 2.0 dated April 2015**  
(substitutes Version 1.0 dated May 2008)

**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](http://www.vda.de)

Copyright  
Reprints and any other form  
of duplication is only permissible  
when the source is cited.

**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.

## Table of Contents

1	Introduction .....	6
1.1	RFID in the Automotive Industry .....	6
1.2	RFID for Parts and Components .....	7
2	Technical Requirements for RFID Transponders .....	9
2.1	Passive RFID Transponders .....	9
2.2	Air Interface and Band Widths .....	9
2.3	Structure and Size of Memory Banks .....	9
2.4	Transponder Types, Positioning and Mounting .....	10
2.5	Determining Factors for RFID Applications .....	11
2.6	Environmental Influences and Durability .....	11
3	Data Structures for RFID Application .....	13
3.1	Principles for Storing Data to RFID Transponders .....	13
3.2	Alternative Data Standards (ISO/IEC, GS1) .....	13
3.3	Storing Data to Memory Bank 01 (ISO/IEC) .....	13
3.4	Storing Data to Memory Bank 11 (ISO/IEC) .....	17
3.5	Read-/Write Protection and Kill-Command .....	18
3.6	Methods for Fraud Prevention and Detection .....	19
4	Additional Optical Identification .....	21
4.1	Application of 1D/2D Labels .....	21
4.2	Application of the RFID Emblem .....	21
5	RFID-specific Data Exchange .....	22
6	References .....	23
7	Attachments .....	24
7.1	Data Identifier for Parts and Components (ISO/IEC) .....	24
7.2	Coding Table (6-bit) .....	25
7.3	Coding Samples according to ISO 17367 .....	26

## Figures

Figure 1: Counterfeit Measures - Object-Oriented Method.....	19
Figure 2: Counterfeit Measures - System-Oriented Method .....	20
Figure 3: DataMatrix-Label for Parts and Components .....	21
Figure 4: RFID Symbol for Parts and Components .....	21

## Tables

Table 1: Application Family Identifier (AFIs).....	14
Table 2: Basic Data Structure for Identifying Parts and Components .....	14
Table 3: Issuing Agency Code (IAC) .....	14
Table 4: Data Structure for Parts and Components .....	15
Table 5: MB 01 Coding Scheme for Parts and Components.....	17
Table 6: Data Identifiers according to ANSI MH10.8.2 .....	24
Table 7: 6-Bit-Character-Encoding compliant to ISO 17367 Table C.1 .....	25

## Abbreviations

0b	binary format
0h	hexadecimal format
AFI	Application Family Identifier
an	alphanumeric
CIN	Company Identification Number
CRC	Cyclic Redundancy Check
DI	Data Identifier
DUNS	Data Universal Numbering System
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EOT	End of Transmission
EPC	Electronic Product Code
EPCIS	Electronic Product Code Information Services
ESD	Electrostatic Discharge
GS1	Global Standards One
IAC	Issuing Agency Code
IEC	International Electrotechnical Commission
IP	International Protection
ISO	International Organization for Standardization
JAIF	Joint Automotive Industry Forum
MB	Memory Bank
n	numeric
OEM	Original Equipment Manufacturer
OID	Object Identifier
PC	Protocol Control
PN	Part Number
PSN	Part Serial Number
PWD	Password
RFID	Radio Frequency Identification
SN	Serial Number
TID	Tag Identification
UHF	Ultra High Frequency
UII	Unique Item Identifier
UM	User Memory
VDA	German Association of the Automotive Industry

# 1 Introduction

Radio Frequency Identification (RFID) provides a high degree of automation and unique item identification. This particularly applies for Ultra High Frequency technology (UHF). RFID offers the possibility to identify multiple objects in very short time and without direct line of sight. Due to these characteristics, RFID is more effective and efficient than other AutoID techniques such as Barcode and DataMatrix and improves object and information management in the automotive supply chain.

## 1.1 RFID in the Automotive Industry

RFID has been successfully applied in the automotive industry for many years. Typically, RFID is applied for Tracking & Tracing objects such as Vehicles, Parts and (Returnable) Transport Items (RTI). So far RFID projects focus on closed loop applications. In the last few years, RFID has also been applied in open loop applications. The latter requires standards and guidelines that provide for cross-company RFID application.

Therefore, the German Association of the German Automotive Industry (VDA) has published the following industry-specific recommendations for implementing RFID technology in cross-company environments:

- VDA 5500 – Basic Principles for RFID Application in the Automotive Industry
- 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 implementations in the automotive industry.

VDA 5510 specifies RFID-specific requirements for the Tracking & Tracing of automotive parts and components. VDA 5510 references VDA 5500 – Basic Principles for RFID Application in the automotive industry and incorporates the “Global Radio Frequency Identification (RFID) Item Level Standard”, which has been published by the Joint Automotive Industry Forum (JAIF).

This document is organized as follows: Section 2 describes technical requirements for RFID transponders that are used for Tracking & Tracing of parts and components. Section 3 covers principles for application specific data structures. Section 4 focuses on the additional optical identification of parts and components. Section 5 addresses complementary data exchange.

## 1.2 RFID for Parts and Components

RFID has several technical advantages compared to other AutoID techniques such as Barcode and DataMatrix:

- Automatized identification without direct line of sight
- Identification of many parts and components at the same time (bulk reading)
- RFID transponders are very robust and resistant to harsh industry environments

These technical characteristics and the unique identification of parts and components (serialization) enable use cases such as:

- Automatized Tracking & Tracing of parts and components
- Automatized production control and documentation
- Managing product recalls due to improved vehicle assembly documentation
- Improved information management within the product life cycle
- Fraud prevention and detection
- Improved recycling due to better documentation of the materials the parts and components consist of

### 1.2.1 Traceability

Unique object identification enables Tracking & Tracing of parts and components within the automotive supply chain and the entire product life cycle. This includes detailed object- and process-orientated documentation (e.g. suppliers, raw materials, sub-components, tests reports, producing plants, tools, settings) and provides for fast and decisive error analysis (functionality, quality). Please review VDA 5005 for further details.

Some parts and components are subject to statutory assembly documentation (airbags, seatbelts etc.), which forces automobile manufacturers to document the assembly of relevant parts and components. This assures for accountability in case of vehicle defects and supports in identifying affected vehicles whenever product recalls, warranty issues or compensation claims apply.

### 1.2.2 Fraud Prevention and Detection

Fraud prevention and detection methods distinguish between original parts and counterfeits. Appropriate measures for fraud prevention and detection also support

the industry in managing related warranty claims. Please review Section 3.6 for further details.



## 2 Technical Requirements for RFID Transponders

The general requirements regarding RFID transponders for Tracking & Tracing of parts and components are described on VDA 5500. In the following, we mainly focus on application-specific details. Please review VDA 5500 for further information about RFID in the automotive context.

### 2.1 Passive RFID Transponders

The Tracking & Tracing of automotive parts and components implements passive RFID transponders. Please review VDA 5500 for further information.

### 2.2 Air Interface and Band Widths

The RFID transponders are compliant with Air Interface Protocol Standard ISO/IEC 18000-63/ EPC Class 1 Gen 2. Applicable band widths may differ according to the geographical zone the RFID transponders are operated in. Please review VDA 5500 for further information.

### 2.3 Structure and Size of Memory Banks

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

- MB 00 „RESERVED“ – Kill- and Access-Password
- MB 01 „EPC“ – Unique Item Identifier (UII)
- MB 10 „TID“ – Tag Identification
- MB 11 „USER“ – User Memory (UM)

MB 01 is used to store the reference-ID, which uniquely identifies the part or component the RFID transponder is attached to. It is also referred to as Unique Item Identifier (UII). Coding a reference-ID consisting of 40 alphanumeric characters requires an MB 01 size of 240 bits (6-bit encoding). Apart from the reference-ID MB 01 also contains the control information (header). The header (CRC and PC) consists of 32 bits. This leads to a MB 01 size of 272 bits (32 bits + 240 bits). Note, that reference-IDs larger than 240 bits may lead to performance limitations. MB 01 shall be protected against unauthorized write access, to protect the initially issued reference-ID from being manipulated.

MB 11 contains additional object and process information. Therefore, MB 11 is also referred to as User Memory (UM).

MB 00 contains two 32 bit passwords, which may be used to protect MB 01 and MB 11 against unauthorized write access. MB 00 needs to be protected against unauthorized read/write access (cf. Section 3.5).

MB 10 contains the Transponder Identifier (TID). The TID is issued by the chip producer and uniquely identifies the RFID transponder.

## 2.4 Transponder Types, Positioning and Mounting

The type, position and mounting of RFID transponders strongly affect the performance of RFID systems. There are different transponder types such as *onMetal* and *nonMetal* transponders (cf. VDA 5500). Automotive parts and components are typically identified with Smart-Labels (adhesive bondings). Some parts and components are particularly exposed to environmental influences (temperature, chemicals) and require alternative transponder types (e.g. hard-tags) or different mounting methods. RFID transponders may also be integrated into parts or components (e.g. injection molding). In some cases the RFID transponder may even be embedded into metal parts (e.g. slot antennas).

Appropriate transponder types and transponder positions mainly depend on the parts and components they are attached to. This includes that the assembly position of the parts and components within the vehicles needs to be considered, if the parts and components shall be identified after having been assembled to the vehicle:

- **Interior/Exterior:** Transponders shall be attached at non-visible positions
- **Underbody/engine department:** Transponders are possibly exposed to particularly rough environmental influences (e.g. temperature/liquids)

The application of RFID transponders requires extensive testing and adequate documentation. Therefore, the vehicle manufacturers are responsible for defining the type and position of the RFID transponders. Both the RFID transponder type and the exact positioning shall be defined in the technical specifications of the parts and components (i.e. drawings). Deviations require the approval of the vehicle manufacturers.

<p><b>Comment:</b> RFID transponders shall not affect the characteristics and the functionality of parts and components they are applied to.</p>
--

## 2.5 Determining Factors for RFID Application

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

- Reflections and shielding effects (metal, liquids)
- Materials absorbing radio signals (e.g. carbon fiber)
- Materials manipulating radio signals (e.g. glass)
- Radio systems interfering with RFID systems (electromagnetic interferences)
- Electrostatic discharges

The Tracking & Tracing of parts and components usually implies two different capturing scenarios:

- Identifying individual parts and components (single or bulk reads)
- Identifying parts and components after they have been assembled to vehicles (single or bulk reads)

Each of the scenarios may be subject to different environmental influences. Often, the Tracking & Tracing of parts and components includes both scenarios. Example: During an early assembly process an individual part or component is identified successfully. After the part or component has been assembled it is covered by other parts and components (e.g. body parts). This causes additional metal reflections and shielding effects and negatively influences RFID performance. Therefore, identifying assembled parts and components is particularly challenging, which emphasizes the need for extensive testing and documentation (cf. Section 2.4).

## 2.6 Environmental Influences and Durability

The RFID transponders shall meet the same requirements as the parts and components they are attached to (e.g. environmental influences, temperature and chemical resistance). This also needs to be considered when selecting the fixing method for the RFID transponders (e.g. adhesive bondings). Typically, the RFID transponders shall meet the requirements of IP 54 (cf. IEC 60529). This includes:

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

Usually, the RFID transponders must resist temperatures between -40° and +70° Celsius. In some production steps (e.g. painting, drying) the temperatures may be significantly higher. This shall be considered when selecting appropriate RFID

transponders. In general, the RFID transponders shall last for approximately 10 years.

### 3 Data Structures for RFID Application

Appropriate and well-defined data structures are essential for successfully identifying automotive parts and components in open loop environments. In the following, we address application-specific aspects. Please review VDA 5500 for additional information.

#### 3.1 Principles for Storing Data to RFID Transponders

MB 01 contains the unique reference-ID that identifies the part or component the RFID transponder is attached to. Once the reference-ID has been issued, MB 01 is protected against unauthorized write access in order to provide for effective unique identification and prevent the reference-ID from being manipulated (cf. Section 3.5).

MB 11 contains additional object and process data. So far the automotive industry has not agreed on standardizing UM contents, therefore the usage of MB 11 requires additional bilateral agreements between involved supply chain partners. Please review Section 3.5 for applicable write protection.

#### 3.2 Alternative Data Standards (ISO/IEC, GS1)

Within the automotive industry two alternative standards for structuring data on RFID transponders have been established:

- ISO/IEC
- GS1

The VDA recommends the application of ISO/IEC standards for cross-company applications (cf. VDA 5500). In the following, we describe how to apply ISO/IEC standards for structuring data in MB 01 and MB 11 accordingly.

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

The reference ID (UII) which uniquely identifies parts and components is 6-bit encoded and stored to MB 01.

ISO/IEC provides two methods for structuring and filtering MB 01 data: Application Family Identifiers (AFI) and Data Identifiers (DI). In the following, we address these methods in more detail. Please review VDA 5500 for additional information.

##### 3.3.1 Application Family Identifier (AFI)

ISO/IEC provides two AFIs for identifying parts and components:

<b>AFI</b>	<b>Standards</b>
A1	ISO 17367 – Supply chain applications of RFID – Product tagging
A4	ISO 17367 – Supply chain applications of RFID – Product tagging (Hazardous Materials)

**Table 1: Application Family Identifier (AFIs)**

### 3.3.2 Data Identifier (DI)

VDA 5510 recommends the application of Data Identifier (DI) 37S for identifying parts and components. DI 37S implies that the part number (PN) and the serial number (SN) are declared separately:

<b>DI</b>	<b>IAC</b>	<b>CIN</b>	<b>PN</b>	<b>+</b>	<b>PSN</b>
Data Identifier	Issuing Agency Code	Company Identification Number	Part Number	Separator	Part Serial Number

**Table 2: Basic Data Structure for Identifying Parts and Components**

By using the separator (“+”) between PN and SN it is possible to identify and filter PN and SN without having precise string length indicators.

The previous version of VDA 5510 (Version 1.0) recommends the application of DI 25S, which implies strictly defined string lengths (cf. Section 7 ).The application of DI 25S is still valid. However, practice has shown that PN and SN may vary in length. This particularly applies to open loop environments. Therefore, the VDA suggests applying DI 37S for contemporary and future RFID applications.

### 3.3.3 Issuing Agency Code (IAC)

The Issuing Agency Code (IAC) identifies the authorized and registered agency (cf. ISO/IEC 15459-2) that has issued the Company Identification Number (CIN). Table 3 indicates common IACs that are applied in the European and international automotive industry.

<b>Agency</b>	<b>Description</b>	<b>IAC</b>	<b>Characters</b>
Dun & Bradstreet	Data Universal Numbering System (DUNS)	UN	2 (an)
Odette Europe	Odette Numbering System	OD	2 (an)

**Table 3: Issuing Agency Code (IAC)**

The VDA recommends the usage of DUNS numbers (cf. VDA 5506).

### 3.3.4 Company Identification Number (CIN)

The Company Identification Number (CIN) is issued by registered and authorized agencies (cf. Section 3.3.3) and uniquely identifies companies and organizational units. The CIN usually identifies the producer or supplier of a part or component. According to DUNS the CIN consists of nine numeric (n) digits. CINs issued by Odette consist of four characters (an). The owner of the CIN guarantees, that the reference ID uniquely identifies the parts or components (worldwide).

### 3.3.5 Part Number (PN) + Part Serial Number (PSN)

The reference-ID includes the parts number (PN) and a serial number (PSN), that assures unique identification. When implementing DI 37S, PN and SN are separated (“+”) and may vary in length (cf. Section 7). By using the separator PN and PSN may be identified without implementing additional string length indicators. However, the length of PN and PSN is limited by available storage capacities (cf. Section 2.3). Table 4 indicates an appropriate data structure for identifying parts and components:

<b>DI</b>	<b>IAC</b>	<b>CIN</b>	<b>PN</b>	<b>+</b>	<b>PSN</b>
Data Identifier	Issuing Agency Code	Company Identification Number	Part Number	Separator	Part Serial Number
37S	UN	Variable	Variable	Fix	Variable
3 char (an)	2 char (an)	9 char (n)	x char (an)	1 char (an)	y char (an)

**Table 4: Data Structure for Parts and Components**

**Comment:** Serial numbers that are used for RFID identification must not necessarily match proprietary serial numbers that have been established by suppliers for parts and components identification.

### 3.3.6 MB 01 Coding Scheme for Parts and Components

In the following, a complete ISO/IEC-compliant data structure for parts and components is described:

Bit Location (HEX)	Data Type	Value	Size	Description
<b>MB 01: CRC + Protocol Control Word</b>				
00 – 0F	CRC-16	Hardware assigned	16 bits	Cyclic Redundancy Check
10 – 14	Length	Variable	5 bits	Represents the number of 16-bit words excluding the PC field and the Attribute/AFI field.
15	PC bit 0x15	0b0 or 0b1	1 bit	0 = No valid User Data, or no MB11 <sub>2</sub> 1 = Valid User Data in MB11 <sub>2</sub>
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
18 – 1F	AFI	<b>0xA1 or 0xA4</b>	8 bits	Application Family Identifier used according to ISO/IEC 15961 and ISO 17367. For hazardous parts use A4.
	<b>Subtotal</b>		<b>32 bits</b>	
<b>MB 01: Unique Item Identifier (UII) with 6 bit encoding</b>				
Start at location 20 Go to end of data / end of available memory	DI	<b>"37S"</b>	3 an	Data Identifier 37S for Part Identification
	Issuing Agency Code (IAC)	"OD" or "UN"	2 an	Issuing Agency Code, according to DUNS, Odette
	Company Identification Code (CIN)	As defined by the IAC	4 an (OD) or 9 an (UN)	Company Identification Number
	Serial Number (SN)	Part Number (PN)	1...X an	X alphanumeric characters for the PN ID assigned by the owner



	<i>Consist of Part Number, Separator and Part Serial Number</i>	+ (Separator)	1 an	+ sign separator (2B <sub>n</sub> )
		Part Serial Number (PSN)	1...Y an	Up to y alphanumeric characters in capital letters
	<EoT>	0b100001	6 bit	End of Transmission ISO/IEC 17367 Table C1
	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	Padding according to ISO/IEC 15962 chapter 13.1
<b>Subtotal</b>		<b>Variable</b>	<b>Up to 240 bits</b>	
<b>TOTAL MB01<sub>2</sub> BITS:</b>		<b>VARIABLE</b>	<b>UP TO 272 BITS</b>	

**Table 5: MB 01 Coding Scheme for Parts and Components**

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

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

MB 11 is used to store additional object and process data. Therefore, MB 11 is also referred to as User Memory (UM). The coding scheme in MB 11 follows a well-defined pattern. Section 7.3.2 contains a coding sample. Please review VDA 5500 for further details. Please consider, that the usage of the UM involves performance limitations, which may negatively affect write/read processes in some applications. This particularly applies, when capturing several moving objects at the same time (e.g. capturing assembled parts in moving vehicles). These limitations need to be considered when planning and implementing RFID projects in order to avoid related writing/reading errors.

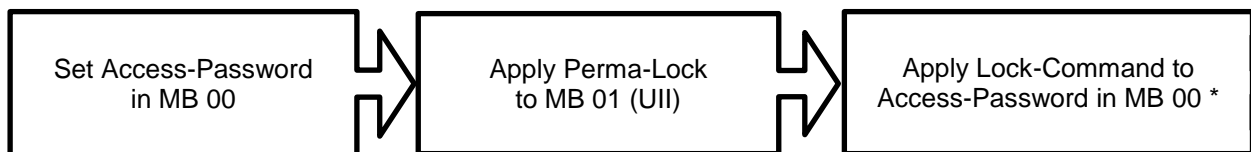
### 3.5 Read-/Write Protection and Kill-Command

RFID-equipped parts and components are subject to complex multi-tier supply chain and service processes. This requires control measures which protect RFID transponders against potential misuse. Appropriate read-/write protection assures that the RFID transponders and stored data may be used throughout the entire product life cycle. This particularly applies for the unique reference-ID.

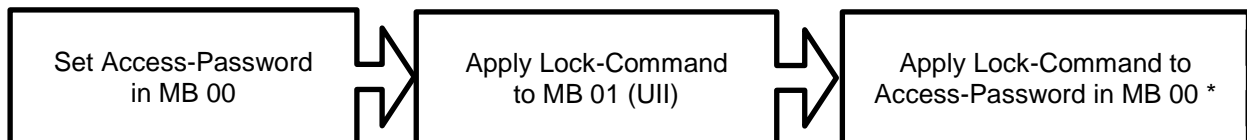
After the reference-ID is written to the UII, MB 01 is protected against unauthorized write access. This assures that the unique reference-ID may not be changed and permanently identifies the associated parts and components throughout the entire product life cycle. Additionally, the kill-password in MB 00 is set to “zero”. This prevents RFID transponders from being deactivated.

In the following, we describe how to apply appropriate read-/write protection:

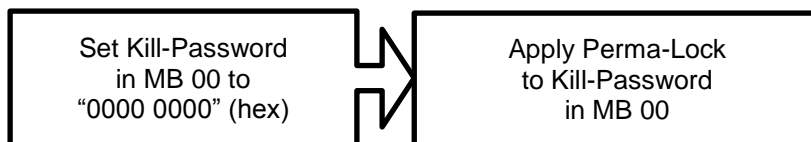
Protect MB 01 against write access (reference-ID may not be changed):



Protect MB 01 against write access (password required to change reference-ID):



After the write access to MB 01 has been restricted, prevent the RFID transponder from being deactivated:



**\* Comment:**

Applying a Lock or a Perma-Lock to the Access-Password in MB 00 assures that the password is protected against third party read access. If a Perma-Lock is applied to MB 01, the additional Lock to the Access-Password in MB 00 is redundant. The Perma-Lock permanently locks MB 01 – even if the correct Access-Password as defined in MB 00 is provided.

Please review VDA 5500 for further information on how to apply read-/write protection to RFID transponders.

### 3.6 Methods for Fraud Prevention and Detection

There are two different methods for fraud prevention and detection:

- Object-oriented methods
- System-oriented methods

**Object-orientated methods** focus on protecting the object-ID and/or data of parts or components. This implies encryption methods that protect the reference-ID (UII) and possibly additional data stored to the UM against unauthorized access. Please review ISO TC 247 for further details.

An additional object-orientated method consists in matching the object-ID (UII) and the inalterable TID, which is issued by the chip producer (Figure 1). The composed reference-ID is stored in a database. Parts and components that are not maintained in the database are likely to be counterfeits.

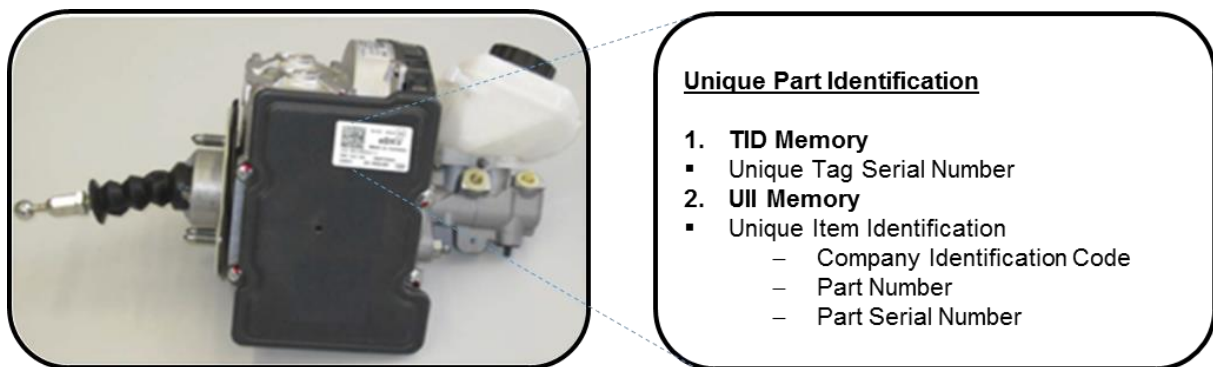
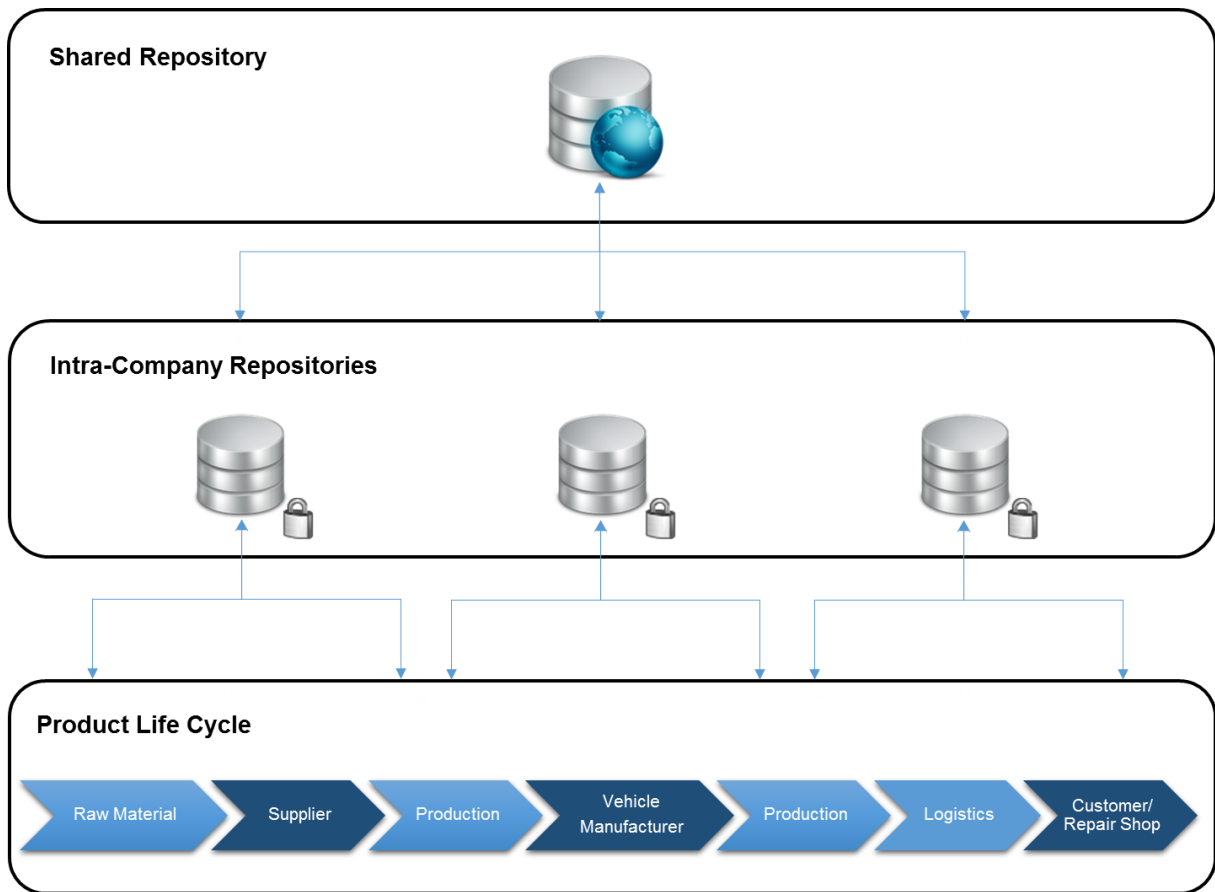


Figure 1: Counterfeit Measures - Object-Oriented Method

**System-orientated methods** imply that the parts and components are frequently captured throughout the supply chain and their entire product life cycle. This results in very detailed electronic documentation, which can be used to run plausibility checks, i.e., inconsistencies support in detecting counterfeits and localizing potential origins. System-orientated methods require a very high level of partner collaboration and process/system integration. The addressed parts and components are frequently captured and the accumulated data is kept in central database systems (Figure 2) which are shared by the business partners (shared repository).



**Figure 2: Counterfeit Measures - System-Oriented Method**

## 4 Additional Optical Identification

RFID applications for the Tracking & Tracing of parts and components shall imply complementary optical identification.

### 4.1 Application of 1D/2D Labels

RFID-equipped parts and components shall carry additional optional identification, i.e. plain writing and DataMatrix codes. The data written to the DataMatrix codes matches the data written to the RFID transponders, i.e, both the RFID transponders and the DataMatrix codes contain the unique reference-ID. The DataMatrix codes may also contain additional data.

Figure 3 shows a sample label for parts and components, which contains the unique reference-ID:

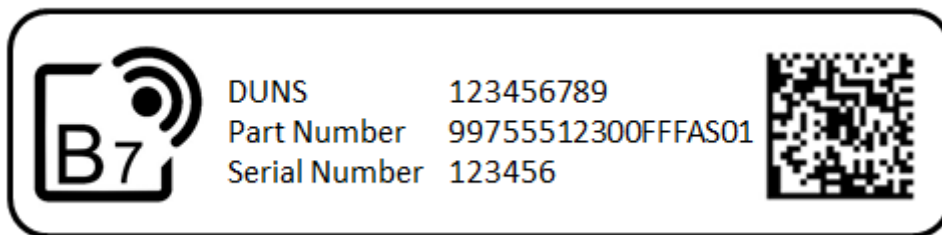


Figure 3: DataMatrix-Label for Parts and Components

Please review VDA 5500 for further information on structuring DataMatrix contents.

### 4.2 Application of the RFID Emblem

The RFID-equipped parts and components shall be marked with RFID emblems as described in ISO/IEC 29160.



Figure 4: RFID Symbol for Parts and Components

Please review <http://www.rfidemblem.eu/> for further details.

## 5 RFID-specific Data Exchange

Cross-company data exchange within the automotive industry is typically based on EDI messaging formats (e.g. EDIFACT). Alternatively, business partners may choose to implement the *auto-gration* Webservice, which was particularly developed to meet the needs of the automotive industry. Please check <http://www.auto-gration.eu/> for further details.

Additionally, EPCIS message may be used for intra-company and cross-company applications. EPCIS messages support the exchange of more detailed and precise object and process information compared to established messaging formats. Please review VDA 5500 and the latest GS1 standards for further information.

## 6 References

- ANSI MH10.8.2-2013 - Data Identifier and Application Identifier Standard
- IEC 60529 - Degrees of protection provided by enclosures (IP Code)
- 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 15459-2 Information technology - Unique identifiers - Part 2: Registration procedures
- 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 17367 - Supply Chains Applications of RFID - Product tagging
- ISO/IEC 18000-63 - Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz
- ISO/IEC 29160 - Information Technology - Radio Frequency Identification for Item Management - RFID Emblem
- ISO TC 247 - Fraud Countermeasures and Controls
- JAIF Global Radio Frequency Identification (RFID) Item Level Standard
- VDA 5500 - Basic Principles for RFID Applications in the Automotive Industry
- VDA 5505 - Traceability of Vehicle Components and Identifiability of their Technical Design
- VDA 5006 - Unique Identification of Business Partners
- VDA 5509 - AutoID / RFID-Application and Data Transfer for Tracking Parts and Components in the Vehicle Development Process.

## 7 Attachments

### 7.1 Data Identifier for Parts and Components (ISO/IEC)

Characters	Data Identifier	Description
an 3 + an... <undefined>	37S	Unique Item Identifier comprised of a sequence of 5 data elements: "IAC", followed by "CIN", followed by "Part Number (PN)", followed by the "+" character, followed by the supplier assigned (or managed) "Part Serial Number (PSN)" that is globally unique within the CIN holder's domain; in the format IAC CIN PN + PSN (spaces provided for visual clarity only; they are not part of the data). See Annex C.11.
	25S	Identification of a party to a transaction assigned by a holder of a Company Identification Number (CIN) and including the related Issuing Agency Code (IAC) in accordance with ISO/IEC 15459 and its registry, structured as a sequence of 3 concatenated data elements: IAC, followed by CIN, followed by the supplier assign serial number that is unique within the CIN holder's domain (See Annex C.11)

**Table 6: Data Identifiers according to ANSI MH10.8.2**



## 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 7: 6-Bit-Character-Encoding compliant to ISO 17367 Table C.1

## 7.3 Coding Samples according to ISO 17367

### 7.3.1 UII Coding Sample (MB 01)

The reference-ID is 6-bit encoded (cf. Table 7). The string is padded until an even number of bytes is reached. This way, in the PC area (*header*) the UII length may be declared in 16-bit words (2 bytes).

Reference-ID (plain text)
37SUN12345678999755512300FFAS+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	<b>100001</b>				

Split into 8-bit fragments including padding bits					
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	0001 <b>1000</b>	<b>00100000</b>

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 of 16-bit words: 0b **0111 1** (30 bytes → #15 words)  
 Valid User Memory: 0b **1** (user memory)  
 XPC: 0b **0** (not used – reserved)  
 EPC or ISO code: 0b **1** (*ISO*)  
 All PC bits: 0b **0111 1101** (hex 7D)

Protocol Control	AFI
7D	A1

**Coded UII content (including header):**

P C I	A F I	UII Reference-ID																													
		7D	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

**7.3.2 UM Coding Sample (MB 11)**

The UM data is coded similar to the UII data. The first part of the data represents the *header*. The length of the *header* is three or four bytes, depending on the length of the following data string (cf. VDA 5500).

In the following, we describe how to code the UM content.

**Sample Data:**

DI	Description	Sample	Length
1P	supplier part number	5221886	9
2P	engineering change level	00C	5
52P	color code	F1F	6
2Q	weight	2	3
4D	manufacturing date (Julian yyddd)	15045	7

The complete data string including DIs, actual data contents and separators is 6-bit encoded (cf. Section 3.4) and padded according to ISO/IEC 15962 Annex T4.1 for MB 11 until an even number of bytes is reached.

**UM Data (plain text)**

```
1P5221886<GS>2P00C<GS>52PF1F<GS>2Q2<GS>4D15045
```

The sample string consists of 30 characters. Additionally, 5 control characters are used (including <EoT>). This results in 35 characters. Therefore, the coding sample requires  $35 * 6 = 210$  bits. Consequently, the length of the header is 3 bytes (24 bits). This results on a total length of 234 bit. The string is padded with 6 padding bits to reach an even number of bytes (header + data string). The overall length including padding is 240 bit (30 bytes = 15 words, 16 bits each).

**Compaction 6-bit code including <EoT>**

110001	010000	110101	110010	110010	110001
111000	111000	110110	011110	110010	010000
110000	110000	000011	011110	110101	110010
010000	000110	110001	000110	011110	110010
010001	110010	011110	110100	000100	110001
110101	110000	110100	110101	<b>100001</b>	

Split into 8-bit fragments including padding bits					
11000101	00001101	01110010	11001011	00011110	00111000
11011001	11101100	10010000	11000011	00000000	11011110
11010111	00100100	00000110	11000100	01100111	10110010
01000111	00100111	10110100	00010011	00011101	01110000
11010011	01011000	01 <b>100001</b>			

Hex code representation					
C5	0D	72	CB	1E	38
D9	EC	90	C3	00	DE
D7	24	06	C4	67	B2
47	27	B4	13	1D	70
D3	58	61			

#### Header data (cf. Section 3.4):

DSFID: 0h **03**  
 PreCursor: 0h **46**  
 Byte Count Indicator Switch: 0b **0** (only one length byte)  
 Byte Count Indicator Length: 0b **001 1011** (27 byte of "6-bit data")  
 All header bytes: 0h **03 46 1B**

#### Coded UM content (including header):

DSFID	Precursor	Byte Count Indicator	UM
03	46	1B	C50D72CB1E38D9EC90C300DED72406C467B24727B4131D70D35861