INTERNATIONAL STANDARD

ISO/IEC 29143

First edition
2011-02-01

Information technology — Automatic identification and data capture techniques — Air interface specification for Mobile RFID interrogators

Technologies de l'information — Techniques d'identification et de captage automatiques des données — Spécification d'interface d'air pour interrogateurs Mobile RFID

Reference number
ISO/IEC 29143:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 29143 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

Introduction

This International Standard provides an air interface specification for Mobile radio frequency identification (RFID) interrogators that are part of a passive backscatter system. This system comprises one or more mobile interrogators, also known as Mobile RFID interrogators, and an undefined number of tags, also known as labels.

Interrogators are not required to support channel sensing, i.e. do not need to implement Listen Before Talk (LBT), and transmit commands on the off chance under the risk of colliding with one or more peer-interrogators. Moreover, interrogators compliant to this International Standard are not obliged to synchronize by any means (wired or wireless), i.e. no control channel dedicated to coordinating Time Division Multiplexing (TDM) is provided.

Tags are powered by the RF signal provided by the interrogator and respond to an interrogator by modulating the reflection coefficient of its antenna, thereby backscattering data to the interrogator. The working mode adopted by the tags is purely passive, i.e. tags do not actively initiate any kind of RF communication.

In this International Standard, collision arbitration and collision avoidance for Mobile RFID applications are defined by specifying methods aimed at mitigating the impact of emerging collisions and mechanisms used to avoid follow-up collisions.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of patents concerning radio-frequency identification technology given in the clauses identified below.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC.

Information on the declared patents may be obtained from:

Contact details	
Patent Holder:	
Legal Name	CISC Semiconductor Design+Consulting GmbH
Contact for license application:	
Name & Department	Markus Pistauer, CEO
Address	Lakeside B07
Address	9020 Klagenfurt, Austria
Tel.	+43(463) 508 808
Fax	+43(463) 508 808-18
E-mail	m.pistauer@cisc.at
URL (optional)	www.cisc.at
Patent holder:	
ETRI (Electronics and Telecommunications Research Institute)	
Contact for license application:	
Name & Department:	Gilwon Kim, Intellectual Property Management Team
Address:	138 Gajeongno, Yuseong-gu
Address:	Daejeon, 305-700, Korea
Tel.	+82-42-860-4908
Fax	+82-42-860-3831
E-mail	kwkim@etri.re.kr
URL (optional)	www.etri.re.kr

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

The latest information on intellectual property that may be applicable to this International Standard can be found at www.iso.org/patents.

Information technology — Automatic identification and data capture techniques — Air interface specification for Mobile RFID interrogators

1 Scope

This International Standard applies to Mobile radio frequency identification (RFID) interrogator devices used to inventory passive or semi-passive backscatter tags at 860 MHz to 960 MHz in a mobile (non-fixed) application independent from specific communication details, i.e. modulation technique and command set.

Furthermore, the scope of this International Standard is mobile consumer applications, whereas mobile enterprise applications are not covered as long as operating in a closed environment.

An operating environment is considered to be closed if it belongs to a central administrative authority able to guarantee for sufficient isolation, i.e. preventing mobile enterprise interrogator devices from being used outside the dedicated operating environment, and if sufficient spatial separation and/or electromagnetic shielding from adjacent operating environments is provided.

An application is considered a consumer application if at least one of two interacting entities is a private individual (consumer) and the interaction is taking place in the public domain. Consequently, a Mobile RFID consumer application is defined as Mobile RFID equipment (e.g. mobile phones equipped with an RFID interrogator) being used in a consumer application.

NOTE As there is currently no active contribution on Mobile HF interrogators, this International Standard covers only UHF.

This International Standard specifies

— Mobile RFID interrogator media access control,

— interrogator to interrogator and multiple interrogator to tag collision arbitration scheme including interrogator requirements,

— interrogator to interrogator and multiple interrogator to tag collision avoidance scheme, and

— tag memory use for Mobile RFID applications.

This International Standard does not specify

— physical interactions (the signaling layer of the communication link) between interrogators and tags,

— interrogator and tag operating procedures and commands, and

— the collision arbitration algorithm used to singulate (separate to the current response slot) a specific tag in a multiple-tag environment.

NOTE These aspects are addressed by other International Standards.

In particular, this International Standard does not replace any existing RFID air interface specification issued by ISO/IEC but extends the existing methodologies for fixed RFID interrogators with mechanisms addressing

the special challenges of Mobile RFID. The concepts and mechanisms described in this International Standard can be integrated in any existing RFID protocol approved by ISO/IEC for the given frequency range of 860 MHz to 960 MHz (unless explicitly prohibited by such protocol) regardless of the actual command set.

The mechanisms defined by this International Standard can be used for Mobile RFID interrogators used in consumer applications and compliant to ISO/IEC 18000-6.

2 Conformance

To claim conformance with this International Standard, an interrogator shall comply with all relevant clauses, except those marked as “optional”. Moreover, the interrogator shall also operate within local radio regulations, which may further restrict operation.

To claim conformance with this International Standard, an interrogator shall also fulfill all requirements to claim conformance with the basic air interface specification ISO/IEC 18000-6.

NOTE The basic assumption is that this International Standard cannot be used standalone. It is not intended to encourage usage of a proprietary air interface in combination with the extension defined in this International Standard and allow claiming conformance with this International Standard in that context.

Mobility of the RFID interrogator device is not a requirement for claiming conformance with this International Standard. It is recommended that all RFID interrogators operating in public areas of service, where interrogator to interrogator and multiple interrogators to tag collisions cannot be ruled out by administrative measures such as Time Division Multiplexing or Frequency Division Multiplexing, support the mechanisms specified in this International Standard regardless of the particular usage of the device (fixed, mobile, or both).

Conformance may also require a license from the owner of any intellectual property utilized by this device.

A mobile device shall only activate its RF for RFID capabilities if it is established that it operates according to the RF regulations of the country where it is turned on. For mobile phones this implies that the phone shall derive the country of operation from the network before activating the RF capabilities for RFID.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18000-6:2010, *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz*

ISO/IEC 19762 (all parts), *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

RFC 2141, *URN Syntax*, May 1997

RFC 3406, *Uniform Resource Names (URN) Namespace Definition Mechanisms*, October 2002

4 Terms, definitions, symbols, abbreviated terms, and notation

4.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 (all parts), ISO/IEC 18000-6 and the following apply.

4.1.1
basic air interface
complementary air interface specification that can be used in combination with this International Standard

4.1.2
channel width
extent of a continuous range of frequencies

NOTE The definition can apply for a transmit or a receive channel. It is usually measured in kilohertz. A definition of the term “channel” can be found in ISO/IEC 19762.

4.1.3
contention period
time interval, starting with the first bit of a protocol data unit being transmitted until the reception of the last bit, in which an interrogator command or tag response is vulnerable and can be destroyed due to interference

4.1.4
EPCglobal Application
application whose usage denotes an acceptance of EPCglobal standards and policies

cf. **ISO Application** (4.1.8)

4.1.5
idealized inventory round
sequence of interrogator commands and tag responses leading to a tag detection without anti-collision being applied

NOTE See ISO/IEC 19762 for a definition of the terms “inventory round” and “anti-collision”.

4.1.6
interrogator to interrogator collision
interrogator command transmitted by an interrogator R2 interfering with a tag response to an interrogator command previously issued by a competing interrogator R1, preventing R1 from successfully decoding a valid tag response

NOTE See ISO/IEC 19762 for a definition of the term “collision” in general.

4.1.7
interrogator transmit channel
channel in which interrogator commands are transmitted

NOTE A definition of the term “channel” can be found in ISO/IEC 19762.

4.1.8
ISO Application
application whose MB01 data structure includes a “1” bit in bit 17h and where bits 18h through 1Fh encode an Application Family Identifier (AFI) as defined in ISO/IEC 15961-3

cf. **EPCglobal Application** (4.1.4)

4.1.9
listen before talk
mechanism to determine the current status of occupation of a communication channel by means of channel sensing

4.1.10
MIIM content name
description of the object associated with mobile item identification and management (MIIM) services

EXAMPLE Brand name, company name, food name, movie title, building name.

4.1.11
Mobile RFID
automatic identification and data capture technique supporting the mobile item identification and management (MIIM) technologies of radio frequency identification (RFID)

4.1.12
Mobile RFID interrogator
electronic equipment that retrieves information from radio frequency (RF) tags by transmitting RF signals to and receiving RF signals from the tags

NOTE Also known as a mobile RFID reader.

4.1.13
multiple interrogators to tag collision
collision in which two or more RFID interrogators issue commands in a way that the transmission of the two commands overlap temporarily, preventing the tag(s) from being able to decode a valid interrogator command

NOTE See ISO/IEC 19762 for a definition of the term “collision” in general.

4.1.14
object directory service
service to provide a mapping relationship between mobile item identification (MII) for something physical or virtual and its corresponding associated information

4.1.15
protocol data unit
any kind of data package transmitted by RFID interrogators or RFID tags, i.e. interrogator commands and tag responses

4.1.16
receive channel
channel in which the tag response is received

NOTE Can be equal to **interrogator transmit channel** (4.1.7). A definition of the term “channel” can be found in ISO/IEC 19762.

4.1.17
receiver timeout
ending of receiver active time triggered by the tag state machine due to inactivity on the communication channel or due to absence of valid RF modulation, encoding or message structure

4.1.18
singulated
⟨one tag in a population of tags⟩ having sent back its response without interference from another tag

NOTE 1 A singulated tag is the result of singulation.

NOTE 2 See also ISO/IEC 19762.

4.1.19
tag anti-collision
process used to prepare for dialogue between an interrogator and one or more RF tags out of the total number of RF tags responding to a request command

4.1.20
tag on tag collision
interference of two or more concurrent tag responses in a way that no valid response can be decoded by the RFID interrogator

NOTE See ISO/IEC 19762 for a definition of the term “collision” in general.

4.2 Symbols

P_{thres} power threshold value used to detect interfering interrogators

W_{Size} moving average filter window size

4.3 Abbreviated terms

CP	contention period
DIM	dense interrogator mode
LBT	listen before talk
MIIM	mobile item identification and management
MinWaitTime	minimum retransmission wait time
MaxWaitTime	maximum retransmission wait time
ODS	object directory service
PDU	protocol data unit
RX	receive
TX	transmit
UII	unique item identifier
URI	uniform resource identifier

4.4 Notation

For the purposes of this document, the following notational conventions apply.

$xxxx_2$ binary notation

$xxxx_h$ hexadecimal notation

Furthermore, the intended usage of the terms “positive” and “negative” in the context of describing the output of specified blocks is as follows.

positive binary 1

negative binary 0

Moreover, parameters are always written in italic font, e.g. *parameter1*.

5 Overview

This International Standard specifies mandatory interrogator transmitter properties, which are defined in Clause 6, a mandatory specification of the media access method for Mobile RFID interrogators in Clause 7, mandatory and optional tag memory structures in Clause 8, optional command extensions introduced for the special purpose of Mobile RFID applications in Clause 9, and a number of informative annexes providing additional non-mandatory information useful for the implementation of this International Standard, which are Annex A to Annex F.

Due to the lack of a dedicated control channel for Mobile RFID interrogators no explicit synchronization of two or more interrogators can be established. Additionally, implicit synchronization as achieved by applying Carrier Sensing or Listen Before Talk is basically not applicable to mobile applications due to the lack of suitable listen thresholds. In general, key figures like the number of active mobile devices at a certain location and the specific local arrangement, e.g. distance to the tagged object(s), possible movement of the involved entities and direction of the antennas are not known in advance. Mobile RFID applications are likely to be more complex and less predictable than fixed applications which results in a demand for additional collision avoidance and collision arbitration mechanisms aimed especially on the requirements of Mobile RFID scenarios.

In contrast to fixed RFID applications, where only Tag on Tag collisions have to be resolved by the anti-collision mechanism of the air interface specification, three different types of collisions need to be addressed for Mobile RFID scenarios. Please refer to Annex A for a detailed overview about possible communication errors in Mobile RFID environments.

This International Standard provides a set of simple, robust and effective mechanisms for implementing media access control for Mobile RFID interrogators. All different types of possible collisions are addressed by reducing the probability of unwanted interference and/or providing mechanisms to recover from possible collisions.

The air interface specification for Mobile RFID interrogators described in this International Standard cannot be used on its own but builds upon an existing RFID command set for fixed RFID that is used as a fundament for the mechanisms described in this International Standard. Suitable air interface specifications for this purpose, e.g. ISO/IEC 18000-6 Type C, are provided by ISO and can be found on the internet at www.iso.org.

6 Transmitter

6.1 Introduction

Mobile RFID interrogators that declare conformance to ISO/IEC 29143 shall comply with 6.2 and all mandatory sub-clauses.

Subclause 6.2 contains all parameters mandatory for mobile UHF interrogators that declare conformance to ISO/IEC 29143. Other frequency bands are currently not supported.

6.2 Mobile UHF Transmitter

6.2.1 Frequency Parameters

6.2.1.1 Frequency Band

The frequency band to be used by Mobile RFID interrogators shall be selected according to local regulations.

Channel access and channel utilization shall be done as specified in Table 1.

In case one or more dedicated channels are available to Mobile RFID within local regulations, such channels shall be accessed by applying LBT unless channel sensing is not required by local regulations. As long as

LBT is supported, Dense Interrogator Mode shall not be mandatory. If a dedicated channel is used for Mobile RFID the media access method specified in Clause 7 shall be mandatory for mobile interrogators.

If no dedicated channels are assigned to Mobile RFID, transmit channels shall be selected according to local regulations (e.g. 4 channel transmit scheme for Europe) and LBT or Frequency Hopping may be applied in accordance to local regulations. Furthermore, the following rules apply:

— In case of Receive Channel Widths of less than 600 kHz, where Receive Channels (RX Channels) are the channels where the tag response is received, see Figure 1, the media access method specified in Clause 7 shall be mandatory if LBT is not used. If Listen Before Talk is used, usage of the media access method specified in Clause 7 is recommended but not mandatory for mobile interrogators.

— If the width of all utilized Receive Channels is greater or equal 600 kHz, Dense Interrogator Mode shall be mandatory, i.e. the spectrum mask specified in Figure 3 applies. If LBT is not used, the media access method specified in Clause 7 shall be mandatory for mobile interrogators. In any other case, usage of the media access method specified in Clause 7 is recommended for mobile interrogators but remains an optional feature.

NOTE 1 Transmit and Receive Channel may be identical, e.g. In-channel backscatter.

NOTE 2 When operating in Dense Interrogator Mode further restrictions regarding signaling may be specified by the basic air interface specification, e.g. ISO/IEC 18000-6 C.

NOTE 3 LBT may always be used regardless of the application of the media access method specified in Clause 7 to identify the least used channel.

Table 1 — UHF Channel Access and Utilization

Dedicated Channel for Mobile RFID available	RX Channel Width (for tag response)	Listen Before Talk (LBT), see NOTE 2	Frequency Hopping (FH), see NOTE 3	Dense Interrogator Mode (DIM)	Commanded Tag Response Format	MAC according Clause 7
Yes	X	X	X	No (NOTE 1)	Not restricted	Mandatory
No	<600 kHz	Yes	No	Not applicable	Not restricted	Recommended
		No	Yes	Not applicable	Not restricted	Mandatory
		No	No	Not applicable	Not restricted	Mandatory
No	≥600 kHz	Yes	No	Yes	Subcarrier	Recommended
		No	Yes	Yes	Subcarrier	Mandatory
		No	No	Yes	Subcarrier	Mandatory

X Don't care

NOTE 1 DIM shall be required if LBT is not applicable due to local regulations.

NOTE 2 Under LBT regulations, the MAC method according Clause 7 is used within dwell time after carrier sensing and first time communication.

NOTE 3 Under FH regulations, the MAC method according Clause 7 is used in the first channel within dwell time and repeated after the channel is changed every dwell time interval.

The RX Channel width in Table 1 shall be defined between the upper edge of the lower frequency band allowed for transmit and the lower edge of the upper frequency band allowed for transmit. Examples are shown in Figure 1 and Figure 2.

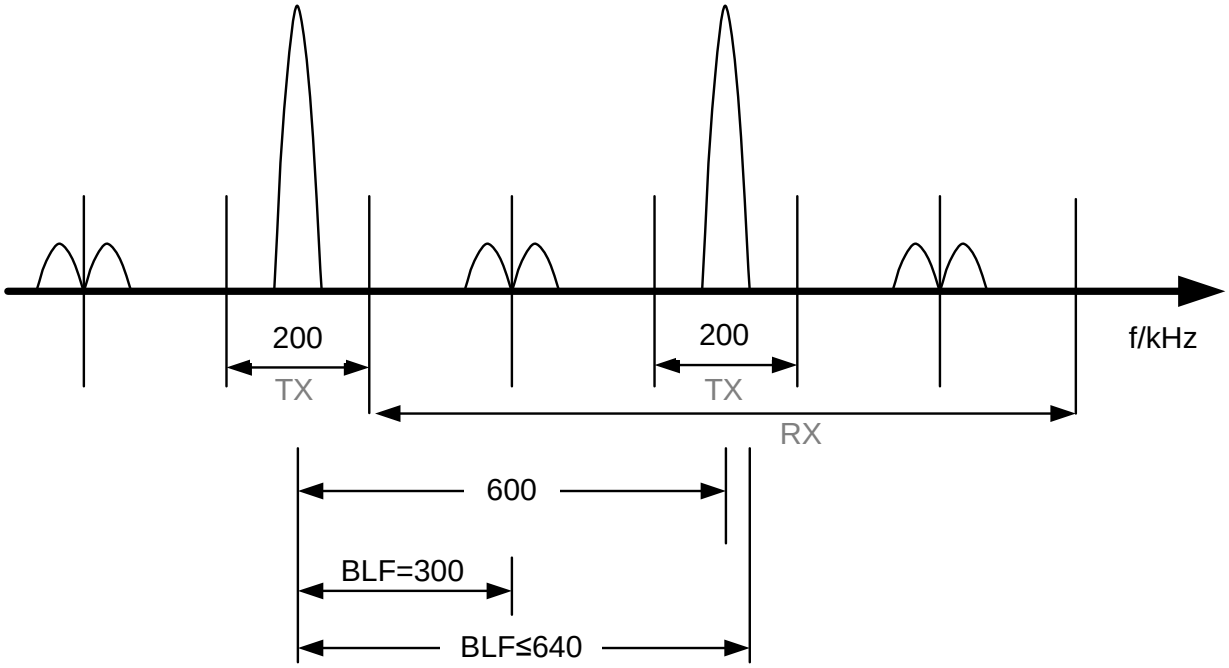

Figure 1 — Example 1 of Possible Transmit and Receive Channel Allocation (e.g. Europe, Korea)

NOTE In Figure 1, the approach of alternative-channel backscatter is shown. In that case the tag response occupies 4 Receive Channels adjacent to the Transmit Channel. Channel width is 200 kHz as according channel plan.

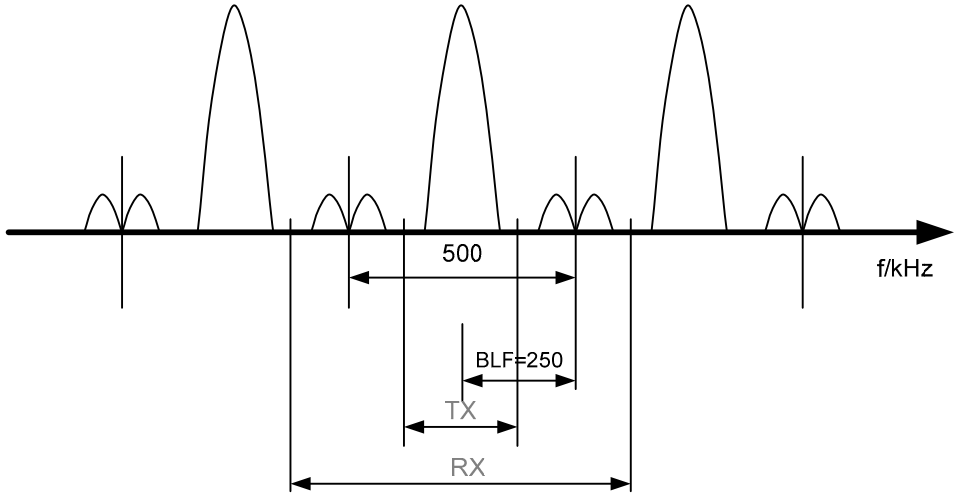

Figure 2 — Example 2 of Possible Transmit and Receive Channel Allocation (e.g. US)

6.2.1.2 Frequency Accuracy

The tolerance of transmit frequency for Mobile RFID shall be set to less than ±8ppm for temperatures between -25°C and +40°C and less than ±10ppm for the extended temperature range of −40°C to +65°C, unless specified differently by local regulations.

6.2.2 Output Power Parameters

6.2.2.1 Maximum Output Power

The maximum interrogator output power shall be selected in accordance with local regulations.

An interrogator output EIRP of less than 23dBm is recommended for preventing Mobile RFID signals from interfering with fixed RFID systems.

6.2.2.2 Spectrum Mask

Interrogators that are claimed to operate according to this International Standard shall meet the local regulations for out-of-channel and out-of-band spurious radio-frequency emissions.

Interrogators shall only support Tari ≥ 12.5 µs, whereas additionally the tolerance according to ISO/IEC 18000-6 shall apply.

Interrogators that are claimed to operate in Dense Interrogator Environments, in addition to meeting the local regulations, shall also meet the Transmit Mask shown in Figure 3.

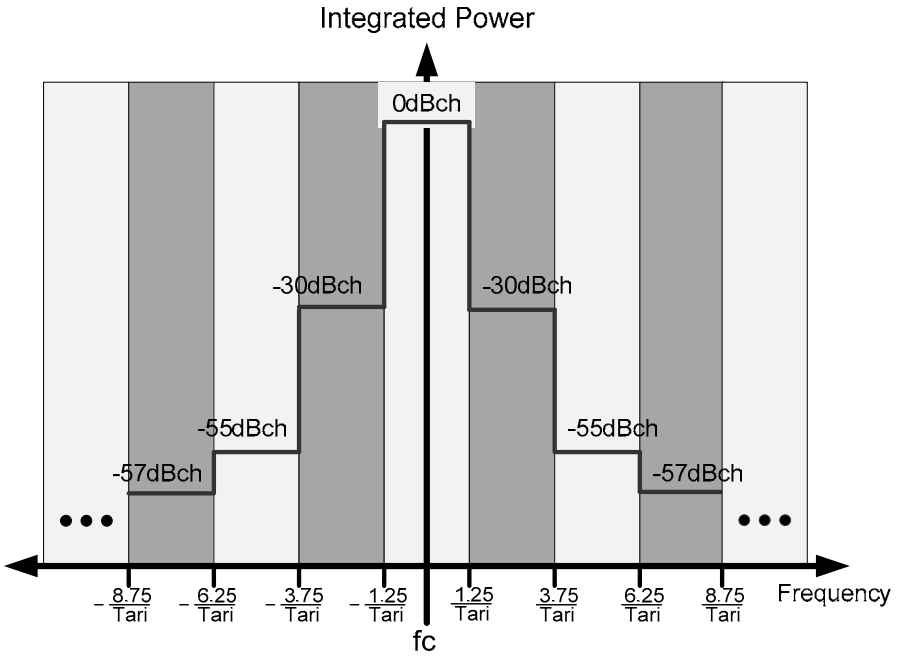

Figure 3 — UHF Transmit Mask for Mobile RFID Interrogators

For an interrogator transmitting random data in channel R, and any other channel S≠R, the ratio of the integrated power P() in channel S to that in channel R shall not exceed the specified values:

|R – S| = 1: 10log10(P(S) / P(R)) < –30 dB

|R – S| = 2: 10log10(P(S) / P(R)) < –55 dB

|R – S| > 2: 10log10(P(S) / P(R)) < –57 dB

Where P() denotes the total integrated power in the specified channel.

7 Media Access Method

7.1 General Approach

Interrogators may start an inventory round whenever ready regardless of the current occupation of the selected frequency band, i.e. no Listen Before Talk (LBT) is required as long as no separate channel is assigned to Mobile RFID. All means of assessing the current status of a channel, e.g. by implementing any kind of carrier sensing, are optional and are out of the scope of this document.

Competing interrogators transmitting within the same channel are not forced to synchronize by any means, i.e. no explicit control channel is established between the involved entities. All means of synchronizing two or more interrogators regardless of the nature of the synchronization concept (centralized or decentralized) are out of the scope of this document. Synchronization between two or more interrogators based on the concepts contained in this International Standard is entirely implicit and does not require any special synchronization infrastructure.

Situational command retransmission combined with adaptive retransmission wait time definition are the key concepts presented in the remaining sections of this document.

Commands are retransmitted if a Multiple Interrogators to Tag Collision or an Interrogator to Interrogator Collision is detected. Interrogators shall pause for a random period as specified in 7.4 before reissuing a command after a collision has been detected. Collisions are not detected while issuing commands and hence collision arbitration starts right after the transmission is finished, i.e. ongoing command transmissions shall not be interrupted on the fly.

Moreover, commands are retransmitted if a receiver timeout (see 4.1) is detected on the interrogator side, e.g. T_2 timeout. Interrogators pause for a random period according to 7.4 before reissuing a command after a receiver timeout.

Collision arbitration is implemented by retransmitting commands at least once – or even multiple times if a corrupted tag reply is received repeatedly, whereas collision avoidance is supported by suspending the interrogator for a random period after a collision is detected under certain circumstances in order to reduce the probability of a follow up collision.

7.2 Collision Detection

Figure 4 shows all relevant components of an UHF RFID interrogator device including all functionality required to detect all different types of collisions described in Annex A and to trigger appropriate measures to recover from the occurring communication clashes as specified in 7.3 and 7.4 respectively.

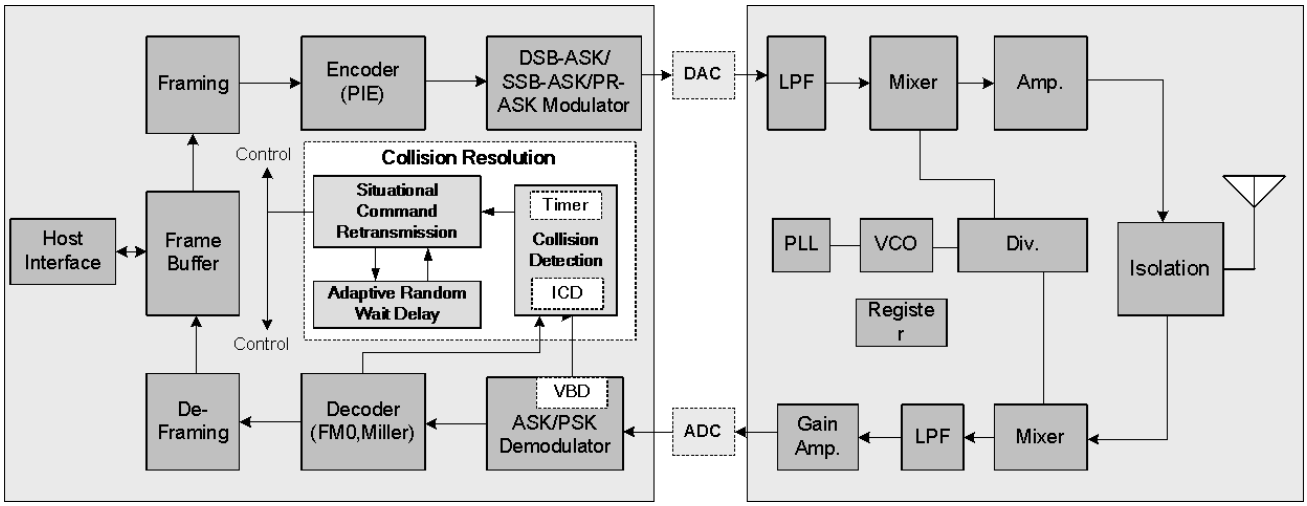

Figure 4 — Interrogator Architecture including Collision Detection Logic

7.2.1 Collision Detection Module

The following inputs are required to detect all 3 different types of collisions:

— Tag response period indicator from timer

— Preamble detect signal from FM0/Miller decoder module

— Cyclic Redundancy Check (CRC) error detect signal from FM0/Miller decoder module

— Valid bit detect signal from Valid Bit Detection module inside the ASK/PSK demodulator module

— Tag response symbol data input from ASK/PSK demodulator module

The only mandatory output of the described Collision Detection module shall be a Collision Type Alarm indicator that allows discriminating among the following different communication scenarios:

1) No collision detected

2) Tag on Tag Collision

3) Multiple Interrogators to Tag Collision

4) Interrogator to Interrogator Collision

Based on the actual value of the Collision Type Alarm indicator, the Collision Resolution module is able to resolve the current communication collision using the mechanism specified in 7.3 and 7.4.

7.2.2 Interrogator Collision Detection (ICD) Module

The purpose of the Interrogator Collision Detection sub-module is to indicate the involvement of a competing interrogator device in an occurring collision such as an Interrogator to Interrogator Collision, see A.4, to be used as an input for the Collision Detection module.

NOTE In the following sub-clauses the term "ICD is positive" is used to indicate that one or more interfering interrogators have been detected, whereas "ICD is negative" is used for the opposite event.

Interference by a nearby mobile or stationary interrogator shall be detected by means of Received Signal Strength Indication (RSSI) where the evaluation of the received signal against the predefined signal threshold value P_{thres} shall be carried out based on the moving average window size W_{Size} that shall be selected in accordance with the implemented sampling interval and air interface specific parameters such as interrogator to tag modulation and encoding type.

The ICD shall be active for the entire tag response period T_{RP} as defined by the basic air interface specification and shall be adapted according the number of bits being transmitted, the link frequency and the number of sub-carrier cycles per symbol (M). In case of tags compliant to ISO/IEC 18000-6 Type C, the tag response period is defined as T_1 + duration of the expected tag response + T_2 if the length of the tag response is known in advance, e.g. transmission of RN16. If the length of the tag backscatter is variable, e.g. in case of the transmission of the UII, the minimum tag response period shall be defined as $\max(T_1 + T_3, T_4)$.

Figure 5 shows how the ICD sub-module shall be implemented using a moving average filter in combination with a comparator, whereas the detailed signal flow is illustrated for a dedicated example input in Figure 6.

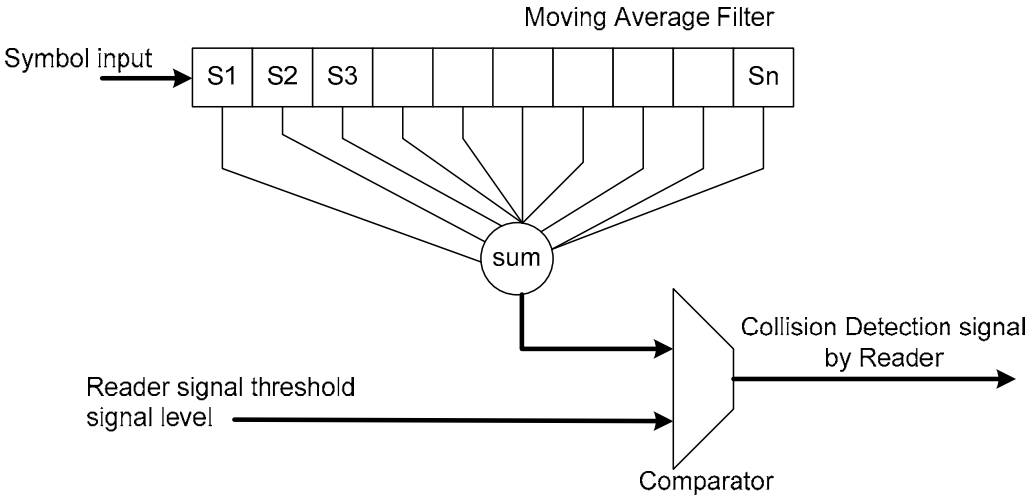

Figure 5 — Interrogator Collision Detection Circuit

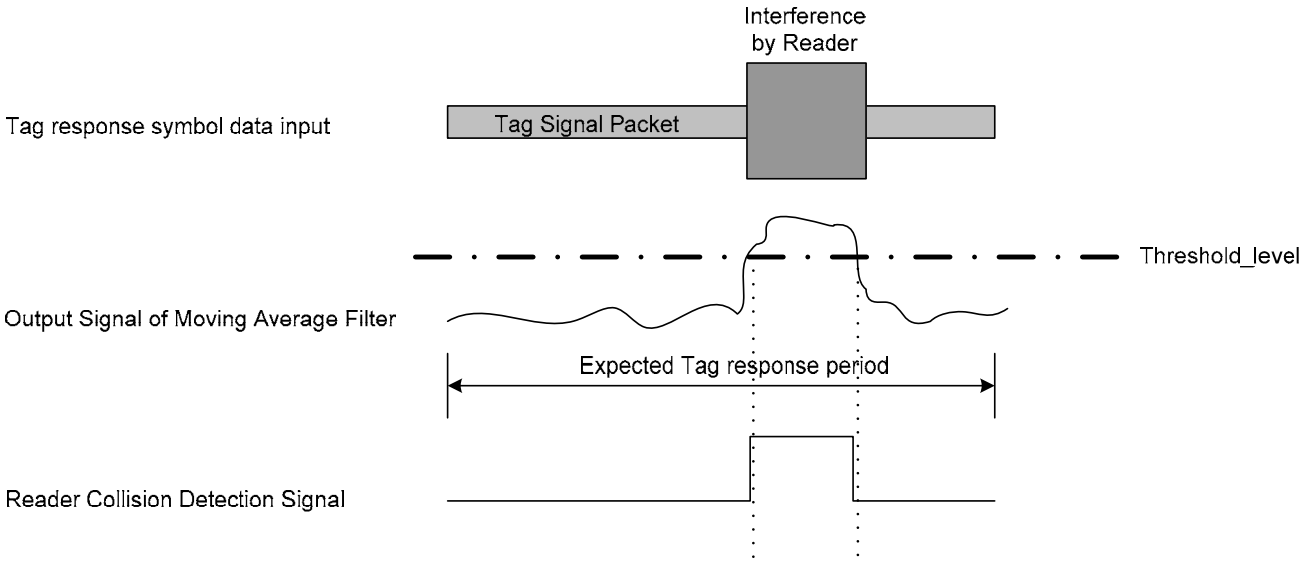

Figure 6 — Example: Signal flow in ICD Module

7.2.3 Valid Bit Detection (VBD) Module

The Valid Bit Detection module is a sub-module of the ASK/PSK demodulator module and has the purpose to indicate the presence of a number of valid logical bits exceeding a dedicated threshold within the observed tag response by detecting rising and falling signal edges, i.e. modulated sub-carrier, within the tolerances defined by the air interface specification.

The following facts are known to the interrogator as the interrogator talks first (ITF) approach of the underlying air interface enables it to dictate all relevant characteristics of the return link (T->R communication link) to the tag by using the following features of the Query command:

— Return link encoding scheme (FM0 or Miller)

— Return link rate in Hz (and hence the bit-time)

— Number of sub-carrier cycles per bit (M=1|2|4|8)

The VBD module shall be able to detect valid return link bits based on the signaling (modulation, encoding scheme, waveform specification …) defined by the basic air interface specification. Refer to Figure 7 for an example of valid bit detection within a Miller-4 encoded signal, where a data-0 bit is defined as a series of 4 periodically occurring rising and falling signal edges within an interval of M/BLF.

NOTE Within the scope of this document the term "VBD is negative" is used to indicate that the VBD module could not detect a sufficient number of valid bits, whereas "VBD is positive" means that a sufficient number of valid bits could be detected in order to distinguish ongoing tag backscatter from noise.

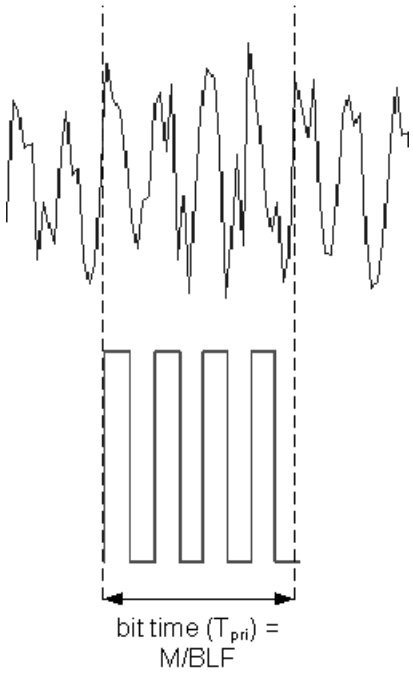

Figure 7 — Example for Valid Bit Detection – Miller 4 Encoded Signal

Valid bit detection shall be based on an observation window of 16 bits (bit duration to be set according selected tag to reader link rate).and shall be carried out using either 8, 16, or 32 samples per bit. Based on the selected return link encoding (FM0 or Miller Modulated Subcarrier) and the implementation dependent number of samples per symbol, the minimum number of valid bits to be used for implying a positive output of the VBD module shall be selected according Table 2.

Table 2 — Minimum Number of Bit Detections Required for Distinction from Noise

Samples per symbol	Decoder	Minimum number of NOT CONTINOUS valid bits (see NOTE 1) required to be detected in order to indicate a positive output of the VBD module	Minimum number of CONTINOUS valid bits (see NOTE 2) required to be detected in order to indicate a positive output of the VBD module
8	FM0	9 bits	4 bits
	M=2	3 bits	2 bits
	M=4	1 bits	1 bit
16	FM0	3 bits	2 bits
	M=2	1 bits	1 bit
	M=4	1 bit	1 bit
32	FM0	1 bit	1 bit
	M=2	1 bit	1 bit
	M=4	1 bit	1 bit

NOTE 1 The number of valid bits does not need to be not continuous. It is just the sum of the valid bit detections within the VBD observation window.

NOTE 2 The number of valid bits shall be continuous. It is the sum of the serial valid bit detections within the VBD observation window.

7.2.4 Rules to Determine the Type of Occurring Collisions

In the Collision Detection module the following rules shall be applied to classify an observed communication collision:

Rule 1: Rule for detecting Multiple Interrogators to Tag Collisions

— No valid preamble detected

— VBD is negative

— No interrogator interference detected (ICD is negative)

Figure 8 show an example of a possible Multiple Interrogators to Tag Collision.

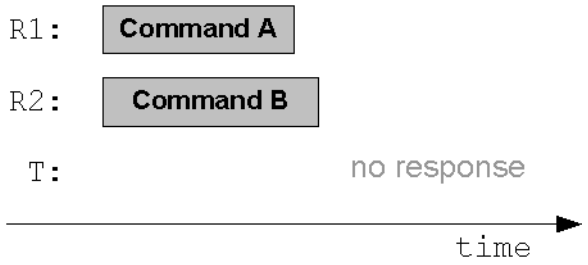

Figure 8 — Example: Multiple Interrogators to Tag Collision

Rule 2: Rule for detecting Interrogator to Interrogator Collisions
A) — Valid preamble detected — CRC error — ICD is positive B) — No valid preamble detected — ICD is positive

Two examples of Interrogator to Interrogator Collisions are presented in Figure 9 and Figure 10.

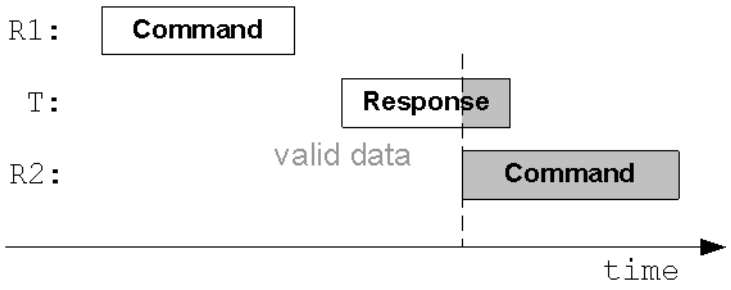

Figure 9 — Example 1: Interrogator to Interrogator Collision

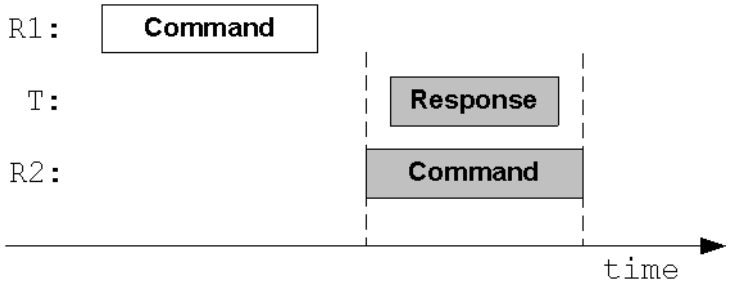

Figure 10 — Example 2: Interrogator to Interrogator Collision

Rule 3: Rule for detecting Tag on Tag Collisions

A)

- Valid preamble detected

- CRC error

- ICD is negative

B)

- No valid preamble detected

- VBD is positive

- ICD is negative

An example for a typical Tag on Tag Collision is shown in Figure 11.

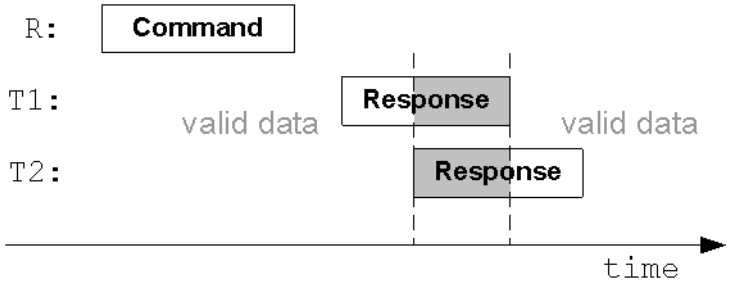

Figure 11 — Example: Tag on Tag Collision

A summary of the rules described in this sub-clause is provided in Table 3.

Table 3 — Summary of Rules to Determine the Type of Occurring Collisions

Collision Type / Detection	Tag on Tag collisions		Multiple Interrogators to Tag collisions	Interrogator to Interrogator collisions	
ICD	Negative		Negative	Positive	
VBD	Positive		Negative	-	
VPD	Positive	Negative	Negative	Positive	Negative
CRC error	Positive	-	-	Positive	-

— ICD : Interrogator Collision Detection

— VBD : Valid Bit Detection

— VPD : Valid Preamble Detection

NOTE Tag on tag collision is the common collision according ISO/IEC 18000-6 and therefore the collision arbitration methods that are defined there apply.

7.3 Command Retransmission (Mandatory)

In case a communication collision is detected by the interrogator after a tag has already been separated to the current response slot, i.e. during the period of tag acknowledgement and tag access, the affected command shall be reissued in order to resolve possible Multiple Interrogators to Tag- or Interrogator to Interrogator Collisions.

During the phase of tag anti-collision, commands shall not be retransmitted unless a Multiple Interrogators to Tag- or Interrogator to Interrogator Collision can be determined by the affected interrogator through any adequate means, i.e. command retransmission is prohibited for all interrogators not equipped with a collision diagnostics function capable of discriminating among the three different types of communication collisions described in Annex A. Instead, tag anti-collision shall be applied to address the common case of Tag on Tag Collisions caused by several tags responding in the same communication slot.

The number of possible retransmission attempts due to collisions is unlimited and may be adapted to fit to the needs of the application. Retransmission may last until a valid tag response is received. The introduction of an upper limit for unsuccessful retransmission attempts in case of emerging collisions is encouraged in order to avoid perpetual communication traffic and resulting communication collisions.

If a receiver timeout is detected by the interrogator (no tag response is received within a predefined time) commands shall be retransmitted only once.

It is important that with respect to emerging receiver timeouts, commands are not repeatedly retransmitted. Instead, anti-collision shall be applied if the receiver timeout persists, e.g. the number of slots may be decreased, if there are still undetected tags expected to be in the interrogation zone to ensure that there is at least one tag allowed to answer the interrogator in the current slot before a command is reissued again to recover from a possible Multiple Interrogator to Tag Collision.

Additionally, it has to be considered that command retransmission makes only sense if the involved tag(s) remain susceptive to the command, i.e. do not change their internal state in the meanwhile due to a receiver timeout. In case of the UHF air interface specified by ISO/IEC 18000-6 Type C, tags are forced to switch back to state Arbitrate in case of a T2 timeout in the Reply- or Acknowledged states, which implies that reissuing a command after a wait time greater equal T2 would be ineffective as it would never result in a tag response. Therefore commands shall only be retransmitted if the expected internal state of the tags addressed by the command does not implement a timeout or the selected wait time (see 7.4) for the command retransmission is smaller than the minimum value of the timeout as specified by the air interface specification. Based on the additional constraint that interrogators are only suspended for a random wait period in the early phase of an inventory round, i.e. are not longer suspended if one or more tags have already been separated, this potential fatality can be automatically ruled out in advance, see 7.4.

Figure 12 shows the whole situational command retransmission scheme in overview, including the application of the random wait time specified in detail in 7.4.

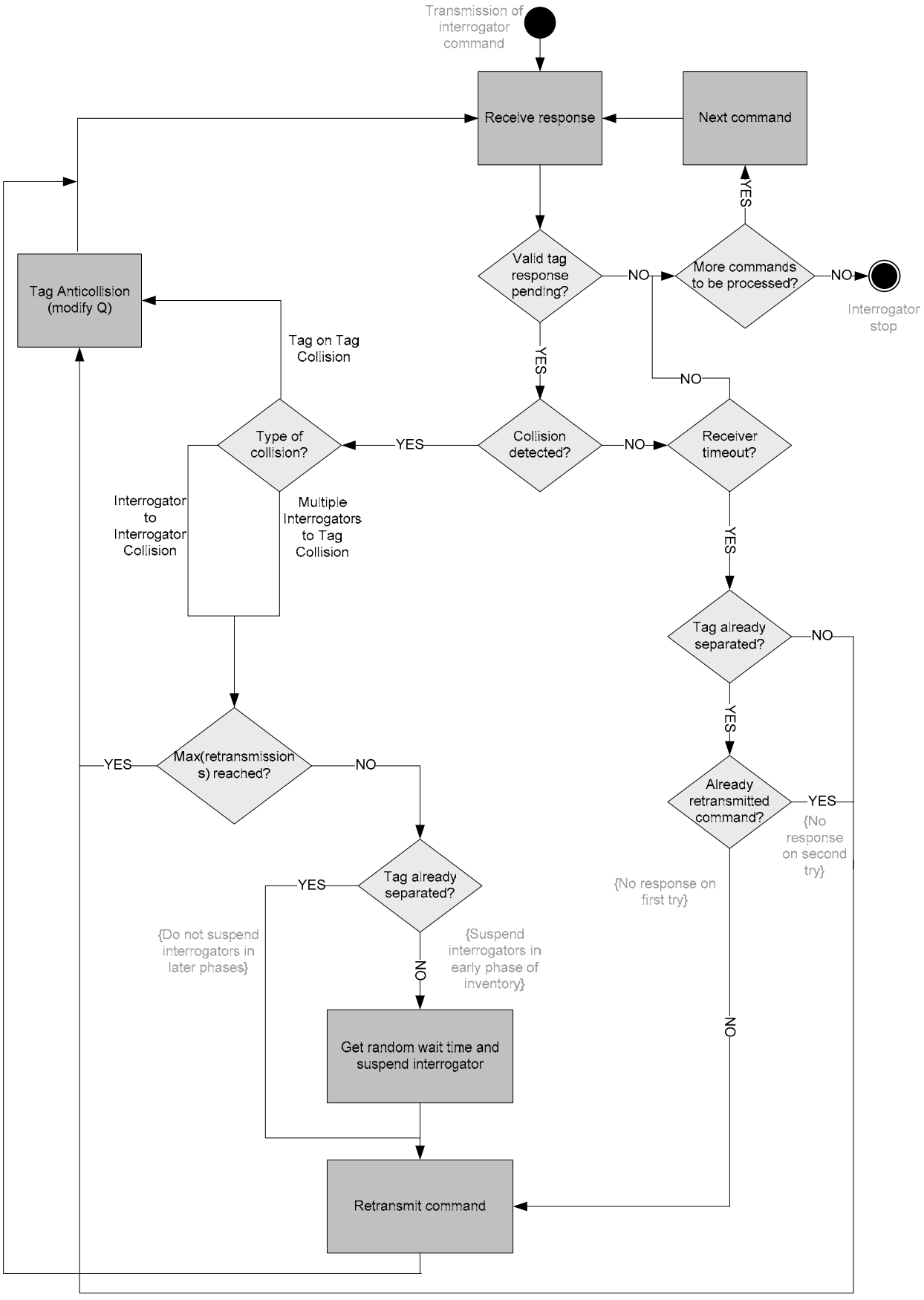

Figure 12 — Block Diagram of Command Retransmission Scheme

7.4 Random Wait Time (Mandatory)

7.4.1 General

To mitigate the negative effects of concurrent command transmissions in Mobile RFID environments, a random wait time T_R is introduced aiming at breaking the regular transmit flows ruled by the underlying basic air interface specification and the resulting sequences of colliding interrogator commands.

To avoid a livelock (starvation) where two competing interrogators block each other with recurrent (re)transmission attempts, a random wait time shall be applied between an unsuccessful transmission of a message and its retransmission if all further preconditions regarding the time of applying the random wait time specified in 7.4.2 are satisfied.

Additionally, a random wait time shall be applied between two subsequent inventory commands dedicated to the process of tag anti-collision, e.g. between a Query and a QueryAdjust in case of ISO/IEC 18000-6 Type C, if the type of the current collision cannot be unambiguously determined or if the interrogator is not equipped with a collision diagnostics function, and if all further preconditions regarding the time of applying the random wait time specified in 7.4.2 are satisfied.

7.4.2 When to Apply the Wait Time

Interrogators shall be suspended for a random wait time before retransmitting a command during the phase of tag selection or tag inventory if no tag has yet been acknowledged (tag singulated and ACK transmitted but no response received) nor inventoried in the course of the current inventory pass.

In contrast, interrogators shall never be suspended during tag access.

It is important that the random wait period is not applied at default but only in case an interrogator is still at the begin of its inventory round, i.e. has not yet separated a tag. Otherwise, two colliding interrogators would both be automatically suspended after a collision and would possibly continue issuing commands almost in parallel after a short transmission break, which would again result in a collision (follow up collision).

Instead, only one of the two interrogators is blocked while the other can retransmit the last command and probably even finish the whole inventory round in the meantime, provided that the second interrogator is suspended for a sufficient period of time.

NOTE The specified approach addresses two different issues at the same time: a) it helps to reduce the probability of overlapping retransmission patterns and hence follow up collisions, and b) it helps to implement a fair wait strategy by assuring "older" inventory rounds are in general finished before "newer" rounds.

Informative examples about when to apply the random wait time can be found in Annex D.

7.4.3 Wait Time Selection

The random wait time T_R needs to be selected accordingly to maximize performance and minimize the probability of a follow up collision. Therefore the wait time shall be randomly picked from an interval defining the minimum and maximum wait time in a way to achieve good results on average.

NOTE The random wait time can be selected by picking a (pseudo) random integer number in between the thresholds specified by Fmin and F_{max} or an integer value that corresponds to a number of clock cycles where the duration of those clock cycles corresponds to a time value between the values given by F_{min} and F_{max}.

The time interval in which protocol data units can overlap is called contention period (CP). During the contention period an interrogator command or tag response is vulnerable and can be destroyed due to interference. To reduce vulnerability of a single protocol data unit or a typical sequence of commands as issued during tag inventory, the random wait time is selected to be proportional to the duration of the mentioned protocol data units.

The lower threshold for the random wait time (MinWaitTime) shall be calculated according to the following formula:

$$F_{\min}: \; MinWaitTime = c * duration(longestExpectedPDU)$$

where *c* is a constant that may be set according to the characteristics of the application (at default c = 1.0) and "duration" is a function returning the time required to transmit a certain protocol data unit over the given air interface at the pre-selected link rates.

This approach ensures that if two competing interrogators R_1 and R_2 use the same link rates and hence calculate the same lower threshold for the wait time, no follow up collision with the same protocol data unit will occur when R2 retransmits its inventory command due to a communication collision after a random delay.

Figure 13 illustrates this context assumed that the longest protocol data unit to be transmitted is the tag response to an ACK command. The scenario shows an interrogator R_1, which has already singulated a tag T to the current response slot but fails to acknowledge the tag due to a second interrogator R_2, which issues a Query that collides with the tag's reply. It is obvious that in order to avoid follow up collisions, interrogator R_2 needs to be suspended at least for the duration of tag T transmitting its response to the ACK consisting of 16 protocol bits (PC), the UII, and a CRC-16, given that tags in general do not quit transmitting in case of a collision.

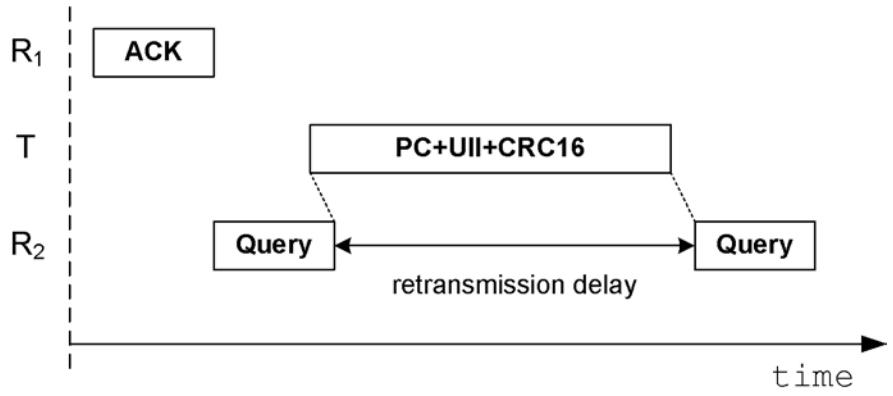

Figure 13 — Definition of Minimum Retransmission Wait Time

However, a follow up collision with a different command issued by interrogator R1 may still occur but may be minimized by setting the maximum retransmission wait time to a value significantly higher than the lower threshold.

Depending on what commands are supported by an interrogator (mandatory commands vs. optional commands) and depending on the actual application (inventory only or inventory + tag access), the longest expected protocol data unit may differ from interrogator to interrogator. Interrogators shall always refer to the maximum of the longest protocol data units to be sent or received in the next inventory round and the longest mandatory command supported by the basic air interface specification in use when calculating the upper- or lower boundary of the retransmission wait time.

Regarding the protocol data units transmitted on the return link (tag responses) the return link rate dictated by the interrogator in the course of an inventory round, e.g. by issuing a Query command, shall be applied for the determination of the longest expected protocol data unit. Wherever the number of bits to be received is unknown in advance, e.g. backscatter of the UII, the highest possible number of bits in the context of the current application shall be assumed. This means for example that if the application supports UII lengths up to 96bits, no more than 96bits shall be used for the determination of the longest expected PDU even if the maximum length of the tag backscatter supported by the basic air interface specification is higher.

The upper threshold for the random wait time (MaxWaitTime) shall be calculated according to the following formula to set it in relation to the duration of an idealized inventory round consisting of Select, Query, a single RN16 response, ACK, and the tag response to the ACK command:

$$F_{\max}: \; MaxWaitTime = c * duration(Select + T4 + Query + T1 + RN16 + T2 + ACK + T1 + UII)$$

where the *c* is again the placeholder for a constant factor.

The results returned by the function "duration" used in formula F_{max} shall depend on the forward and return link rates to be used by the interrogator in the next inventory round and on the expected length of the tag response to the ACK command. Similar to formula F_{min}, the highest possible number of bits in the context of the current application shall be assumed for the determination of the length of UII to be backscattered by the tags.

The rationale of this approach is illustrated by Figure 14, which shows an idealized scenario where a maximum retransmission threshold according to formula F_{max} can potentially resolve a collision between two interrogators R_1 and R_2 if it is picked at random.

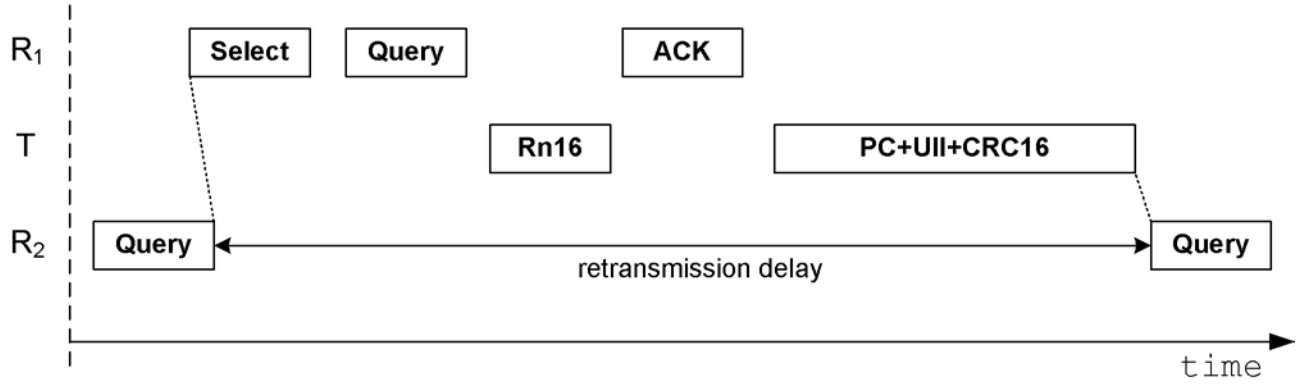

Figure 14 — Definition of Maximum Retransmission Wait Time

Examples of a valid definition of MinWaitTime and MaxWaitTime in dependency on the link rate and command length are given in Annex F.

7.4.4 Tuning of the Random Wait Time

To provide best fit with the needs of a dedicated application, parameter *c* is used to tune the upper and lower retransmission wait thresholds in order to find best balance between performance and upcoming collisions depending on the actual application scenario.

Parameter *c* used in formulas F_{min} and F_{max} shall be set to a value greater equal 1.0 (c >= 1.0) at begin of each inventory round and shall not be decreased until a tag could be acknowledged by the interrogator. This is in favor of reducing the probability of collisions caused by this interrogator in order to protect nearby interrogators that may have already advanced to inventory and access one or more tags of the actual population.

After a tag has been successfully detected by an interrogator, parameter *c* may be changed without further restrictions (i.e. parameter *c* may be increased/decreased at the users' discretion at any point of time) for the duration of the remaining inventory round and MinWaitTime and MaxWaitTime may be recalculated accordingly.

NOTE Restricting the initial boundaries for the retransmission wait time helps to implement a "fair" scheme for channel utilization. Interrogators that have already advanced to detecting one or more tags out of a tag population are allowed to implement lower wait times in order to finish their inventory round, whereas "new" interrogators that become active in the meantime are forced to use the default settings, which result in a lower duty cycle.

Due to the fact that the prevailing RFID air interface specifications allow for user defined link rates two competing interrogators are likely to operate at different link rates, which will result in a gap between the wait time thresholds calculated by a interrogator R_1 and a interrogator R_2. Therefore, it is recommended to adapt parameter *c* in case of recurrent follow up collisions. Inversely, the same parameter can also be adapted in favor of better overall throughput if the number of observed collisions is enduringly low.

An example how parameter *c* could be modified in the course of an inventory round can be found in Annex C.

7.5 Practical Implementation

In general, the air interface specification for Mobile RFID interrogators specified in this document may be combined with any compatible basic air interface specification developed for the usage with stationary RFID interrogators. An existing air interface specification to be used with this International Standard shall be considered compatible with this International Standard if supporting this air interface does not conflict with being compliant to this International Standard, and vice versa.

For a detailed definition on how to claim conformance with this International Standard refer to Clause 2.

A pseudo-code notation of the collision arbitration and collision avoidance algorithm described in this chapter, adopted for usage with the air interface specification defined by ISO/IEC 18000-6 Type C can be found in Annex B.

8 Tag Memory

8.1 General

Tag memory shall be organized according to the underlying basic air interface. Additionally, tags according to this International Standard shall provide data structures dedicated to Mobile RFID as specified in 8.2.

8.2 Data Structures Dedicated to Mobile RFID

8.2.1 MIIM content name stored in the User Memory

RFID tags designed for usage in Mobile RFID applications shall provide a MIIM content name in its user memory enabling for fast and convenient access to a Mobile RFID service. The memory address in the user memory to be used for this purpose may be allocated at the manufacturer's discretion and shall be pointed to by the mechanism specified in 8.2.2.

Figure 15 shows how the MIIM content name shall be arranged in the user memory. The MIIM content name shall be preceded by 16 bits containing an 8 bit length field and 8 bit code type as Table 4. The data itself and shall be stored in sequential order starting with the first character, followed by the second character up to the last character of the N-bit MIIM content name. Characters shall be stored most significant bit (MSB) first and are composed to be values according the specific code at the code type field.

Table 4 — MIIM content name code type

Code type	Code list
00_h	RFU
01_h	ISO/IEC 8859-1
02_h	ISO/IEC 8859-2
03_h – 10_h	RFU
11_h	ISO/IEC 10646(UTF-8)
12_h	ISO/IEC 10646(UTF-16)
13_h	ISO/IEC 10646(UTF-32)
14_h - FF_h	RFU

The MIIM content name shall be prefixed by header consist of a 8-bit length field and a 8-bit code type field. Currently, only the 8 most significant bits are used as a length indicator, whereas the remaining 8 bits are a code type indicator. The length indicator shall contain the length of the MIIM content name field in bytes as a numerical (non EBV) value.

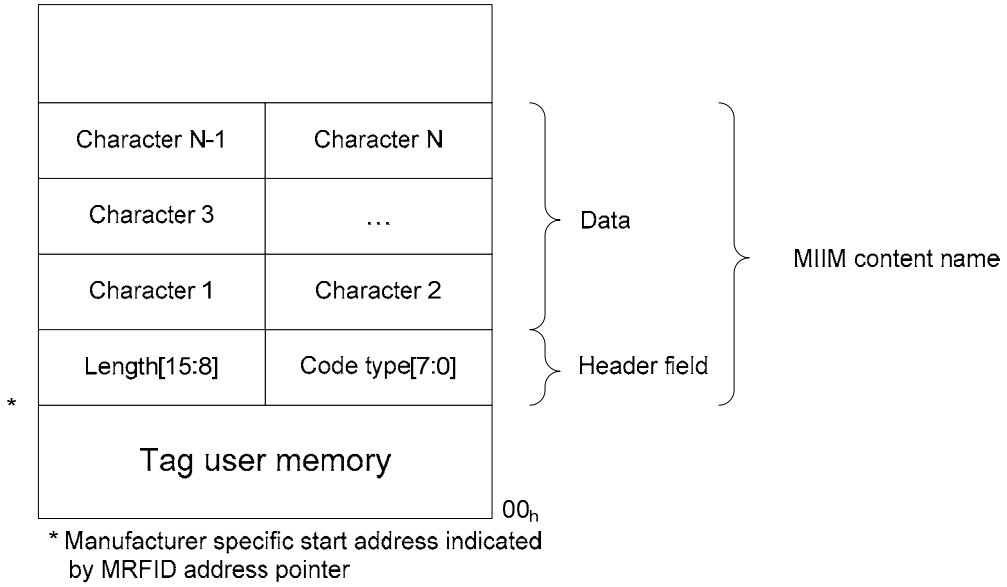

Figure 15 — MIIM content name stored in User Memory

Tags providing MIIM content name dedicated to Mobile RFID in their user memory shall use the mechanism specified in 8.2.3 to indicate the presence of such data to interrogators.

8.2.2 Mobile RFID Address stored in TID Memory

Tags that support MIIM content name in its user memory, see 8.2.1, shall provide a valid (non zero) 32-bit Mobile RFID Address at memory locations 300h to $31F_h$ of the TID memory according to ISO/IEC 18000-6C.

The Mobile RFID Address in TID memory shall point to the address where the code type of the MIIM content name can be found, see 8.2.1.

The structure of the Mobile RFID Address shall be as shown in Table 5.

Table 5 — Structure of Mobile RFID Address

Bit position TID memory	300_h:305_h	306_h:307_h	308_h:$31Fh_h$
	RFU	MB	Start Pointer [23:0]
# of bits	6	2	24
description	Reserved for future use	Memory bank selector	Starting address of MIIM content name in user memory(LSB of code type field)

8.2.3 Usage of Extended Protocol Control to Indicate Support of MIIM content name

To indicate that the data structures according 8.2.1 are supported, tags shall assign the Extended Protocol Control (XPC) bits as described in Table 6:

Table 6 — MIIM allocation of XPC bits

Bit 213_h	Bit 212_h	Meaning
0	0	no MIIM
0	1	MIIM content name
1	0	RFU
1	1	RFU

8.3 Data Exchange between Interrogator and Tag

8.3.1 Overview

In order to transmit the optional MIIM content name specified in 8.2.1 from the tag to the interrogator one of two possible mechanisms shall be used:

— The Mobile RFID interrogator may request the MIIM content name being included in the tag response to the ACK command appended to the UII by using the Flex_Query command defined in 9.2 in the course of an inventory round, or

— The Mobile RFID interrogator may use the Mobile RFID Address defined in 8.2.2 to find out the starting address and memory ranges where the MIIM content name is stored on the tag to use these parameters to retrieve the MIIM content name by issuing a Read command.

8.3.2 Direct Access of MIIM content name by Appending MIIM content name to the UII (optional)

The structure of the tag response to the ACK command in case of MIIM content name being requested by use of Flex_Query as specified in 9.2 including the MIIM content name indicator according 8.2.3 and the MIIM content name field according 8.2.1 are shown in Figure 16, where it is assumed that the tag has been addressed to participate in the inventory round by the according Tag Type Select bit of the Flex_Query.

Steps to be carried out:

1) Initiate a new inventory round by issuing a Flex_Query
   i) MRFID response flag set to 1_2
   ii) Tag Type Select bit 3 (Mobile RFID) set to 1_2
2) Singulate a tag
3) Acknowledge tag using the ACK command

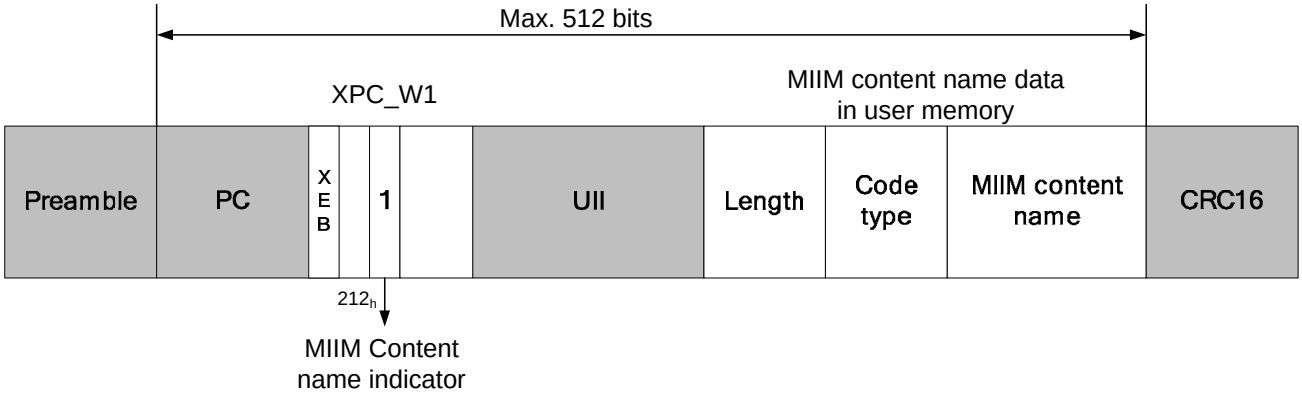

Figure 16 – Example of Appending MIIM content name to the UII

In case the data fields exceed 512 bits (see Figure 16), then the MIIM content name shall be truncated accordingly. As the MIIM content name length does not fit to the actual transmitted MIIM content name, this notifies the reader that the MIIM content name has been truncated. Therefore, it is recommended that the MIIM content name does not exceed 16 bytes.

8.3.3 Indirect Access to MIIM content name by Using a Separate Read

Complementary to the concept described in 8.3.2, the MIIM content name can be read by the interrogator by using an access command such as Read in ISO/IEC 18000-6 Type C.

Steps to be carried out:

1) Separate and acknowledge tag

2) Retrieve access handle

3) Read Mobile RFID Address stored in TID memory

4) Read 8-bit MIIM content name length field and 8 bit MIIM content name code type field stored at address indicated by Mobile RFID Address

5) Read MIIM content name field according length field.

NOTE This access method does not require the support of any additional commands.

9 Extended Command Set

9.1 Overview

Additional to the command set of the underlying air interface, Mobile RFID tags and interrogators may support the optional commands specified in this clause for convenience.

9.2 Flex_Query(optional)

Mobile RFID interrogators may utilize the Flex_Query command, which is specified in ISO/IEC 18000-6, for the following purposes:

— Select/deselect Mobile RFID tags to participate in the current inventory round by means of the Flex_Query Tag Type Select field, see Table 8

— Request transmission of MIIM content name appended to the UII by asserting the according MRFID Response flag, see Table 7

The structure of the Flex_Query command shall be according ISO/IEC 18000-6 with exception of bit 22 utilized as MRFID Response flag under the scope of this International Standard, and a different meaning of bit 3 of the Tag Type Select field. Table 7 is copied from ISO/IEC 18000-6 and shows the structure of the Flex_Query command defined in ISO/IEC 18000-6.

Table 7 — *Flex_Query* command (optional)

	Command	**Tag Type Select**	**SS Response**	**MRFID Response** Note 2	**DR**	**M**	**TRext**	**Sel**	**Session**	**Target**	**Q**	**CRC-5**
# of bits	8	12	1	1	1	4	1	2	2	1	4	5
description	11001111	Note 1	0: Disable 1: Enable	0: Disable 1: Enable	0: DR=8 1: DR=64/3	0000: M=1 0001: M=2 0010: M=4 0011: M=8 0100: M=16 0101: M=32 0110: M=64 0111 to 1111: RFU	0: No pilot tone 1: Use pilot tone	00: All 01: All 10: **~SL** 11: **SL**	00: S0 01: S1 10: S2 11: S3	0: *A* 1: *B*	0–15	

NOTE 1 See Table 8 for full definition of tag types to be pulled into the Query round.

NOTE 2 The MRFID response flag authorizes automatic transmission of MIIM content name in cases where Mobile RFID tags have been selected. Tags without MIIM content name shall ignore the MRFID response flag.

The Tag Type Select field shall be implemented according ISO/IEC 18000-6 except bit 3, which shall be used to select/deselect Mobile RFID tags compliant to this International Standard to participate in the inventory round initialized by the according Flex_Query command, see Table 8.

Table 8 — *Flex_Query* command Tag Type Select field

RFU	**RFU**	**Mobile RFID**	**Sensor Alarm**	**Full Function Sensor**	**Simple Sensor**	**RFU**	**RFU**	**RFU**	**Battery Assisted Passive**	**RFU**	**Passive (RFU)**
1	1	1	1	1	1	1	1	1	1	1	1
		0: Disable 1: Enable	0: Disable 1: Enable	0: Disable 1: Enable	0: Disable 1: Enable				0: Disable 1: Enable		0: Disable 1: Enable

Mobile RFID tags shall respond to an ACK command with the response shown in Table 9 in case of participating in an inventory round initiated by a Flex_Query (bit 3 of the Tag Type Select field = 1_2) and MRFID response being requested. Otherwise, an appropriate error code shall be backscattered.

The MIIM content name attached to the UII shall be truncated for ACK commands to ensure that the total reply length does not exceed bits (excl. CRC-16).

Table 9 — Response to the ACK command including MIIM content name

	Response	**MIIM content name**	**CRC-16** (PacketCrC)
#bits	512		16
#bits detail	5 – 512	0 - 507	16
description	{PC, XPC, UII} or {00000_2, truncated UII} as specified for the ACK command	Truncated MIIM content name (if supported by the tag)	

The tag response to the ACK command shall be protected by a 16-bit PacketCrC, which is a dynamic CRC according ISO/IEC 18000-6.

NOTE In case the there is no response to a Fley_Query command, it is recommend to use the Query command. There is no particular means to indicate the interrogator in advance whether a Flex_Query command is supported by a tag.

Annex A
(informative)

Communication Collisions

A.1 Introduction

The following types of collision may occur in Mobile RFID applications:

1) Tag on Tag Collisions

2) Multiple Interrogators to Tag Collisions

3) Interrogator to Interrogator Collisions

A.2 Tag on Tag Collision

This type of collision is the most common type of collision and may even occur in synchronized RFID environments. An inventory command issued by a single interrogator is answered by two (or more) tags at the same time, which causes the parallel tag responses to interfere with each other, see Figure A.1 — Tag on Tag Interference. As a consequence a corrupted tag response (decoding errors) is observed at the interrogator and no valid tag response can be separated.

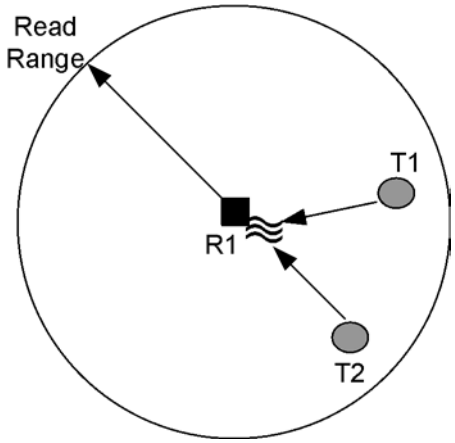

Figure A.1 — Tag on Tag Interference

This type of collision is handled by the anti-collision algorithm described by the basic air interface specification, e.g. ISO/IEC 18000-6 Type C.

If the usage of RFID handhelds is limited to a single frequency channel and/or the forward and return link cannot be sufficiently spectrally separated, tag responses may also interfere with interrogator commands and vice versa resulting in two additional types of communication collisions.

A.3 Multiple Interrogators to Tag Collision

This kind of collision is a result of multiple interrogators operating at close proximity without implementing a synchronization mechanism or LBT. Commands issued by two or more different interrogators interfere in a way that the decoding of a valid interrogator command is not feasible at the tag.

Figure A.2 — Multiple Interrogators to Tag Interference illustrates the mentioned scenario.

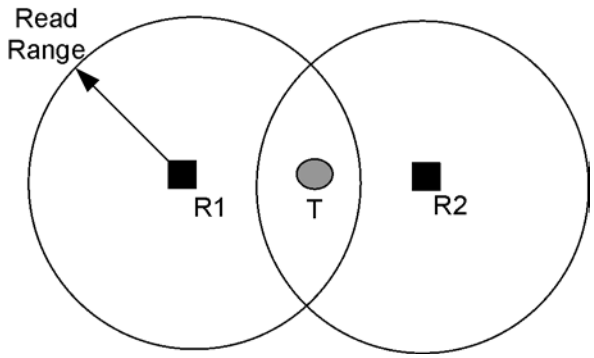

Figure A.2 — Multiple Interrogators to Tag Interference

A.4 Interrogator to Interrogator Collision

This kind of collision happens, if an inventory command issued by a interrogator R2 collides with the tag response to a command previously issued by a different interrogator R1. In such a case, a corrupted tag response is detected by interrogator R1 and may even result in interrogator R1 mistakenly applying tag anti-collision handling because a common Tag on Tag Collision is assumed. Interrogator to Interrogator Collisions may occur even if the read ranges of the two interrogators do not overlap as shown in Figure A.3 — Interrogator to Interrogator Interference.

Mobile RFID is especially prone to be affected by Interrogator to Interrogator Collisions because unsynchronized multiple interrogator environments are the common case in areas of high RFID traffic, e.g. urban centers.

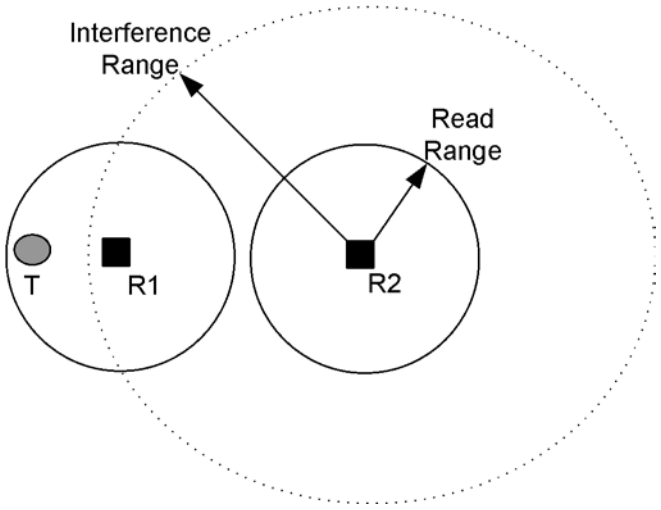

Figure A.3 —Interrogator to Interrogator Interference

Annex B
(informative)

Pseudo-Code Notation of the Collision Resolution Algorithm

This annex provides a pseudo code notation of the media access method specified in Clause 7.

Figure B.1 — Pseudo-Code Notation of the Collision Resolution Algorithm contains an abstract representation of the mechanisms described in the body of this document. A procedural notation similar to that used in the well known C language is used. Comments are marked with "//".

This example is based on using the concepts for mobile RIFD interrogators defined by this International Standard on top of the air interface specification given by ISO/IEC 18000-6 Type C. Therefore, all names used to describe commands and internal interrogator states in the pseudo-code notation are related to this air interface.

Moreover, retransmission wait time calculation is not shown in Figure B.1. It can be assumed that the variation of the algorithm presented in this annex is based on static retransmission wait time calculation based on the formulas defined in 7.4.3 while using a fixed *c*.

Please note that the given code is just an informative illustration. Many details are left to imagination and may not even be indicated. Implementing the algorithm specified in Figure B.1 may not be sufficient to guarantee conformance with this International Standard. A detailed definition of conformance can be found in Clause 2 and Clause 3 respectively.

NOTE The method "anticollision()" referenced in the algorithm should be seen as the default implementation of the collision arbitration mechanism specified by the basic air interface specification. Of course, "anticollision()" needs to check several pre-conditions (e.g. number of slots >1) to decide if it makes sense to issue any further inventory commands such as QueryAdjust or QueryRep in case of a receiver timeout.

```
...
while (1){      //Note 1
  transmit(command);
  receiveResponse();  //this procedure asserts or deasserts a series of status flags

  retrAttempts = 0;
  maxRetrAttempts = X;

  while(validTagResponsePending == true){       //Note 2

       if(collisionDetected){
                  switch(typeOfCollision){
                        case ToT:      //Tag on Tag Collision
                              retransmit = false;
                              applayWaitTime = false;
                              break;
                        case MtoT:     //Multiple Interrogators on Tag Collision
                        case ItoI:     //Interrogator to Interrogator Collision
                              if(retrAttempts < maxRetrAttempts){
                                    retransmit = true;
                                    retrAttempts = retrAttempts+1;
                                    if(internalState <= Reply && tagsDetected == 0){
                                          applyWaitTime = true;
                                    }
                              }
                              break;
                  }
       }else if(receiverTimeout){
             if(internalState <= Reply && tagsDetected == 0{
                  retransmit = false;
                  applyWaitTime = false;
             }else{
                  if(retrAttempts == 0){
                        retransmit = true;
                        retrAttempts = retrAttempts+1;
                  }else{
                        retransmit = false;
                  }
                  applyWaitTime = false;
             }
       }

       if(applyWaitTime == true){
             waitTime = getRandomWaitTime();
             wait(waitTime);
       }

       if(retransmit == true){
             retransmit(last_command);
       }else{
             anticollision();  /Note 3
       }
  }
}
...
```

Note 1

Interrogator send and receive loop. Assumed that interrogator remains always active.

Note 2

In case of commands Query, QueryAdjust, QueryRep, a valid response is only pending, if it is apparent from the context that a tag should have answered in the current slot, e.g. transmitted Query with Q = 0. Else Note2 applies.

Note 3

Default procedure. The number of slots is increased / decreased until all tags have been detected. Detailed behavior, e.g. nr of inventory passes, may be application/ manufacturer dependent.

Figure B.1 — Pseudo-Code Notation of the Collision Resolution Algorithm

Annex C
(informative)

Example: Random Wait Time Adaptation

Figure C.1 shows an example how parameter *c* used to calculate the upper and lower threshold for the random wait time could be dynamically adapted depending on the current collision percentage, which is the average number of collisions per command (ratio of issued commands in relation to valid tag responses) as logged by the interrogator. Diamond shapes are used in the figure to indicate conditional branches whereas rectangular shapes indicate actions. The starting point of the diagram refers to the start of a new inventory round.

In this example, the interrogator is starting its inventory round with c = 1.0. As specified in 7.4, parameter c is not modified until at least one tag has been acknowledged.

After the first tag detection, *c* is decreased by a factor *f* in favor of better throughput if a certain predefined threshold regarding the collision percentage is under stepped, whereas *c* is increased by the same factor *f* if a certain threshold is over stepped in order to reduce the probability of follow up collisions by prolonging the average retransmission wait time.

NOTE 1 There is no exact value given for factor f, because f may depend on the actual situation and should be selected to fit to the needs of the application. In general, one could expect f to be a value between 0.1 and 1.0.

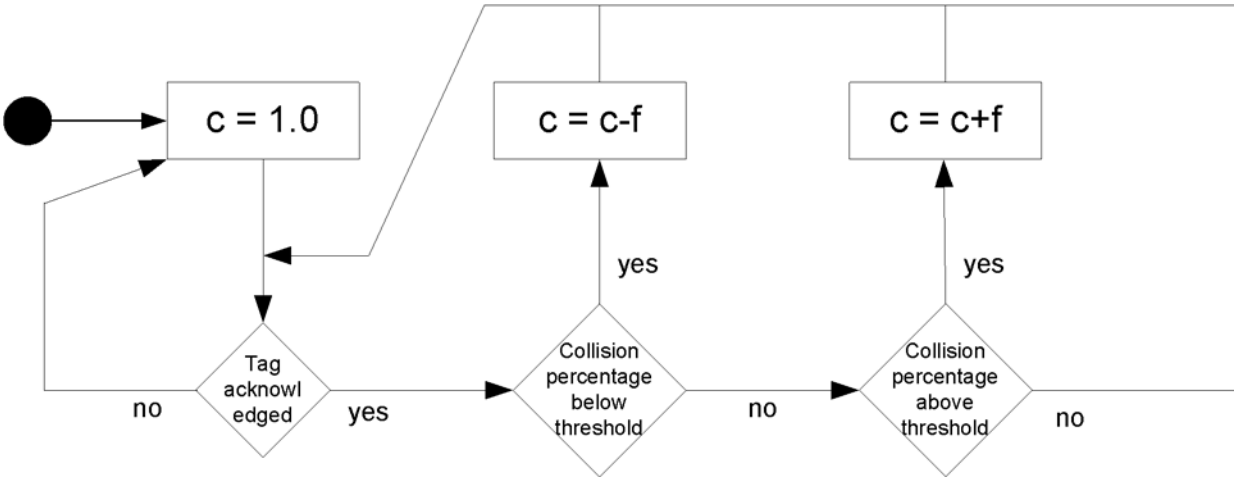

Figure C.1 — Example: Retransmission Threshold Parameter Adaptation

NOTE 2 The collision percentage threshold mentioned in this example is depending on the actual application scenario. For example, if the number of Mobile RFID users at close proximity is expected to be high (e.g. at a bus station) one will use a higher threshold than for an application where the number of users is expected to be low (e.g. using RFID in your own apartment). In general, the term "collision percentage" is used to denote the fraction of tag responses that are lost due to interference, i.e. cannot be successfully decoded by the interrogator.

Figure C.2 is an extension of Figure C.1 and shows how additionally the observed receiver timeout percentage (ratio of unanswered interrogator commands) can be used in combination with a predefined timeout threshold to dynamically increase or reset *c* in case of recurrent receiver timeouts depending on the current collision situation.

In general, all conditions shown in the diagram are referring to the interrogator side. For instance, "Collision visible" means that a collision is detectable for the interrogator by evaluating the received bit stream, which does not include Multiple Interrogators to Tag Collisions that are only revealed on the tag side. Additionally, it

has to be considered that an emerging receiver timeout on the interrogator side is not always due to the absence of a matching tag in the current response slot but may also indicate a hidden Multiple Interrogators to Tag Collision – therefore a connection between the conditions "Timeout percentage above threshold" and "Collision percentage above threshold" has been introduced.

NOTE 3 The term "timeout percentage" refers to the ratio of unanswered interrogator commands. For instance, if an interrogator transmits 4 commands but receives a response (valid or invalid) only on 2 of them, this results in a timeout percentage of 0.5. Commands that do not require any tag response such as Select are not used to calculate the statistics. The exact value of the timeout percentage threshold is depending on the actual application any may differ from one scenario to another.

This approach ensures that retransmissions due to receiver timeouts do not additionally deteriorate the collision situation if collisions are already at their peak when a receiver timeout is observed. Moreover, parameter *c* is reset to its initial value again in favor of protocol performance if the current timeout ratio drops below the timeout threshold. The default value of *c* = 1.0 is never under stepped in case of reception timeouts.

NOTE 4 The term "Collision" used in the diagram is a placeholder for any type of collision. No differentiation between the different possible types of collision (as described in Annex A) is assumed here.

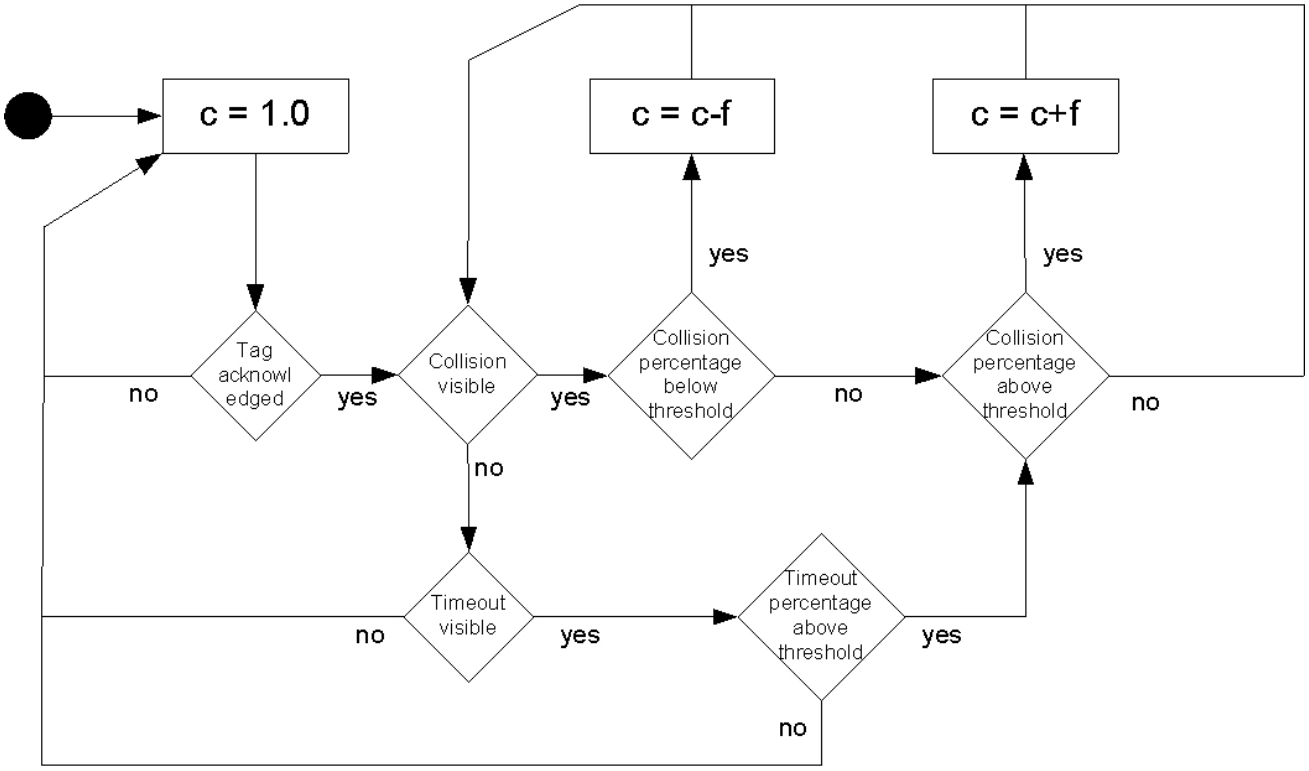

Figure C.2 — Example: Enhanced Retransmission Threshold Adaptation

Annex D
(informative)

Random Wait Time Application Examples

This annex contains a series of informative illustrations of ISO/IEC 18000-6 Type C command and response sequences including communication collisions and the resulting wait time selection compliant to 7.4. The presented examples represent only a selected subset of all possible scenarios.

Figure D.1 shows a Multiple Interrogators to Tag Collision, where interrogator R_1 has already separated a tag T when the collision occurs. As a consequence, R_1 is allowed to immediately reissue the last command following the timing constraints of ISO/IEC 18000-6 C, whereas R_2 is suspended for a random wait time T_R.

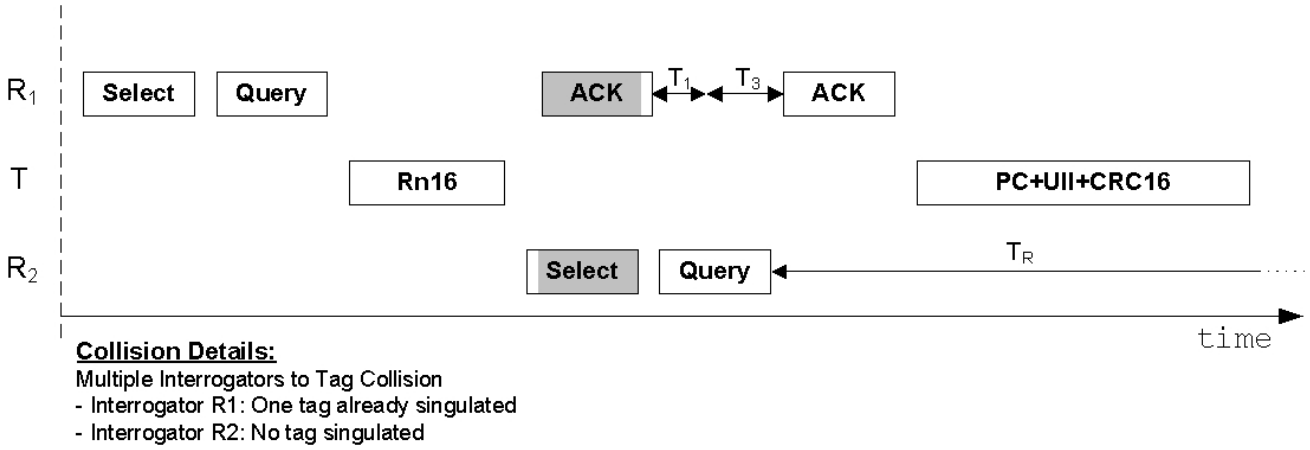

Figure D.1 — Random Wait Time Application Example 1

In contrast, Figure D.2 shows an Interrogator to Interrogator Collision of two interrogators colliding in an early phase of their inventory rounds. Both interrogators have to wait for a random period before being allowed to resume.

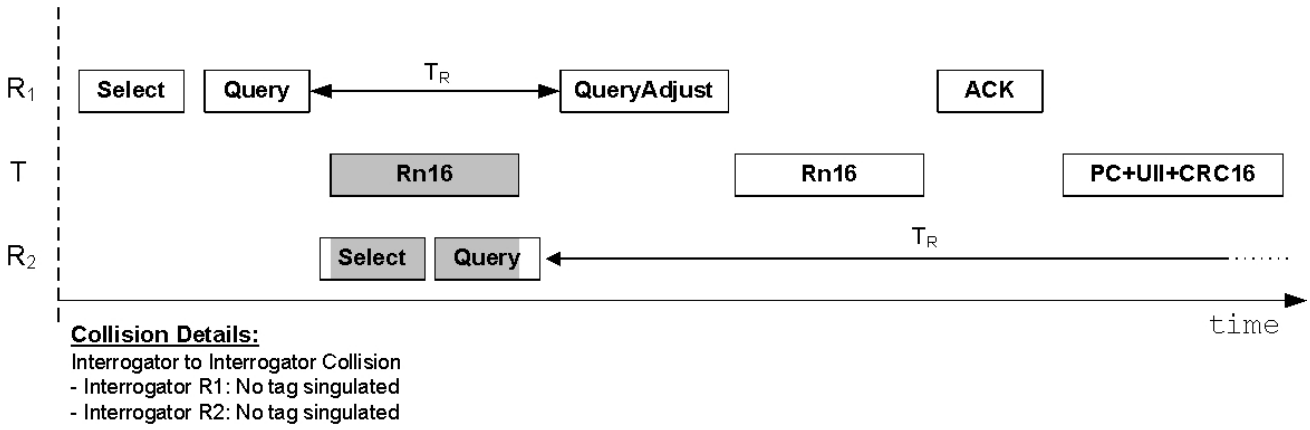

Figure D.2 — Random Wait Time Application Example 2

Complementary, Figure D.3 illustrates what happens if interrogator R_1 has already progressed to separating a tag when the Interrogator to Interrogator Collision occurs. In that particular case, R_1 may retransmit the ACK after T_2 while R_2 is suspended for T_R.

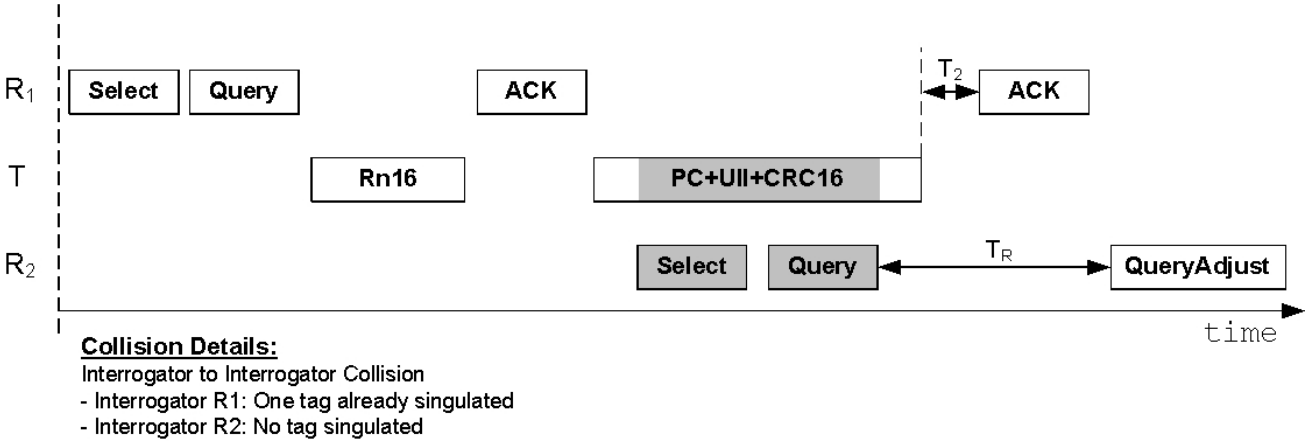

Figure D.3 — Random Wait Time Application Example 3

NOTE Gray-shaded areas represent overlapping sections of commands (collisions).

Annex E
(informative)

Mobile RFID Application Family Identifier

E.1 AFI for Mobile RFID

The AFI value for Mobile RFID applications is assigned by the ISO/IEC 15961-2 registration authority (RA). The actual value applicable for applications according this International Standard was not defined at the time, when this document was edited. Actually value should be obtained directly to the RA.

Mobile RFID interrogators may support either the concept specified in E.2.1 or the concept specified in E.2.2, or both, for the purpose of providing content assigned to the identification data stored on the tag (such as a UII) to the end user.

E.2 Tag Access and Data Processing Method Examples

E.2.1 Based on an Object Directory Service

Mobile RFID interrogators may connect to an Object Directory Service for the purpose of retrieving the web-address of a content provider for the identification data, e.g. UII, read from a tag.

After a tag has been acknowledged by the interrogator and the tag response is available at the interrogator the following steps may be carried out:

Step 1: Decode AFI

Step 2: Decode UII

Step 3: Connect to ODS using the UII as a service parameter

Step 4: Decode URI received from ODS

Step 5: Request content for UII specified by URI from content provider

Figure E.1 shows the required interactions in overview.

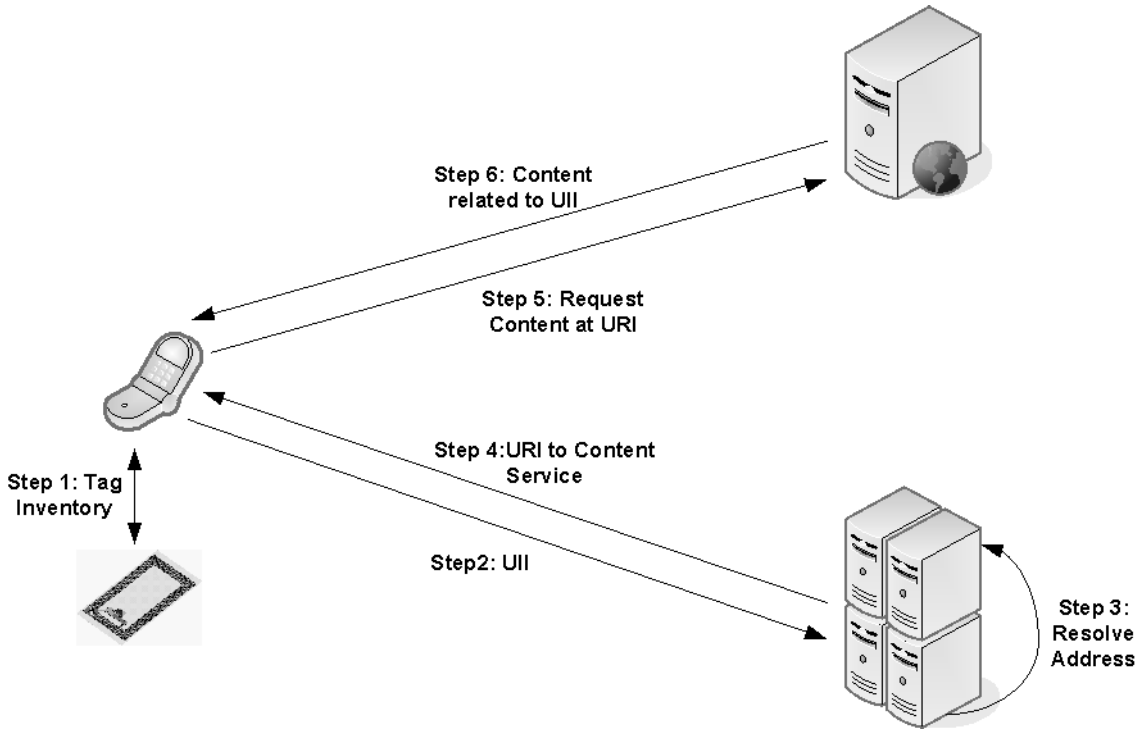

Figure E.1 — Providing Item Related Content using an Object Directory Service

E.2.2 Based on a Stored data

After a tag has been acknowledged by the interrogator and the tag response is available at the interrogator the following steps may be carried out, assumed that the stored data, see 8.2.1, needs to be explicitly requested by the interrogator:

Step 1: Decode AFI

Step 2: Decode UII

Step 3: Read MIIM content name referring to the Mobile RFID service from user memory

(Further sub-steps may be required if memory access is password protected and the tag needs to be put to the Secured state prior to issuing the Read command)

Step 4: Open web page specified by "MIIM content name/UII"

In contrast, the following steps may be carried out if the MIIM content name is present in the tag response to the ACK in case the basic air interface provides the feature of appending user data to the UII in case of non ISO/IEC 18000-6 C tags, or the other type of ACK command, which request UII and MIIM content name at a time, specified in 9.2 is supported by a ISO/IEC 18000-6 C compliant tag:

Step 1: Decode AFI

Step 2: Decode UII

Step 3: Decode MIIM content name

Step 4: Open web page specified by " MIIM content name /UII"

Figure E.2 shows the interactions basically required for this approach regardless of the actual mechanism of obtaining the MIIM content name from the tag.

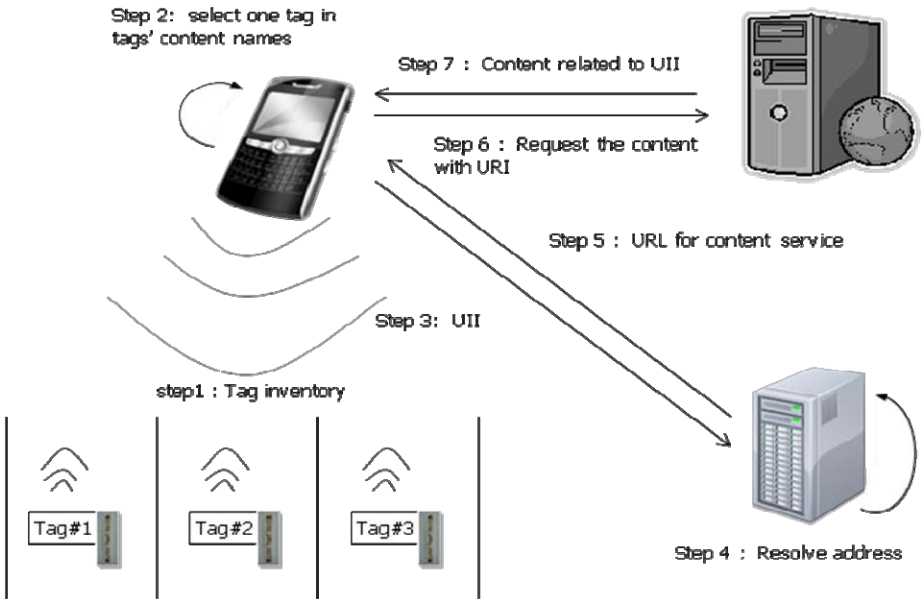

Figure E.2 — Providing Item Related Content using a Stored MIIM content name

E.3 Examples of MIIM content name stored in Mobile RFID user memory

Example 1: Example of MIIM content name stored in user memory

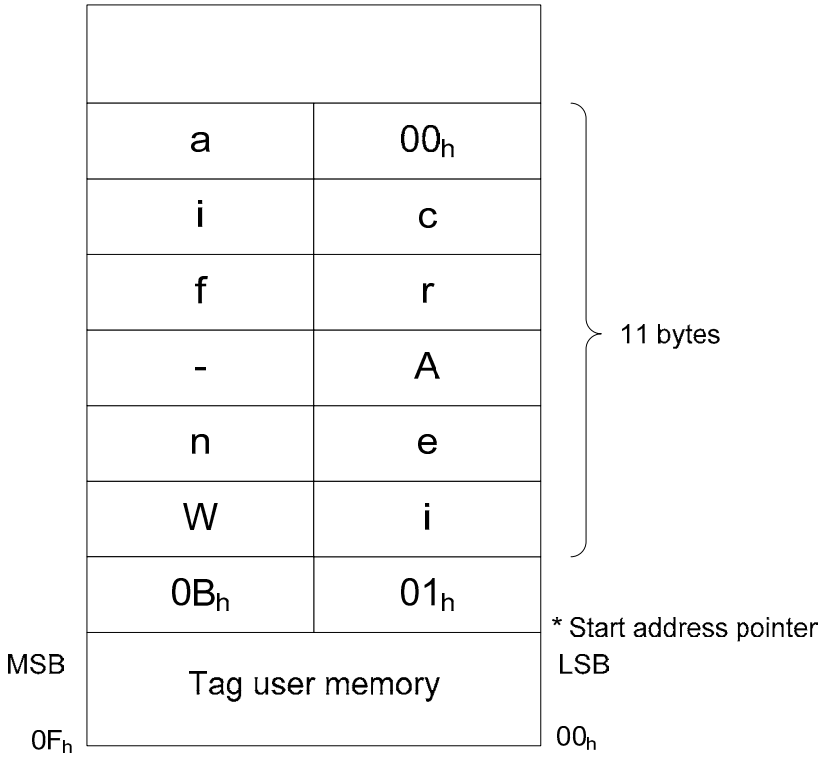

Figure E.3 — Example of MIIM content name and MIIM content name length codes in the tag user memory

NOTE The MIIM content name of the example is Wine-Africa, length 11 bytes ($0B_h$)

Annex F
(informative)

Examples of Minimum and Maximum Wait Time Definition

This annex shows an example on how MinWaitTime and MaxWaitTime can be calculated in an ISO/IEC 18000-6 Type C environment.

As specified in 7.4.3 the lower and upper thresholds for the random wait time according F_{min} and F_{max} are to be selected in accordance with the used link rates and protocol data units to be transmitted. Table F.1 lists the timings of all relevant protocol data units assuming a forward link rate based on a symbol length of Tari = 25µs for data0 (0_2) and 1.5*Tari for data1 (1_2). Moreover, a return link of 40 kbits/s FM0 encoded data is assumed. Wherever the underlying air interface allows for choices, typical values have been selected.

Table F.1 — Example of Timings in an ISO/IEC 18000-6 Type C Environment

Subject	Value	Unit	Comment
data0	25.0	µs	Tari
data1	37.5	µs	1.5 * Tari
RTcal	62.5	µs	data0 + data1
TRcal	200.0	µs	BLF = DR / TRCal
DR	8.0	1	DR = false
Tpri	25.0	µs	trCal / DR
T1	250.0	µs	MAX(RTcal, 10 * Tpri)
T2	75.0	µs	3 * Tpri
T3	0.0	µs	0 * Tpri
T4	125.0	µs	2 x RTcal
PIE delimiter	12.5	µs	fixed duration
PIE preamble	300.0	µs	delimiter + data0 + RTCal + TRCal
PIE frame synch	100.0	µs	delimiter + data0 + RTCal
FM0 preamble	150.0	µs	6*Tpri
Select	1375.0	µs	45-bit Select (empty Mask field)
Query	962.5	µs	incl. preamble
ACK	662.5	µs	incl. frame synch
RN16	550.0	µs	incl. preamble
UII	3350.0	µs	incl. preamble; PC + UII + CRC16; 96-bit UII assumed

Complementary, Table F.2 shows the bit structure of the PIE encoded interrogator commands assumed in the example for a better understanding of the calculated command durations in Table F.1.

Table F.2 — Command Structure Assumed for the Example

Protocol Data Unit	Bits Total	Bits 0_2	Bits 1_2
Select	45	33	12
Query	22	13	9
ACK	18	9	9

Based on the results presented in Table F.1, the boundaries for the random wait time selection are calculated as follows:

MinWaitTime = c * duration(longestExpectedPDU) = c * duration(UII) = **c * 3350**

MaxWaitTime = c * duration(Select + T4 + Query + T1 + RN16 + T2 + ACK + T1 + UII) = c * (1375.0 + 125.0 + 962.5 + 250.0 + 550.0 + 75.0 + 662.5 + 250.0 + 3350.0) = **c * 7600**

NOTE This example is based on a "detection only" scenario. If further steps such as tag access are to be carried out, the involved additional interrogator commands and tag responses need to be considered also for F_{min} and F_{max} definition.

Bibliography

[1] ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

[2] ISO/IEC 8859-2, *Information technology — 8-bit single-byte coded graphic character sets — Part 2: Latin alphabet No. 2*

[3] ISO/IEC 10646, *Information technology — Universal Multiple-Octet Coded Character Set (UCS)*

[4] ISO/IEC 15961, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: application interface*

[5] ISO/IEC 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

[6] ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tags*

[7] ISO/IEC 18000-1, *Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized*

[8] ISO/IEC 29172, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Reference architecture for Mobile AIDC services*[1)]

[9] ISO/IEC 29173-1, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-6 type B and type C*[1)]

[10] ISO/IEC 29174, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — UII scheme and encoding format for Mobile AIDC services*[1)]

[11] ISO/IEC 29175, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Application data structure and encoding format for Mobile AIDC services*[1)]

[12] ISO/IEC 29176, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Consumer privacy-protection protocol for Mobile RFID services*[1)]

[13] ISO/IEC 29177, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Object Directory Service for Mobile AIDC services*[1)]

[14] ISO/IEC 29178, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Service broker for Mobile AIDC services*[1)]

[15] ISO/IEC 29179, *Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Mobile AIDC application programming interface*[1)]

[16] EPCglobal Tag Data Standards, EPCglobal Inc.

[17] RFC 5092, *IMAP URL Scheme*, November 2007

1) Under preparation.

ICS 35.040

Price based on 42 pages