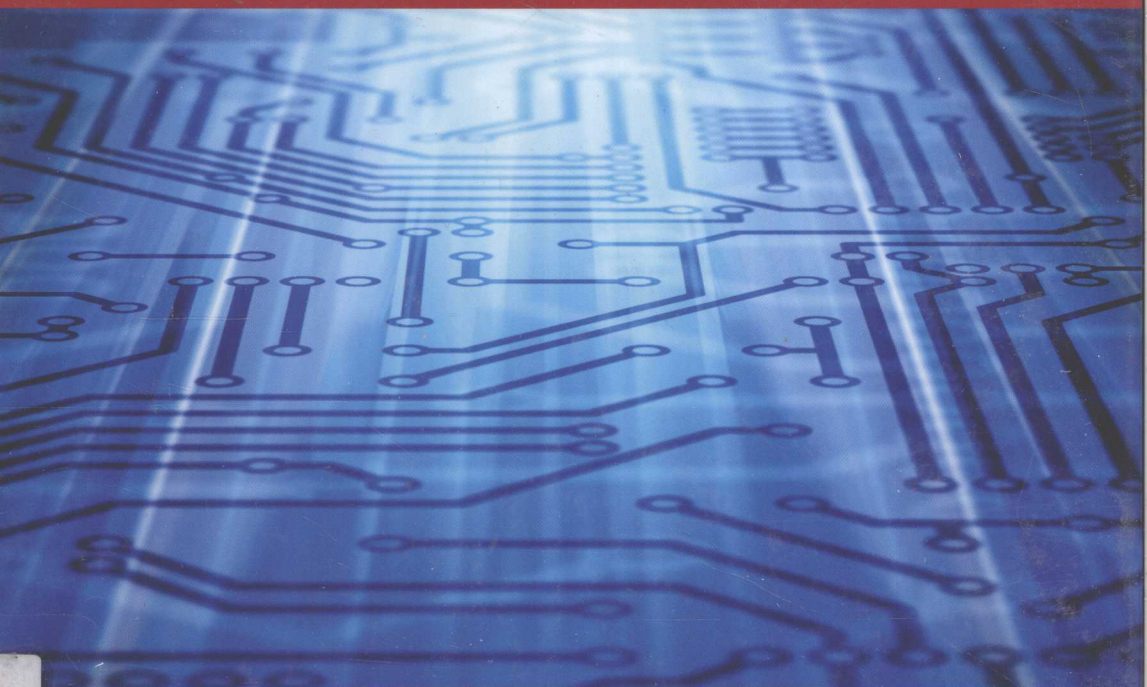


RFID and the Internet of Things

Edited by Hervé Chabanne

Pascal Urien and Jean-Ferdinand Susini



ISTE

 **WILEY**



30807718

RFID **and** **the Internet of Things**

Edited by
Hervé Chabanne
Pascal Urien
Jean-Ferdinand Susini



iSTE

 **WILEY**

First published 2011 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.
Adapted and updated from *RFID et l'internet des choses* published 2010 in France by Hermes
Science/Lavoisier © LAVOISIER 2010

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd 2011

The rights of Hervé Chabanne, Pascal Urien, Jean-Ferdinand Susini to be identified as the authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

Library of Congress Cataloging-in-Publication Data

RFID et l'internet des choses. English

RFID and the internet of things / edited by Herve Chabanne, Pascal Urien, Jean-Ferdinand Susini.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-84821-298-5

1. Radio frequency identification systems. 2. Embedded Internet devices. I. Chabanne, Herve. II. Urien, Pascal. III. Susini, Jean-Ferdinand. IV. Title.

TK6570.I34R479 2011

384.6--dc22

2011008134

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library

ISBN 978-1-84821-298-5

Printed and bound in Great Britain by CPI Antony Rowe, Chippenham and Eastbourne.



Foreword

The RFID (*Radio Frequency Identification*) technology allows automatic identification of information contained in a tag by using radio waves. An RFID tag contains an antenna and a microchip to transmit and receive.

It appears as an alternative to barcodes that are facing the growth of the trade and new trade modes based on it. Indeed, if barcodes have proved, over a long period, their efficiency in data coding, they currently face some limitations such as the use of an optical reader (scanner) which has to be located at a relatively short distance from the identified object, or in a small data storage system.

The RFID technology is characterized by the deployment of three essential components: a microchip, an antenna and a reader. The tag is placed on the object or the person to be identified. It contains information that is decrypted by the server by using an antenna for transmitting signals between the reader and the chip. The radio frequencies used by the RFID technology are in the 50 kHz to 2.5 GHz range.

Therefore it is necessary to establish a comparison between the barcodes and the RFIDs, to understand why the RFIDs can replace the barcodes, and how they still have some limitations. The first difference between the two systems is their reading mode: a barcode is read by an optical laser, while an RFID tag is scanned by a reader that identifies the data contained in this tag. The reading distance of the RFID tags can be higher. Indeed, it extends from a few centimeters to 200 meters. In addition, the RFID tags can store more information than the barcodes, and the collected data can be up to several kilobytes. It is also important to note that the RFID tags can be recycled because new information can be registered in it. One of the drawbacks of the deployment of the RFID technology is its cost, which varies and can slow down its implementation, or perturbations between the tags and their sensitivity to interference waves.

The RFID technology is still a topic of great interest to many: it not only makes it possible to solve the problems faced by barcodes, but is also of importance to key sectors of economy and trade, such as distribution and transport. The implementation of this technology could revolutionize the pharmaceutical industry and represent a significant advance in the field of health which would benefit everyone: in fact, who would not expect to benefit from quality care and not like to avoid being a victim of medical errors? Applied to pharmaceutical products, smart tags would guarantee the authenticity and thus avoid counterfeiting. With regard to blood donations, their use would significantly reduce the risk of possible confusions. Medical staff would be able to authenticate the source of a blood sample without error, and thus lead to a correct transfusion.

It is clear that the RFID tags are more and more inescapable and deserve our attention. This was the main reason for us to write this book, which provides a description of the famous “smart tags” from a scientific viewpoint. It is divided into five parts: part 1 looks at the operation of the RFID systems. It establishes the classification of RFIDs, studies the physical aspect of tags and antennae, as well as coding techniques of RFID information. Part 2 is devoted to the application of RFID. It traces its evolution from the barcodes to the RFID tags by making a comparison between the two systems, and shows in a concrete manner various application examples of the RFID technology. Part 3 describes the cryptographic protocols of RFID.

The data contained in the tags must be identified without jeopardizing the privacy of the persons who possess them. Part 4 focuses on the global standardization of RFID: EPC (Electronic Product Code). It is a global architecture initialized by the Internet of objects and the desire to establish a large quantum of data for all products, while ensuring the specificity and authenticity of each one of them. And finally, part 5 attempts to describe the architecture to implement “the Internet of things” as efficiently as possible and by adapting to the evolution of needs: middlewares.

Guy PUJOLLE
April 2011

Table of Contents

Foreword	xi
Guy PUJOLLE	
PART ONE: PHYSICS OF RFID	1
Chapter 1. Introduction	3
Simon ELRHARBI, Stefan BARBU	
1.1. Bibliography	5
Chapter 2. Characteristics of RFID Radio Signals	7
Simon ELRHARBI, Stefan BARBU	
2.1. Description and operating principle of RFID systems	7
2.1.1. Classification of RFID systems	7
2.1.2. Available operating frequency ranges	8
2.1.3. Transponder types	8
2.1.4. Energy and data transmission modes	12
2.1.5. Features of RFID chips	18
2.2. Transmission channel	19
2.2.1. Maxwell's equations	19
2.2.2. Electromagnetic field generated by an electric dipole	20
2.2.3. Electromagnetic field generated by a magnetic dipole	21
2.2.4. Field zones surrounding antennae	22
2.2.5. Wave impedance	24
2.2.6. Antenna impedance	26
2.2.7. Radiated power	26
2.2.8. Near-field coupling	27
2.3. First level electric model in inductive coupling	31
2.3.1. Magnetic loop	32
2.3.2. Base station antenna	33
2.3.3. RFID chip antenna	37

2.3.4. Design issue of RFID antennae in inductive coupling	40
2.3.5. Far field coupling	43
2.4. Bibliography	55
Chapter 3. RFID Communication Modes	57
Simon ELRHARBI, Stefan BARBU	
3.1. Communication modes	57
3.1.1. Waveforms and usual communication codes of RFID systems . .	57
3.1.2. Data coding	58
3.1.3. Modulation	61
3.1.4. Integrity of transmissions in RFID systems	62
3.1.5. Anti-collision protocol	65
3.2. Bibliography	68
PART TWO: RFID APPLICATIONS	69
Chapter 4. Applications	71
François LECOCQ, Cyrille PÉPIN	
4.1. Introduction	71
4.2. History: evolution from barcodes to RFID tags	72
4.2.1. Description of barcodes	72
4.2.2. One-dimensional (or linear) barcodes	73
4.2.3. Stacked linear barcodes	78
4.2.4. Two-dimensional barcodes	80
4.3. RFID tags	83
4.3.1. Characteristics of RFID tags	84
4.3.2. Operating principle	84
4.4. Normalization/standardization	89
4.4.1. ISO standards for RFID	90
4.4.2. ISO standards for middleware	93
4.4.3. User guidance	93
4.4.4. Protocols	94
4.4.5. EPCglobal standards	94
4.4.6. Communication layer	95
4.4.7. Different types of tags	96
4.5. Advantages/disadvantages of RFID tags	98
4.5.1. Advantages	98
4.5.2. Disadvantages	100
4.6. Description of RFID applications	102
4.7. Application examples	103
4.7.1. RFIDs in commerce	103
4.7.2. Access control	105
4.7.3. Culture and RFID	105

4.7.4. Payment	106
4.7.5. RFID and health	107
4.7.6. European biometric passport	109
4.7.7. Future perspectives	109
4.8. Conclusion	109
4.9. Bibliography	111
PART THREE: CRYPTOGRAPHY OF RFID	113
Chapter 5. Cryptography and RFID	115
Julien BRINGER, Hervé CHABANNE, Thomas ICART, Thanh-Ha LE	
5.1. Introduction	115
5.2. Identification protocols and security models	116
5.2.1. Definition of an identification protocol	116
5.2.2. Classical notions of security	117
5.2.3. Privacy notions	118
5.3. Identification protocols	121
5.3.1. Symmetric cryptography-based protocols	122
5.3.2. Asymmetric cryptography-based protocols	129
5.3.3. Protocols based on physical properties	135
5.3.4. Summary	140
5.4. Conclusion. Physical attacks on RFID devices	141
5.4.1. Side-channel attacks	141
5.4.2. Fault injection attacks	143
5.4.3. KeeLoq	143
5.5. Bibliography	144
PART FOUR: EPCGLOBAL	151
Chapter 6. EPCglobal Network	153
Dorice NYAMY, Mathieu BOUET, Daniel DE OLIVEIRA CUNHA, Vincent GUYOT	
6.1. Introduction	153
6.2. Tags	154
6.2.1. EPC codes	154
6.2.2. Classes of tags	158
6.2.3. Standards of tags	160
6.3. EPCglobal architecture	164
6.3.1. Reader protocol	164
6.3.2. Application Level Events (ALE) interface	166
6.3.3. Object Name Service (ONS)	170
6.3.4. Physical Mark-up Language (PML)	173
6.3.5. EPC Information Service interface	175
6.3.6. Security	176

6.4. Conclusion	179
6.5. Bibliography	180
PART FIVE: MIDDLEWARE	183
Chapter 7. Middleware for the Internet of Things: Principles	185
David DURAND, Yann IAGOLNITZER, Patrice KRZANIK, Christophe LOGE, Jean-Ferdinand SUSINI	
7.1. Distributed applications	187
7.1.1. Principles	187
7.1.2. Client-server model	187
7.2. RPC: Remote Procedure Call	188
7.3. Object-oriented middlewares	189
7.3.1. Examples	191
7.4. Summary of object-oriented middleware architectures	195
7.5. The XML revolution	199
7.5.1. Overview of XML	199
7.5.2. Definition of the structure of an XML document	200
7.5.3. Web services	202
7.5.4. Description of Web services-WSDL	203
7.5.5. Location of Web services	206
7.5.6. SOAP	207
7.6. Middleware for the Internet of Things	208
7.6.1. Service-oriented middlewares	209
7.6.2. Data-oriented middleware	211
7.7. Conclusion	213
7.8. Bibliography	213
Chapter 8. Middleware for the Internet of Things: Standards	217
Yann IAGOLNITZER, Patrice KRZANIK, Jean-Ferdinand SUSINI	
8.1. EPCglobal application environment	218
8.2. General introduction to message-oriented middleware	219
8.2.1. General instruction to message-oriented middleware	219
8.2.2. Java Messaging Service (JMS)	221
8.2.3. XMPP	225
8.3. Service-oriented middleware	231
8.3.1. OSGi	231
8.3.2. UPnP	237
8.4. Conclusion	242
8.5. Bibliography	242

Chapter 9. Middleware for the Internet of Things: Some Solutions	245
Yann IAGOLNITZER, Patrice KRZANIK, Jean-Ferdinand SUSINI	
9.1. EPCglobal and SUN Java RFID software	246
9.1.1. Software architecture of SUN Java System RFID	246
9.1.2. Java System RFID event manager	247
9.1.3. Java System RFID information server	249
9.2. .NET and RFID services platform	250
9.2.1. .NET platform	250
9.2.2. Distributed applications - .NET Remoting	252
9.2.3. RFID Service Platform	253
9.3. IBM Websphere RFID Suite	256
9.3.1. Data capture layer	256
9.3.2. Premise servers	257
9.4. Singularity	258
9.4.1. Middleware	258
9.4.2. Hibernate - JBoss	260
9.5. Middleware for embedded systems	260
9.5.1. TinyDB	260
9.5.2. GSN	262
9.6. ObjectWeb projects and the Internet of Things	265
9.6.1. Presentation of ObjectWeb	265
9.6.2. JORAM, component of ObjectWeb RFID	265
9.6.3. Architecture of JORAM	266
9.6.4. Advanced functions of JORAM	266
9.6.5. Ongoing works on JORAM	268
9.6.6. JINI technology and the Internet of Things	268
9.6.7. JONAS, component of ObjectWeb RFID	271
9.6.8. ASPIRE initiative of OW2	273
9.7. Conclusion	276
9.8. Bibliography	276
List of Authors	279
Index	283

PART ONE

Physics of RFID

Chapter 1

Introduction

RFID (*Radio Frequency Identification*) systems use electromagnetic waves to transmit, at distance, energy and data to devices that perform a scheduled process of information contained in these exchanges. The origin of RFID technologies, dates back to the invention of RADAR, where, during the Second World War, fighter pilots cleverly maneuvered their planes to be remotely identified by friendly radar operators, who distinguished them from their foes (*Identify Friend or Foe*).

However, the RFID technology received a boost in the early 1970s. The very first RFID devices were simple resonant analog circuits. Then, advances in microelectronics allowed the integration of increasingly complex digital functions. The initial applications were designed to track and monitor dangerous materials in sensitive areas (usually military or nuclear). In the late 1970s, applications of these devices also included the civilian domain, typically the monitoring of animals, vehicles and automated production lines [DOB 07].

Usual tracking technologies such as barcodes, invented in 1970 by an IBM engineer, have shown their limitations for applications in an altered environment, such as animal tracking or in the engine assembly lines. Indeed, the barcode must pass through a scanning window to be scanned by a mobile reader without obstacles or of dirt traces which degrade or block the reading operation. This is why RFID technologies are being developed to replace barcodes in identification functions, so as to make it possible to read or write information at a distance using electromagnetic waves.

RFID technologies and contactless smart cards consist of one or more electronic tags connected to one or more antennae or terminals that radiate an electromagnetic field through their antennae. These devices communicate by RF (Radio Frequency) or UHF (Ultra High Frequency) channels. Some RFID applications and contactless smart cards require embedded energy sources to facilitate the data exchange between the tags and the terminal readers. Other more common RFID technologies and contactless smart cards perform remote energy transmission to enable data exchange.

Depending on the frequencies used, the transmitted energy necessary for operations can be stored in a geometric volume, site of an electromagnetic induction effect (as in the case of low frequencies or radio frequencies), or propagated (as in the case of Ultra High Frequency).

The deployment of RFID technologies presupposes that a number of electrical electronic, mechanical and material parameters have been controlled [ELR 04].

Indeed, given the nature of energy and data transmissions between the devices of the RFID system, the geometric space in which the energy transmission and data exchanges are performed may reveal communication failures between tags and terminals. In particular, the phenomena of echo due to reflection and absorption signals (as in the case of UHF) must be controlled. The coupling intensity in the near field (as in case of LF or HF frequencies) can degrade the signal to noise ratio or, in other cases, lead to very high impedance mismatch at the power stage level and cause a malfunction of the baseband station [BAR 05]. The antenna orientation of RFID tag/terminal pairs in correlation with the energy and data propagation should be minimized and the writing and reading distance should be optimized by taking into account the complete front-end architecture (stages of power, reception and power control). These issues (operational zones and antenna configurations) mainly relate to physical and electrical properties.

Regarding electronic aspects, the anti-collision processing should allow us to establish data exchange between all the RFID tags in the operating zone of the terminal(s) under the conditions predefined by RFID system specifications and ISO standards. The processing time of transmission, which should be secured by cryptographic algorithms, should be optimized (in terms of bandwidth and data rates), so that the processing time is compatible with the high flux of expected transactions.

Finally, the interoperability between different RFID systems, their robustness (in terms of electrical features) and their compatibility with ISO standards must be guaranteed. The mechanical parameters (connections between chips and antennas) and materials (from a point of view of electric behaviors) are all very important in this context.

By nature of their capture and data processing abilities, the RFID technology is well suited for automation of the complete supply chain, with better utilization flexibility

and operation under varying environmental constraints, even when the object is in movement and occupies various positions. RFID technologies follow the unprecedented development of international trade exchanges. These technologies make it possible to save money by avoiding logistical and human errors and by limiting fraud, irrespective of their origin [ROU 05].

Information system architectures that aggregate data from RFID systems are based on normative networks, which define international ISO standards, or the coalition of managers and assignees such as EPCglobal Inc. which implements EPC (Electronic Product Code) codes. These codes are allocated to objects for identification at a worldwide level, while providing an interconnection service to servers dedicated to identification and localization of objects by the Internet.

Today, due to the joint progress of micro-electronics, microcomputer and telecommunications, RFID systems are not only reserved for automatic identification, but have also spread to other areas such as secure access to buildings, to networks or the completion of secured transactions between remote electronic devices.

1.1. Bibliography

- [BAR 05] BARBU S., Design and implementation of an RF metrology system for contactless identification systems at 13.56 MHz, PhD Thesis, University of Marne La Vallée, 2005.
- [DOB 07] DOBKIN D.M., *The RF in RFID*, Elsevier, Oxford, 2007.
- [ELR 04] ELRHARBI S., BARBU S., GASTON L., Why Class 1 PICC is not suitable for ICAO / NTWG E-passport - New proposal for a Class 1 PCD, Contribution ISO/IEC JTC1/SC17/WG8/TF2 num. N430, ISO/IEC JTC1/SC17/WG8/TF2, June 2004.
- [ROU 05] ROURE F., GORICHON J., SARTORIUS E., RFID technologies: industrial and society issues, Report of CGTI committee num. Report N° II-B.9 - 2004, CGTI, January 2005.

Chapter 2

Characteristics of RFID Radio Signals

This chapter describes the main characteristics of electrical signals exchanged in RFID systems.

2.1. Description and operating principle of RFID systems

RFID systems typically consist of fixed elements (called base station, reader, coupling device, terminal, etc.), whose function is to identify and process, by using radio waves, the information contained in one or more deported elements such as transponders, tags, badges, electronic tokens, or contactless smart cards. The different designations of the fixed and deported elements may vary, depending on applications, contexts, and their hardware and software resources. The fixed elements are themselves connected to servers for data processing at middleware and application levels for analysis, archiving and traceability (Figure 2.1).

2.1.1. *Classification of RFID systems*

Because of the variety of devices, features, applications and uses, there are a multitude of possible classifications due to the availability of a variety of devices, features and applications. However, we can retain some of the recurrent criteria found in these systems, such as:

- operating frequencies;
- types of transponders;
- modes of energy and data transmission;
- features.

Chapter written by Simon ELRHARBI and Stefan BARBU.