ISO/IEC 29167-14:2015-10 (E)

Information technology - Automatic identification and data capture techniques - Part 14: Crypto sui te AES OFB security services for air interface communications

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Conformance 1
2.1 Claiming conformance 1
2.2 Interrogator conformance and obligations 1
2.3 Tag conformance and obligations 1

3 Normative references 2

4 Terms and definitions 2

5 Symbols and abbreviated terms 2
5.1 Symbols 2
5.2 Abbreviated terms 2

6 Cipher introduction 3
6.1 General 3
6.2 Encryption in AES OFB mode 3
6.3 Decryption in AES OFB mode 3

7 Parameter definitions 4

8 State diagram 5

9 Initialization and resetting 5

10 Authentication 5
10.1 General 5
10.1.1 Authentication types 5
10.1.2 CS_Initialization (Authentication type: AuthMethod "111", Mandatory) 6
10.2 Tag authentication (Authentication type: AuthMethod = "000", Mandatory) 7
10.2.1 Tag authentication 7
10.2.2 Commands and responses for tag authentication 8
10.3 Interrogator authentication (Authentication type: AuthMethod = "001", Optional) 9
10.3.1 Interrogator authentication 9
10.3.2 Commands and responses for interrogator authentication 10
10.4 Mutual authentication (Authentication type: AuthMethod = "010", Mandatory) 12
10.4.1 Mutual authentication 12
10.4.2 Commands and responses for mutual authentication 13

11 Communication 15

12 Key management and key update 15
12.1 Master key selection 15
12.2 Keystream generation 16
12.3 Key update 17
12.3.1 General 17

12.3.2 Command 17

Annex A (normative) Crypto suite state transition tables 20

Annex B (normative) Error Codes 21

Annex C (normative) Cipher description 22

Annex D (informative) AES OFB test vectors 23

Annex E (normative) Protocol specific operation 26

Annex F (informative) Tag authentication via server 32

Bibliography 35