ISO/IEC 29167-13:2015-05 (E)

Information technology - Automatic identification and data capture techniques - Part 13: Crypto suite Gra in-128A security services for air interface communications

Contents

Page

Foreword v

Introduction vi

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

7 Parameter definition 3

8 State diagram 4

9 Initialization and resetting 5

10 Authentication 5
10.1 General 5
10.2 Tag Authentication (TA) 7
10.2.1 General 7
10.2.2 CryptoAuthCmd(TA.1 Payload for Tag CS) 7
10.2.3 CryptoAuthResp(TA.1 Payload for Interrogator CS) 7
10.2.4 Final Interrogator Processing 7
10.3 Interrogator Authentication (IA) 8
10.3.1 General 8
10.3.2 CryptoAuthCmd(IA.1 Payload for Tag CS) 8
10.3.3 CryptoAuthResp(IA.1 Payload for Interrogator CS) 8
10.3.4 CryptoAuthCmd(IA.2 Payload for Tag CS) 9
10.3.5 CryptoAuthResp(IA.2 Payload for Interrogator CS) 9
10.4 Mutual Authentication (MA) 9
10.4.1 General 9
10.4.2 CryptoAuthCmd (MA.1 Payload for Tag CS) 10
10.4.3 CryptoAuthResp(MA.1 Payload for Interrogator CS) 10
10.4.4 CryptoAuthCmd(MA.2 Payload for Tag CS) 10
10.4.5 CryptoAuthResp(MA.2 Payload for Interrogator CS) 11
10.4.6 Final Interrogator Processing 11

11 Communication 11
11.1 General 11
11.2 Authenticated Communication 12

11.3 Secure Authenticated Communication 13

12 Key table and key update 14

Annex A (normative) State transition tables 15

Annex B (normative) Error conditions and error handling 19

Annex C (normative) Cipher description 20

Annex D (informative) Test vectors 23

Annex E (normative) Protocol specific 30

Bibliography 39