ISO/IEC 29167-16:2015-11 (E)

Information technology - Automatic identification and data capture techniques - Part 16: Crypto suite ECD SA-ECDH 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 2

3 Normative references 2

4 Terms and definitions 2

5 Symbols and abbreviated 3
5.1 Symbols 3
5.2 Abbreviated terms 3

6 Cipher introduction 4

7 Parameter definitions 4
7.1 Parameter definitions 4
7.2 Certiticate format 5

8 State diagram 6

9 Initialization and resetting 6

10 Authentication 6
10.1 General 6
10.2 Authenticate message 7
10.2.1 Message in Authenticate command and reply 7
10.2.2 Authenticate(MAM1.1 Message) 8
10.2.3 MAM1.1 Response 8
10.2.4 Authenticate(MAM1.2 Message) 9
10.2.5 MAM1.2 Response 10
10.3 Authentication procedure 11
10.3.1 Protocol requirements 11
10.3.2 Procedure 11

11 Communication 12
11.1 Authenticate Communication 12
11.2 Secure Communication 13

Annex A (normative) State transition table 15

Annex B (normative) Error codes and error handling 16

Annex C (normative) Cipher description 17

Annex D (informative) Test Vectors 18

Annex E (normative) Protocol specific 23

Annex F (normative) Protocol message's fragmentation and defragmentation 28

Annex G (informative) Examples of ECC parameters 29

Annex H (normative) TTP involving 30