ISO/IEC 29167-19:2016-05 (E)

Information technology - Automatic identification and data capture techniques - Part 19: Crypto suite RAMON se curity 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 3
5.1 Symbols 3
5.2 Abbreviated terms 3
5.3 Notation 4

6 Crypto suite introduction 5
6.1 Overview 5
6.2 Authentication protocols 6
6.2.1 Tag Identification 6
6.2.2 Symmetric mutual authentication 7
6.3 Send Sequence Counter 8
6.4 Session key derivation 9
6.4.1 KDF in counter mode 9
6.4.2 Key Derivation Scheme 10
6.5 IID, SID, Used Keys and Their Personalisation 11
6.6 Key table 13

7 Parameter definitions 14

8 State diagrams 14
8.1 General 14
8.2 State diagram and transitions for Tag identification 15
8.2.1 Partial Result Mode 15
8.2.2 Complete Result Mode 16
8.3 State diagram and transitions for mutual authentication 17
8.3.1 Partial Result Mode 17
8.3.2 Complete Result Mode 18
8.3.3 Combination of complete and partial result mode 19

9 Initialization and resetting 20

10 Identification and authentication 20
10.1 Tag identification 20
10.1.1 Partial Result Mode 20
10.1.2 Complete Result Mode 20
10.2 Mutual authentication 21

10.2.1 Partial Result Mode 21
10.2.2 Complete Result Mode 22
10.3 The Authenticate command 23
10.3.1 Message formats for Tag identification 23
10.3.2 Message formats for Mutual Authentication 24
10.4 Authentication response 25
10.4.1 Response formats for Tag identification 25
10.4.2 Response formats for mutual authentication 26
10.4.3 Authentication error response 28
10.5 Determination of Result Modes 29

11 Secure communication 30
11.1 Secure communication command 30
11.2 Secure Communication response 31
11.2.1 Secure communication error response 31
11.3 Encoding of Read and Write commands for secure communication 31
11.4 Application of secure messaging primitives 32
11.4.1 Secure Communication command messages 32
11.4.2 Secure Communication response messages 34
11.4.3 Explanation of cipher block chaining mode 37

Annex A (normative) State transition tables 39

Annex B (normative) Error codes and error handling 42

Annex C (normative) Cipher description 43

Annex D (informative) Test Vectors 58

Annex E (normative) Protocol specific 61

Annex F (informative) Non-traceable and integrity-protected Tag identification 68

Annex G (informative) Memory Organization for Secure UHF Tags (Proposal) 71

Bibliography 75