ISO/IEC 29167-21:2018 (E)

Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON security services for air interface communications

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions
3.2 Symbols
3.3 Abbreviated terms

4 Conformance

4.1 Air interface protocol specific information
4.2 Interrogator conformance and obligations
4.3 Tag conformance and obligations

5 Introducing the SIMON cryptographic suite

6 Parameter and variable definitions

7 Crypto suite state diagram

8 Initialization and resetting

9 Authentication

9.1 General
9.2 Message and response formatting
9.3 Tag authentication (AuthMethod “00”)
9.3.1 General
9.3.2 TAM1 message
9.3.3 Intermediate Tag processing
9.3.4 TAM1 response
9.3.5 Final Interrogator processing
9.4 Interrogator authentication (AuthMethod “01”)
9.4.1 General
9.4.2 IAM1 message
9.4.3 Intermediate Tag processing #1
9.4.4 IAM1 response
9.4.5 Intermediate Interrogator processing
9.4.6 IAM2 message
9.4.7 Intermediate Tag processing #2
9.4.8 IAM2 response
9.4.9 Final Interrogator processing
9.5 Mutual authentication (AuthMethod “10”)
9.5.1 General
9.5.2 MAM1 message
9.5.3 Intermediate Tag processing #1
9.5.4 MAM1 response
9.5.5 Intermediate Interrogator processing
9.5.6 MAM2 message

9.5.7 Intermediate Tag processing #2
9.5.8 MAM2 response
9.5.9 Final Interrogator processing

10 Communication

10.1 General
10.2 Message and response formatting
10.3 Transforming a payload prior to encapsulation
10.3.1 General
10.3.2 Encapsulating an Interrogator command
10.3.3 Cryptographically protecting a Tag reply
10.4 Processing an encapsulated or cryptographically-protected reply
10.4.1 General
10.4.2 Recovering an encapsulated Interrogator command
10.4.3 Recovering a cryptographically-protected Tag response

11 Key table and key update

Annex A (normative) Crypto suite state transition table

Annex B (normative) Errors and error handling

Annex C (normative) Description of SIMON and SILC v3

C.1 SIMON
C.2 SILC v3

Annex D (informative) Test vectors

Annex E (normative) Protocol specific information

E.1 General
E.1.1 Protocol specific information
E.1.2 Supported security services
E.2 Security services for ISO/IEC 18000-3 mode 1
E.3 Security services for ISO/IEC 18000-3 mode 3
E.4 Security services for ISO/IEC 18000-63
E.4.1 General
E.4.2 ISO/IEC 18000-63 protocol commands
E.4.3 Security commands in ISO/IEC 18000-63
E.4.4 Implementation of crypto suite error conditions in ISO/IEC 18000-63
E.4.5 Key properties

Page count: 46