ISO/IEC 29167-10:2015-05 (E)

Information technology - Automatic identification and data capture techniques - Part 10: Crypto suite AES-128 security services for air interface communications

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Conformance 1
2.1 Air interface protocol specific information 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 4
5.1 Symbols 4
5.2 Abbreviated terms 4

6 Introduction of the AES-128 crypto suite 5

7 Parameter definitions 5

8 Crypto suite state diagram 6

9 Initialization and resetting 6

10 Authentication 6
10.1 Introduction 6
10.2 Message and Response formatting 7
10.3 Tag authentication (Method "00" = TAM) 7
10.3.1 TAM1 and TAM2 7
10.3.2 TAM1 Message 7
10.3.3 TAM1 Response 8
10.3.4 Final Interrogator processing TAM1 8
10.3.5 TAM2 Message 8
10.3.6 TAM2 Response 11
10.3.7 Final Interrogator processing TAM2 13

11 Communication 13

12 Key Table 13

Annex A (normative) Crypto Suite State transition tables 15

Annex B (normative) Error conditions and error handling 16

Annex C (normative) Cipher description 17

Annex D (informative) Test vectors 18

Annex E (normative) Protocol specific information 19

Annex F (informative) Examples 23

Bibliography 26