ISO/IEC 29167-11:2014-08 (E)

Information technology - Automatic identification and data capture techniques - Part 11: Crypto suite PRE SENT-80 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 terms 3
5.1 Symbols 3
5.2 Abbreviated terms 3

6 Introduction of the PRESENT-80 crypto suite 4

7 Parameter definitions 4

8 Crypto Suite State diagram 4

9 Initialization and resetting 4

10 Authentication 4
10.1 Introduction 4
10.2 Message and Response formatting 5
10.3 Tag authentication (Method "00" = TAM1) 5

11 Key table and key update 6

Annex A (normative) Crypto Suite State transition table 7

Annex B (normative) Error conditions and error handling 8

Annex C (normative) Formal Reference for PRESENT 9

Annex D (informative) Test vectors 10

Annex E (normative) Protocol specific information 11

Bibliography 14