ISO/IEC 19823-22:2019 (E)

Information technology — Conformance test methods for security service crypto suites — Part 22: Crypto suite SPECK

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions, symbols and abbreviated terms

4 Test methods

4.1 General
4.2 By demonstration
4.3 By design

5 Test requirements for ISO/IEC 18000-63 interrogators and tags

6 Test methods with respect to ISO/IEC 29167-22 interrogators and tags

6.1 Test map for optional features
6.2 Crypto suite requirements
6.2.1 General
6.2.2 Crypto suite requirements of ISO/IEC 29167-22:2018, Clauses 1 to 8 and Annexes A to C
6.2.3 Crypto suite requirements of ISO/IEC 29167-22:2018, Clauses 9 to 12 and Annex E
6.3 Test patterns
6.3.1 General
6.3.2 Test_Pattern 1
6.3.3 Test_Pattern 2
6.3.4 Test_Pattern 3
6.3.5 Test_Pattern 4
6.3.6 Test_Pattern 5
6.3.7 Test_Pattern 6
6.3.8 Test_Pattern 7
6.3.9 Test_Pattern 8
6.3.10 Test_Pattern 9
6.3.11 Test_Pattern 10
6.3.12 Test_Pattern 11

Page count: 20