ISO/IEC 19823-22:2026-03 (E)

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

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions, symbols and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Symbols and abbreviated terms 2

4 Test methods **2**
4.1 General 2
4.2 By demonstration 2
4.3 By design 2

5 Test requirements for ISO/IEC 18000-63 Interrogators and Tags **2**

6 Test methods with respect to ISO/IEC 29167-22 Interrogators and Tags **2**
6.1 Test map for optional features 2
6.2 Crypto suite requirements 3
6.2.1 General 3
6.2.2 Crypto suite requirements of ISO/IEC 29167-22:2026, Clauses 4 to 8 and Annexes A to C 3
6.2.3 Crypto suite requirements of ISO/IEC 29167-22:2026, Clauses 9 to 12 and Annex E 3
6.3 Test patterns 12
6.3.1 General 12
6.3.2 Test Pattern 1 12
6.3.3 Test Pattern 2 12
6.3.4 Test Pattern 3 13
6.3.5 Test Pattern 4 13
6.3.6 Test Pattern 5 14
6.3.7 Test Pattern 6 14
6.3.8 Test Pattern 7 15
6.3.9 Test Pattern 8 15
6.3.10 Test Pattern 9 16
6.3.11 Test Pattern 10 16
6.3.12 Test Pattern 11 17

Bibliography **18**