ISO/IEC 19823-21:2026-03 (E)

Information technology - Conformance test methods for security service crypto suites - Part 21: Crypto suite SIMON

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Test methods **2**

4.1 General 2

4.2 By design 2

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

6 Test methods related to ISO/IEC 29167-21 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 29167-21:2026, Clauses 4 to 8 and Annexes A to C 3

6.2.3 Crypto suite requirements of ISO/IEC 29167-21:2026, Clauses 9 to 12 and Annex E 3

6.3 Test patterns 10

6.3.1 General 10

6.3.2 Test Pattern 1 10

6.3.3 Test Pattern 2 11

6.3.4 Test Pattern 3 11

6.3.5 TestPattern 4 12

6.3.6 Test Pattern 5 12

6.3.7 Test Pattern 6 13

6.3.8 Test Pattern 7 13

6.3.9 Test Pattern 8 14

6.3.10 Test Pattern 9 14

6.3.11 TestPattern 10 15

6.3.12 Test Pattern 11 15

Bibliography **16**