

ISO/IEC 19823-13:2026-03 (E)

Information technology - Conformance test methods for security service crypto suites - Part 13: Crypto suite Grain-128A

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..... 1
- 4 Test methods..... 2
 - 4.1 General..... 2
 - 4.2 By demonstration..... 2
 - 4.3 By design..... 2
- 5 Test requirements for ISO/IEC 18000-62 Interrogators and Tags..... 2
- 6 Test methods related to the ISO/IEC 29167-13 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 29167-13:2026, Clauses 5 to 8 and Annexes A to C..... 3
 - 6.2.3 Crypto suite requirements of ISO/IEC 29167-13:2026, 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..... 13
 - 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 Test pattern 10..... 14
 - 6.3.12 Test pattern 11..... 14
 - 6.3.13 Test pattern 12..... 15
 - 6.3.14 Test pattern 13..... 15
 - 6.3.15 Test pattern 14..... 15
 - 6.3.16 Test pattern 15..... 15
 - 6.3.17 Test pattern 16..... 16
 - 6.3.18 Test pattern 17..... 16
 - 6.3.19 Test pattern 18..... 16
 - 6.3.20 Test pattern 19..... 16
 - 6.3.21 Test pattern 20..... 17
 - 6.3.22 Test pattern 21..... 17
 - 6.3.23 Test pattern 22..... 17
 - 6.3.24 Test pattern 23..... 17
 - 6.3.25 Test pattern 24..... 18
 - 6.3.26 Test pattern 25..... 18
- Bibliography..... 19