ISO/IEC 19823-16:2026-03 (E)

Information technology - Conformance test methods for security service crypto suites - Part 16: Crypto suite ECDSA-ECDH

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 ... 1
3.3 Abbreviated terms ... 2

4 Test methods ... **2**
4.1 General ... 2
4.2 By demonstration ... 2
4.3 By design ... 3

5 Test methods related to ISO/IEC 18000-4:2018, MODE 4 ... **3**
5.1 Default items applicable to the test methods ... 3
5.1.1 General ... 3
5.1.2 Test environment ... 3
5.1.3 Pre-conditioning ... 3
5.1.4 Default tolerance ... 3
5.1.5 Total measurement uncertainty ... 3
5.2 Test setup and measurement equipment ... 3
5.2.1 General ... 3
5.2.2 Test setup for Interrogator testing ... 4
5.2.3 Test setup for Tag testing ... 4
5.2.4 Test equipment ... 4

6 Test methods related to ISO/IEC 29167-16 Interrogators and Tags ... **5**
6.1 Test map for optional features ... 5
6.2 Crypto suite requirements ... 5
6.2.1 General ... 5
6.2.2 Crypto suite requirements of ISO/IEC 29167-16:2022, Clauses 5 to 6 ... 5
6.2.3 Crypto suite requirements of ISO/IEC 29167-16:2022, Clauses 7 to 11 ... 5
6.2.4 Crypto suite requirements of ISO/IEC 29167-16:2022, Annex A ... 9
6.2.5 Crypto suite requirements of ISO/IEC 29167-16:2022, Annex E ... 10
6.3 Test patterns for ISO/IEC 18000-4:2018, MODE 4 ... 11
6.3.1 General ... 11
6.3.2 Test pattern 1 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 11
6.3.3 Test pattern 2 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 13
6.3.4 Test pattern 3 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 13
6.3.5 Test pattern 4 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 13
6.3.6 Test pattern 5 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 13
6.3.7 Test pattern 6 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 14
6.3.8 Test pattern 7 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 14
6.3.9 Test pattern 8 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 14
6.3.10 Test pattern 9 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 14
6.3.11 Test pattern 10 utilizing ISO/IEC 18000-4:2018, 9.3.3 ... 15

Annex A (informative) **Example of test parameters** ... **16**

Bibliography ... **20**