ISO/IEC 19823-10:2020-01 (E)

Information technology - Conformance test methods for security service crypto suites - Part 10: Crypto suite AES-128

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 methods with respect to the ISO/IEC 18000 series ... **2**
5.1 Test requirements for ISO/IEC 18000-3 Interrogators and Tags ... 2
5.2 Test requirements for ISO/IEC 18000-63 Interrogators and Tags ... 3

6 Test methods with respect to the ISO/IEC 29167-10 Interrogators and Tags ... **3**
6.1 Test map for optional features ... 3
6.2 Additional parameters required as input for the test ... 4
6.3 Crypto suite requirements ... 4
6.3.1 General ... 4
6.3.2 Crypto suite requirements of ISO/IEC 29167-10:2017, Clauses 1 to 6 ... 5
6.3.3 Crypto suite requirements of ISO/IEC 29167-10:2017, Clauses 7 to 12 ... 5
6.3.4 Crypto suite requirements of ISO/IEC 29167-10:2017, Annex A ... 21
6.3.5 Crypto suite requirements of ISO/IEC 29167-10:2017, Annex E ... 21

7 Test patterns ... **26**
7.1 General ... 26
7.2 Test pattern information ... 26
7.2.1 General ... 26
7.2.2 Information related to ISO/IEC 18000-3 MODE 1 ... 26
7.2.3 Information related to ISO/IEC 18000-63 ... 27
7.3 Test pattern descriptions ... 27
7.3.1 General ... 27
7.3.2 Test pattern 01 (TAM reject message when "AuthMethod" is '11') ... 27
7.3.3 Test pattern 02 (TAM1 execution and error handling) ... 28
7.3.4 Test pattern 03 (TAM1 execution for all keys) ... 29
7.3.5 Test pattern 04 (TAM1 store Tag reply in the response buffer) ... 30
7.3.6 Test pattern 05 (TAM1 with Challenge, read Tag reply from the response buffer) ... 31
7.3.7 Test pattern 06 (TAM2 execution and error handling) ... 32
7.3.8 Test pattern 07 (TAM2 unauthorized use of KeyID for profile) ... 36
7.3.9 Test pattern 08 (TAM2 execution for all keys) ... 37
7.3.10 Test pattern 09 (MAM1 execution and error handling) ... 37
7.3.11 Test pattern 10 (MAM2 execution and error handling) ... 39
7.3.12 Test pattern 11 (MAM1 and MAM2 execution for all keys) ... 43

Bibliography ... **45**