ISO/IEC 19823-16:2020 (E)

Information technology — Conformance test methods for security service crypto suites — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions
3.2 Symbols
3.3 Abbreviated terms

4 Test methods

4.1 General
4.2 By demonstration
4.3 By design

5 Test methods in respect to ISO/IEC 18000-4 Mode 4

5.1 Default items applicable to the test methods
5.1.1 Test environment
5.1.2 Pre-conditioning
5.1.3 Default tolerance
5.1.4 Total measurement uncertainty
5.2 Test setup and measurement equipment
5.2.1 Test setup for interrogator testing
5.2.2 Test setup for tag testing
5.2.3 Test equipment
5.2.3.1 Spectrum analyser
5.2.3.2 Signal generator
5.2.3.3 Logic analyser

6 Test methods in respect to ISO/IEC 29167-16 interrogators and tags

6.1 Test map for optional features
6.2 Crypto suite requirements
6.2.1 General
6.2.2 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 1 - 6
6.2.3 Crypto suite requirements of ISO/IEC 29167-16:2015, Clauses 7 - 11
6.2.4 Crypto suite requirements of ISO/IEC 29167-16:2015, Annex A
6.2.5 Crypto suite requirements of ISO/IEC 29167-16: 2015 in Annex E
6.2.5.1 Command definitions for ISO/IEC 29167-16:2015 in Annex E1
6.2.5.2 Command definitions for ISO/IEC 29167-16:2015, Annex E.2
6.3 Test patterns for ISO/IEC 18000-4:2018, Mode 4
6.3.1 Test pattern 1 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.2 Test pattern 2 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.3 Test pattern 3 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.4 Test pattern 4 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.5 Test pattern 5 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.6 Test pattern 6 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.7 Test pattern 7 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.8 Test pattern 8 utilizing ISO/IEC 18000-4:2018, 9.3.3
6.3.9 Test pattern 9 utilizing ISO/IEC 18000-4:2018, 9.3.3

6.3.10 Test pattern 10 utilizing ISO/IEC 18000-4:2018, 9.3.3

Annex A (informative) Test parameters example

A.1 Authentication elliptic E curve
A.2 Authentication parameters
A.3 Authentication process

Page count: 21