ISO/IEC 18367:2016-12 (E)

Information technology - Security techniques - Cryptographic algorithms and security mechanisms conformance testing

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 6

5 Objectives 7

6 Types of cryptographic algorithms and security mechanisms from a conformance testing perspective 8
6.1 General 8
6.2 Asymmetric key algorithms 8
6.3 Digital signature 8
6.4 Digital signature with message recovery 8
6.5 Hashing algorithms 8
6.6 Key establishment mechanisms 8
6.7 Lightweight cryptography 9
6.8 Message authentication algorithms 9
6.9 Random bit generator algorithms 9
6.9.1 Deterministic random bit generator algorithms 9
6.9.2 Non-deterministic random bit generator algorithms 9
6.10 Symmetric key algorithms 10
6.10.1 Block cipher symmetric key algorithms 10
6.10.2 Stream cipher symmetric key algorithms 10

7 Conformance testing methodologies 10
7.1 Overview 10
7.2 Black box testing 11
7.2.1 General 11
7.2.2 Known-answer test vectors 11
7.2.3 Multi-block message testing 11
7.2.4 Monte Carlo or statistical testing 11
7.3 Glass box or white box testing 11
7.3.1 Source code inspection 11
7.3.2 Binary analysis 11

8 Levels of conformance testing 12
8.1 Introduction 12
8.2 Level of basic conformance testing 12
8.3 Level of moderate conformance 12

9 Conformance testing guidelines 12
9.1 General guidelines 12
9.1.1 Identification 12
9.1.2 Guidelines for black box testing 13

9.1.3 Guidelines for white box testing 13
9.2 Guidelines specific to encryption algorithms 16
9.2.1 Identification of encryption algorithms 16
9.2.2 Selecting a set of conformance test items 17
9.2.3 Guidelines for each conformance test item 18
9.3 Guidelines specific to digital signature algorithms 29
9.3.1 Identification of digital signature algorithms 29
9.3.2 Selecting a set of conformance test items 29
9.3.3 Guidelines for each conformance test item 29
9.4 Guidelines specific to hashing algorithms 30
9.4.1 dentification of hashing algorithms 30
9.4.2 Selecting a set of conformance test items 31
9.4.3 Guidelines for each conformance test item 31
9.5 Guidelines specific to MAC algorithms 33
9.5.1 Identification of MAC algorithms 33
9.5.2 Selecting a set of conformance test items 34
9.5.3 Guidelines for each conformance test item 34
9.6 Guidelines specific to RBG algorithms 35
9.6.1 Identification of RBG algorithms 35
9.6.2 Selecting a set of conformance test items 35
9.6.3 Guidelines for each conformance test item 35
9.7 Guidelines specific to key establishment mechanisms 36
9.7.1 Identification of key establishment mechanisms 36
9.7.2 Selecting a set of conformance test items 36
9.7.3 Guidelines for each conformance test item 37
9.8 Guidelines specific to key derivation function 39
9.8.1 Identification of key derivation function 39
9.8.2 Selecting a set of conformance test items 39
9.8.3 Guidelines for each conformance test item 39
9.9 Guidelines specific to prime number generation 40
9.9.1 Identification of prime number generation 40
9.9.2 Selecting a set of conformance test items 40
9.9.3 Guidelines for each conformance test item 41

10 Conformance testing 41
10.1 Level of conformance testing 41
10.2 Symmetric key cryptographic algorithms 42
10.2.1 n-bit block cipher 42
10.3 Asymmetric key cryptographic algorithms 43
10.3.1 Digital Signature Algorithm (DSA) 43
10.3.2 RSA 47
10.3.3 Elliptic Curve Digital Signature Algorithm (ECDSA) 49
10.4 Dedicated hashing algorithms 51
10.4.1 General 51
10.4.2 Black box testing 51
10.4.3 White box testing 51
10.5 Message Authentication Codes (MAC) 51
10.5.1 Black box testing 51
10.5.2 White box testing 52
10.6 Authenticated encryption 53
10.6.1 Black box testing 53
10.6.2 White box testing 54
10.7 Deterministic Random Bit Generation algorithms 54
10.8 Key agreement 58
10.8.1 Black box testing 58
10.8.2 White box testing 61
10.9 Key Derivation Functions (KDF) 62
10.9.1 Black box testing 62
10.9.2 White box testing 63

Annex A (informative) Common mistakes in cryptographic algorithm implementations 64

Annex B (informative) Examples of known-answer test vectors 65

Bibliography 66