ISO/IEC 20543:2019-10 (E)

Information technology - Security techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 7

5 Structure of this document 7

6 Overview of non-deterministic random bit generators 7
6.1 Introductory remarks on random bit generation 7
6.2 Modelling of random sources 8
6.2.1 Stochastic models 8
6.2.2 Heuristic analysis of entropy sources 10
6.2.3 Physical and non-physical sources 11
6.2.4 Overview of the evaluation of the random source of a TNRBG 11
6.2.5 Overview of the evaluation of the random source of an NNRBG 12
6.3 General design template and taxonomy for non-deterministic random bit generators 12
6.3.1 Overview 12
6.3.2 Functional model of a NRBG 12
6.3.3 Components of a NRBG 15

7 Conformance testing of NRBG 18
7.1 Overview 18
7.2 Testing 19
7.2.1 Design documentation 19
7.2.2 Analysing entropy 19
7.2.3 Min entropy 23
7.2.4 Statistical tests 24
7.3 Evaluation 25
7.3.1 General 25
7.3.2 Vendor input to conformance testing 25

8 Overview of deterministic random bit generators 27
8.1 General remarks 27
8.2 Structural overview of a deterministic random bit generator 28

9 Conformance testing of DRBG 29
9.1 Overview 29
9.2 Testing 29
9.2.1 Design documentation 29
9.2.2 Analysis of seed entropy 29

10 Testing methodology 30
10.1 General 30
10.2 Vendor requirements 30

10.3 Tests requirements 30

Annex A (normative) General statistical methodology 31

Annex B (informative)Testfiles 38

Bibliography 39