

ISO/IEC 18031:2025-02 (E)

Information technology - Security techniques - Random bit generation

| Contents | | Page |
|--------------------|---|-------------|
| Foreword | | v |
| Introduction | | vi |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 1 |
| 4 | Symbols | 7 |
| 5 | Properties and requirements of a random bit generator | 8 |
| 5.1 | Properties of a random bit generator | 8 |
| 5.2 | Requirements of an RBG | 9 |
| 5.3 | Additional information for an RBG | 10 |
| 6 | RBG model | 10 |
| 6.1 | Conceptual functional model for random bit generation | 10 |
| 6.2 | RBG basic components | 11 |
| 6.2.1 | Introduction to the RBG basic components | 11 |
| 6.2.2 | Randomness source | 11 |
| 6.2.3 | Additional inputs | 12 |
| 6.2.4 | Internal state | 12 |
| 6.2.5 | Internal state transition functions | 13 |
| 6.2.6 | Output generation function | 14 |
| 6.2.7 | Health test | 15 |
| 7 | Types of RBGs | 15 |
| 7.1 | Introduction to the types of RBGs | 15 |
| 7.2 | Non-deterministic random bit generators | 16 |
| 7.3 | Deterministic random bit generators | 17 |
| 7.4 | The RBG spectrum | 17 |
| 8 | Overview and requirements for an NRBG | 17 |
| 8.1 | NRBG overview | 17 |
| 8.2 | Functional model of an NRBG | 18 |
| 8.3 | NRBG entropy sources | 20 |
| 8.3.1 | General | 20 |
| 8.3.2 | Primary entropy source for an NRBG | 20 |
| 8.3.3 | Physical entropy sources for an NRBG | 22 |
| 8.3.4 | NRBG non-physical entropy sources | 22 |
| 8.3.5 | NRBG additional entropy sources | 23 |
| 8.3.6 | Hybrid NRBGs | 24 |
| 8.4 | NRBG additional inputs | 24 |
| 8.4.1 | NRBG additional inputs overview | 24 |
| 8.4.2 | Requirements for NRBG additional inputs | 24 |
| 8.5 | NRBG internal state | 25 |
| 8.5.1 | NRBG internal state overview | 25 |
| 8.5.2 | Requirements for the NRBG internal state | 25 |
| 8.5.3 | Additional information for the NRBG internal state | 26 |
| 8.6 | NRBG internal state transition functions | 26 |

| | | |
|-----------------------|--|----|
| 8.6.1 | NRBG internal state transition functions overview | 26 |
| 8.6.2 | Requirements for the NRBG internal state transition functions | 27 |
| 8.6.3 | Recommendations for the NRBG internal state transition functions | 27 |
| 8.7 | NRBG output generation function | 27 |
| 8.7.1 | NRBG output generation function overview | 27 |
| 8.7.2 | Requirements for the NRBG output generation function | 28 |
| 8.8 | NRBG health tests | 28 |
| 8.8.1 | NRBG health tests overview | 28 |
| 8.8.2 | General NRBG health test requirements | 29 |
| 8.8.3 | NRBG health test on deterministic components | 29 |
| 8.8.4 | NRBG health tests within entropy sources | 30 |
| 8.8.5 | NRBG health tests on random output | 31 |
| 8.9 | NRBG component interaction | 32 |
| 8.9.1 | NRBG component interaction overview | 32 |
| 8.9.2 | Requirements for NRBG component interaction | 32 |
| 8.9.3 | Recommendations for NRBG component interaction | 33 |
| 9 | Overview and requirements for a DRBG | 33 |
| 9.1 | DRBG overview | 33 |
| 9.2 | Functional model of a DRBG | 33 |
| 9.3 | DRBG randomness source | 36 |
| 9.3.1 | Primary randomness source for a DRBG | 36 |
| 9.3.2 | Generating seed values for a DRBG | 37 |
| 9.3.3 | Additional randomness sources for a DRBG | 38 |
| 9.3.4 | Hybrid DRBGs | 38 |
| 9.4 | Additional inputs for a DRBG | 38 |
| 9.5 | Internal state for a DRBG | 39 |
| 9.6 | Internal state transition function for a DRBG | 39 |
| 9.7 | Output generation function for a DRBG | 40 |
| 9.8 | Health tests for a DRBG | 40 |
| 9.8.1 | DRBG health tests overview | 40 |
| 9.8.2 | DRBG health test | 41 |
| 9.8.3 | DRBG deterministic algorithm test | 41 |
| 9.8.4 | DRBG software/firmware integrity test | 41 |
| 9.8.5 | DRBG critical functions test | 41 |
| 9.8.6 | DRBG software/firmware load test | 41 |
| 9.8.7 | DRBG manual key entry test | 42 |
| 9.8.8 | Continuous tests on noise sources in entropy sources | 42 |
| 9.9 | Additional requirements for DRBG keys | 42 |
| Annex A (normative) | Combining RBGs | 44 |
| Annex B (normative) | Conversion methods for random number generation | 45 |
| Annex C (informative) | Deterministic random bit generators | 48 |
| Annex D (informative) | NRBG examples | 75 |
| Annex E (informative) | Security considerations | 84 |
| Annex F (informative) | Discussion on the estimation of entropy | 88 |
| Annex G (informative) | RBG assurance | 89 |
| Annex H (normative) | RBG boundaries | 90 |
| Annex I (informative) | Rationale for the design of statistical tests | 92 |
| Bibliography | | 93 |