

# ISO/IEC 18031:2005-11 (E)

## Information technology - Security techniques - Random bit generation

---

<b>Contents</b>		<b>Page</b>
Foreword .....		vi
Introduction .....		vii
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>4</b>	<b>Symbols .....</b>	<b>5</b>
<b>5</b>	<b>Overarching objectives and requirements of a random bit generator .....</b>	<b>5</b>
5.1	Required properties of randomness .....	6
5.2	Backward and forward secrecy .....	6
5.3	Top-level objectives and requirements for a random bit generator (RBG) output .....	7
5.4	Top-level objectives and requirements for RBG operation .....	7
5.5	Random bit generator functional requirements .....	8
<b>6</b>	<b>General functional model for random bit generation .....</b>	<b>8</b>
6.1	Basic components .....	8
6.1.1	Entropy source .....	9
6.1.2	Additional inputs .....	10
6.1.3	Internal state .....	10
6.1.4	Internal state transition functions .....	11
6.1.5	Output generation function .....	12
6.1.6	Support functions .....	13
<b>7</b>	<b>Types of random bit generators .....</b>	<b>14</b>
7.1	Non-deterministic random bit generators (NRBGs) .....	14
7.2	Deterministic random bit generators (DRBGs) .....	15
7.3	The RBG spectrum .....	15
<b>8</b>	<b>Overview and requirements for a non-deterministic random bit generator .....</b>	<b>16</b>
8.1	Overview .....	16
8.2	Functional model of a non-deterministic random bit generator .....	16
8.2.1	Overview of the model .....	16
8.3	Entropy sources .....	18
8.3.1	Primary entropy source .....	18
8.3.2	Physical entropy sources .....	20
8.3.3	Non-physical entropy sources .....	21
8.3.4	Additional entropy sources .....	21
8.3.5	Hybrid non-deterministic random bit generators .....	22
8.4	Additional inputs .....	23
8.4.1	Overview .....	23
8.4.2	Mandatory requirements .....	23
8.5	Internal state .....	23
8.5.1	Overview .....	23
8.5.2	Mandatory requirements .....	24
8.5.3	Optional requirements .....	24
8.6	Internal state transition functions .....	25
8.6.1	Overview .....	25

8.6.2	Mandatory requirements .....	26
8.6.3	Optional requirements .....	26
8.7	Output generation function .....	26
8.7.1	Overview .....	26
8.7.2	Mandatory requirements .....	26
8.7.3	Optional requirement .....	27
8.8	Health tests .....	27
8.8.1	Overview .....	27
8.8.2	General health test requirements .....	27
8.8.3	Health test on deterministic components .....	28
8.8.4	Health tests on entropy sources .....	28
8.8.5	Health tests on random output .....	29
8.9	Component interaction .....	31
8.9.1	Overview .....	31
8.9.2	Mandatory requirements .....	31
8.9.3	Optional requirements .....	32
9	Overview and requirements for a deterministic random bit generator .....	32
9.1	Overview .....	32
9.2	Functional model of DRBG .....	33
9.2.1	Overview of the model .....	33
9.3	Entropy source .....	35
9.3.1	Primary entropy source .....	35
9.3.2	Generating seed values .....	37
9.3.3	Additional entropy sources .....	37
9.3.4	Hybrid deterministic random bit generator .....	38
9.4	Additional inputs .....	38
9.5	Internal state .....	38
9.6	Internal state transition function .....	39
9.7	Output generation function .....	40
9.7.1	Overview .....	40
9.8	Support functions .....	40
9.8.1	Overview .....	40
9.8.2	Self test .....	40
9.8.3	Deterministic algorithm test .....	41
9.8.4	Software/Firmware integrity test .....	41
9.8.5	Critical functions test .....	41
9.8.6	Software/Firmware load test .....	41
9.8.7	Manual key entry test .....	41
9.8.8	Continuous random bit generator test .....	42
9.9	Additional DRBG functional requirements .....	42
9.9.1	Keys .....	42
Annex A (normative) Combining random bit generators .....		44
Annex B (normative) Conversion methods .....		45
B.1	Random number generation .....	45
B.1.1	The simple discard method .....	45
B.1.2	The complex discard method .....	45
B.1.3	The simple modular method .....	46
B.1.4	The complex modular method .....	46
B.2	Extracting bits in the Dual_EC_DRBG .....	47
B.2.1	Potential bias in an elliptic curve over a prime field $F_p$ .....	47
B.2.2	Adjusting for the missing bit(s) of entropy in the x coordinates .....	48
B.2.3	Values for E .....	49
B.2.4	Observations .....	51
Annex C (normative) Deterministic random bit generators .....		52
C.1	Introduction .....	52
C.2	Deterministic RBGs based on a hash-function .....	52

C.2.1	Hash-function DRBG (Hash_DRBG) .....	52
C.3	DRBG based on block ciphers .....	60
C.3.1	CTR_DRBG .....	61
C.3.2	OFB_DRBG ( .....) .....	70
C.4	Deterministic RBGs based on number theoretic problems .....	72
C.4.1	Dual Elliptic Curve DRBG (Dual_EC_DRBG) .....	72
C.4.2	Micali Schnorr DRBG (MS_DRBG) .....	81
<b>Annex D (normative) Application specific constants .....</b>		<b>91</b>
D.1	Constants for the Dual_EC_DRBG .....	91
D.1.1	Curves over Prime Fields .....	91
D.1.2	Curves over binary fields .....	94
D.2	Default moduli for the MS_DRBG ( .....) .....	103
D.2.1	Default modulus n of size 1024 bits .....	103
D.2.2	Default modulus n of size 2048 bits .....	103
D.2.3	Default modulus n of size 3072 bits .....	104
D.2.4	Default modulus n of size 7680 bits .....	104
D.2.5	Default modulus n of size 15360 bits .....	105
<b>Annex E (informative) Non-deterministic random bit generator examples .....</b>		<b>107</b>
E.1	Canonical coin tossing example .....	107
E.1.1	Overview .....	107
E.1.2	Description of basic process .....	107
E.1.3	Relation to standard NRBG components .....	107
E.1.4	Optional variations .....	108
E.1.5	Peres unbiasing procedure .....	108
E.2	Hypothetical noisy diode example .....	109
E.2.1	Overview .....	109
E.2.2	General structure .....	109
E.2.3	Details of operation .....	110
E.2.4	Failsafe design consequences .....	114
E.2.5	Modified example .....	114
E.3	Mouse movement example .....	115
<b>Annex F (informative) Security considerations .....</b>		<b>116</b>
F.1	Attack model .....	116
F.2	The security of hash-functions .....	116
F.3	Algorithm and key size selection .....	116
F.3.1	Equivalent algorithm strengths .....	117
F.3.2	Selection of appropriate DRBGs .....	118
F.4	The security of block cipher DRBGs .....	119
F.5	Conditioned entropy sources and the derivation function .....	119
<b>Annex G (informative) Discussion on the estimation of entropy .....</b>		<b>120</b>
<b>Annex H (informative) Random bit generator assurance .....</b>		<b>121</b>
<b>Annex I (informative) Random bit generator boundaries .....</b>		<b>122</b>
<b>Bibliography .....</b>		<b>124</b>