

# ISO/IEC 18370-2:2016-07 (E)

## Information technology - Security techniques - Blind digital signatures - Part 2: Discrete logarithm based mechanisms

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols .....	3
5	General requirements .....	4
6	Blind signature mechanisms .....	4
6.1	General .....	4
6.2	Mechanism 1 .....	4
6.2.1	Security parameters .....	4
6.2.2	Key generation process .....	5
6.2.3	Blind signature process .....	5
6.2.4	Verification process .....	6
7	Blind signature mechanisms with partial disclosure .....	6
7.1	General .....	6
7.2	Mechanism 2 .....	6
7.2.1	Security parameters .....	6
7.2.2	Key generation process .....	6
7.2.3	Blind signature process with partial disclosure .....	7
7.2.4	Verification process .....	8
7.3	Mechanism 3 .....	8
7.3.1	Symbols .....	8
7.3.2	Key generation process .....	8
7.3.3	Blind signature process with partial disclosure .....	9
7.3.4	Verification process .....	9
8	Blind signature mechanisms with selective disclosure .....	10
8.1	General .....	10
8.2	Mechanism 4 .....	10
8.2.1	Security parameters .....	10
8.2.2	Key generation process .....	10
8.2.3	Blind signature process with selective disclosure .....	10
8.2.4	Presentation process .....	12
8.2.5	Verification process .....	12
9	Traceable blind signature mechanisms .....	13
9.1	General .....	13
9.2	Mechanism 5 .....	13
9.2.1	Symbols .....	13
9.2.2	Key generation process .....	13
9.2.3	Traceable blind signature process .....	14
9.2.4	Verification process .....	16

9.2.5	Requestor tracing process .....	16
9.2.6	Signature tracing process .....	17
9.2.7	Requestor tracing evidence evaluation process .....	17
9.2.8	Signature tracing evidence evaluation process .....	17
Annex A (normative) Object identifiers .....		19
Annex B (normative) Conversion functions .....		20
Annex C (normative) Group description .....		21
Annex D (informative) Special hash-functions .....		22
Annex E (informative) Security considerations and comparison of blind signature mechanisms .....		24
Annex F (informative) Numerical examples .....		26
Bibliography .....		78