

# ISO/IEC 18370-1:2016-11 (E)

## Information technology - Security techniques - Blind digital signatures - Part 1: General

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Abbreviated terms and figure elements .....	7
5	Blind signatures .....	8
5.1	General .....	8
5.2	Entities .....	8
5.3	Key generation .....	8
5.4	Blind signature process .....	8
5.5	Verification process .....	9
6	Blind signatures with partial disclosure .....	10
6.1	General .....	10
6.2	Entities .....	10
6.3	Key generation .....	10
6.4	Blind signature process with partial disclosure .....	10
6.5	Verification process .....	11
7	Blind signatures with selective disclosure .....	12
7.1	General .....	12
7.2	Entities .....	13
7.3	Key generation .....	13
7.4	Blind signature process with selective disclosure .....	13
7.5	Presentation process .....	14
7.6	Verification process .....	15
8	Traceable blind signatures .....	16
8.1	General .....	16
8.2	Entities .....	17
8.3	Key generation .....	17
8.4	Traceable blind signature process .....	17
8.5	Verification process .....	18
8.6	Requestor tracing process .....	19
8.7	Requestor tracing evidence evaluation process .....	20
8.8	Signature tracing process .....	21
8.9	Signature tracing evidence evaluation process .....	22
Annex A (informative) Comparison table of blind digital signature mechanisms .....		23
Annex B (informative) Additional security information for blind signatures with selective disclosure .....		24
Bibliography .....		27