

# ISO/IEC 20008-2:2013-11 (E)

## Information technology - Security techniques - Anonymous digital signatures - Part 2: Mechanisms using a group public key

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols (and abbreviated terms) .....	2
5	General model and requirements .....	3
6	Mechanisms with linking capability .....	4
6.1	General .....	4
6.2	Mechanism 1 .....	5
6.2.1	Symbols .....	5
6.2.2	Key generation process .....	5
6.2.3	Signature process .....	8
6.2.4	Verification process .....	9
6.2.5	Linking process .....	10
6.2.6	Revocation process .....	10
6.3	Mechanism 2 .....	10
6.3.1	Symbols .....	10
6.3.2	Key generation process .....	11
6.3.3	Signature process .....	13
6.3.4	Verification process .....	14
6.3.5	Linking process .....	15
6.3.6	Revocation process .....	15
6.4	Mechanism 3 .....	16
6.4.1	Symbols .....	16
6.4.2	Key generation process .....	16
6.4.3	Signature process .....	17
6.4.4	Verification process .....	18
6.4.5	Linking process .....	19
6.4.6	Revocation process .....	19
6.5	Mechanism 4 .....	20
6.5.1	Symbols .....	20
6.5.2	Key generation process .....	20
6.5.3	Signature process .....	22
6.5.4	Verification process .....	22
6.5.5	Linking process .....	23
6.5.6	Revocation process .....	23
7	Mechanisms with opening capability .....	23
7.1	General .....	23
7.2	Mechanism 5 .....	23
7.2.1	Symbols .....	23
7.2.2	Key generation process .....	24
7.2.3	Signature process .....	25

7.2.4	Verification process .....	26
7.2.5	Opening process .....	26
7.2.6	Revocation process .....	26
7.3	Mechanism 6 .....	27
7.3.1	Symbols .....	27
7.3.2	Key generation process .....	27
7.3.3	Signature process .....	28
7.3.4	Verification process .....	29
7.3.5	Opening process .....	29
7.3.6	Revocation process .....	29
8	Mechanisms with both opening and linking capabilities .....	29
8.1	General .....	29
8.2	Mechanism 7 .....	30
8.2.1	Symbols .....	30
8.2.2	Key generation process .....	30
8.2.3	Signature process .....	32
8.2.4	Verification process .....	32
8.2.5	Opening process .....	33
8.2.6	Evidence evaluation process .....	33
8.2.7	Linking process .....	33
8.2.8	Revocation process .....	34
Annex A (normative) Object identifiers .....		35
Annex B (normative) Special hash-functions .....		37
Annex C (informative) Security guidelines for the anonymous signature mechanisms .....		39
Annex D (informative) Comparison of revocation mechanisms .....		42
Annex E (informative) Numerical examples .....		45
Annex F (informative) Proof of correct generation in Mechanism 5 .....		80
Bibliography .....		84