

# ISO/IEC 20008-1:2013-12 (E)

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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Terms and definitions .....	1
3	Abbreviations and legend for figures .....	8
4	Options for a group public key and multiple public keys .....	9
5	General requirements .....	11
6	Mechanisms using a group public key .....	12
6.1	General model .....	12
6.2	Entities .....	13
6.3	Key generation process .....	13
6.4	Group signature process .....	14
6.5	Group signature verification process .....	14
6.6	Group membership opening process .....	14
6.7	Group signature linking process .....	15
6.8	Group signature revocation process .....	16
7	Mechanisms using multiple public keys .....	19
7.1	General model .....	19
7.2	Entities .....	19
7.3	Key generation process .....	19
7.4	Ring signature process .....	19
7.5	Ring signature verification process .....	19
Bibliography .....		20