

ISO/IEC 14888-1:2008-04 (E)

Information technology - Security techniques - Digital signatures with appendix - Part 1: General

| Contents | | Page |
|--|---|-------------|
| Foreword | | iv |
| Introduction | | v |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 1 |
| 4 | Symbols, conventions, and legend for figures | 3 |
| 4.1 | Symbols | 3 |
| 4.2 | Coding convention | 4 |
| 4.3 | Legend for figures | 4 |
| 5 | General | 4 |
| 6 | General model | 5 |
| 7 | Options for binding signature mechanism and hash-function | 6 |
| 8 | Key generation | 6 |
| 9 | Signature process | 7 |
| 9.1 | General | 7 |
| 9.2 | Computing the signature | 7 |
| 9.3 | Constructing the appendix | 7 |
| 9.4 | Constructing the signed message | 7 |
| 10 | Verification process | 8 |
| Annex A (informative) On hash-function identifiers | | 10 |
| Bibliography | | 11 |