

ISO/IEC 13888-1:2009-07 (E)

Information technology - Security techniques - Non-repudiation - Part 1: General

| Contents | | Page |
|--------------------|--|-------------|
| Foreword | | iv |
| Introduction | | v |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 1 |
| 4 | Symbols and abbreviated terms | 8 |
| 5 | Organisation of the remainder of this part of ISO/IEC 13888 | 8 |
| 6 | Requirements | 9 |
| 7 | Generic non-repudiation services | 9 |
| 7.1 | Entities involved in the provision and verification of evidence | 9 |
| 7.2 | Non-repudiation services | 10 |
| 8 | Trusted third party involvement | 10 |
| 8.1 | General | 10 |
| 8.2 | Evidence generation phase | 10 |
| 8.3 | Evidence transfer, storage and retrieval phase | 11 |
| 8.4 | Evidence verification phase | 11 |
| 9 | Evidence generation and verification mechanisms | 12 |
| 9.1 | General | 12 |
| 9.2 | Secure envelopes | 12 |
| 9.3 | Digital signatures | 13 |
| 9.4 | Evidence verification mechanism | 13 |
| 10 | Non-repudiation tokens | 13 |
| 10.1 | General | 13 |
| 10.2 | Generic non-repudiation token | 14 |
| 10.3 | Time-stamping token | 15 |
| 10.4 | Notarization token | 15 |
| 11 | Specific non-repudiation services | 15 |
| 11.1 | General | 15 |
| 11.2 | Non-repudiation of origin | 16 |
| 11.3 | Non-repudiation of delivery | 16 |
| 11.4 | Non-repudiation of submission | 16 |
| 11.5 | Non-repudiation of transport | 16 |
| 12 | Use of specific non-repudiation tokens in a messaging environment | 17 |
| Bibliography | | 19 |