

ISO/IEC 9798-3:2019 (E)

IT Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques

Contents

| | |
|---------|---|
| | Foreword |
| 1 | Scope |
| 2 | Normative references |
| 3 | Terms and definitions |
| 4 | Symbols and abbreviated terms |
| 5 | General |
| 5.1 | Time variant parameters |
| 5.2 | Tokens |
| 5.3 | Use of text fields |
| 6 | Requirements |
| 7 | Mechanisms without an on-line trusted third party |
| 7.1 | Unilateral authentication |
| 7.1.1 | General |
| 7.1.2 | Mechanism UNI.TS — One-pass authentication |
| 7.1.3 | Mechanism UNI.CR — Two-pass authentication |
| 7.2 | Mutual authentication |
| 7.2.1 | General |
| 7.2.2 | Mechanism MUT.TS — Two-pass authentication |
| 7.2.3 | Mechanism MUT.CR — Three-pass authentication |
| 7.2.4 | Mechanism MUT.CR.par — Two-pass parallel authentication |
| 8 | Mechanisms involving an on-line trusted third party |
| 8.1 | General |
| 8.2 | Unilateral authentication |
| 8.2.1 | General |
| 8.2.2 | Mechanism TP.UNI.1 — Four-pass authentication (initiated by A) |
| 8.2.3 | Mechanism TP.UNI.2 — Four-pass authentication (initiated by B) |
| 8.3 | Mutual authentication |
| 8.3.1 | General |
| 8.3.2 | Mechanism TP.MUT.1 — Five-pass authentication (initiated by A) |
| 8.3.3 | Mechanism TP.MUT.2 — Five-pass authentication (initiated by B) |
| 8.3.4 | Mechanism TP.MUT.3 — Seven-pass authentication (initiated by B) |
| Annex A | (normative) Object Identifiers |
| A.1 | Formal definition |
| A.2 | Use of subsequent object identifiers |
| Annex B | (informative) Usage guidance |
| B.1 | Security properties |
| B.1.1 | Entity Authentication |
| B.1.2 | Unilateral and mutual authentication |
| B.1.3 | Certificate distribution and trust |
| B.2 | Comparison and selection of mechanisms |
| B.2.1 | Comparison |
| B.2.2 | Recommendations for the selection of a mechanism |
| Annex C | (informative) Use of text fields |