ISO/IEC 9798-2:2019 (E)

IT Security techniques — Entity authentication — Part 2: Mechanisms using authenticated encryption

Contents

Foreword

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 General

6 Requirements

7 Mechanisms not involving an on-line trusted third party

- 7.1 General
- 7.2 Unilateral authentication
- 7.2.1 General
- 7.2.2 Mechanism UNI.TS — One-pass authentication
- 7.2.3 Mechanism UNI.CR — Two-pass authentication
- 7.3 Mutual authentication
- 7.3.1 General
- 7.3.2 Mechanism MUT.TS — Two-pass authentication
- 7.3.3 Mechanism MUT.CR — Three-pass authentication

8 Mechanisms involving an on-line trusted third party

- 8.1 General
- 8.2 Mechanism TP.TS — Four-pass authentication
- 8.3 Mechanism TP.CR — Five-pass authentication

Annex A (normative) Object Identifiers

- A.1 Formal definition
- A.2 Use of subsequent object identifiers

Annex B (informative) Use of text fields

Annex C (informative) Properties of entity authentication mechanisms

Page count: 15