ISO/IEC 29128-2:2026-09 (E)

Information security, cybersecurity and privacy protection - Verification of cryptographic protocols - Part 2: Evaluation methods and activities for cryptographic protocols

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Security assessment and verification of cryptographic protocols 2
4.1 Overview 2
4.2 Prover 4
4.2.1 Prover assurance level 4
4.2.2 Prover confidence level 4
4.3 Models 4
4.3.1 Cryptographic protocol model 4
4.3.2 Adversarial model 5
4.3.3 Formal protocol specification 5
4.3.4 Security properties 6

5 Method for cryptographic protocol security evaluation 6
5.1 Overview 6
5.2 Scope of cryptographic evaluation method 6
5.3 Cryptographic protocol evaluation method 7
5.3.1 General 7
5.3.2 Prover evaluation method 7
5.3.3 Model evaluation method 7

6 Activities for cryptographic protocol security evaluation 8

Annex A (informative) List of tools for automated model verification 10

Annex B (informative) Evaluation of the prover 11

Annex C (informative) Extension model 12

Annex D (informative) Relationship between confidence levels with Implementation Assurance Levels in ISO/IEC 29128-3 13

Bibliography 14