

ISO/IEC 29128-1:2023-03 (E)

Information security, cybersecurity and privacy protection - Verification of cryptographic protocols - Part 1: Framework

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Formal verification of cryptographic protocols	2
4.1	Methods for modelling cryptographic protocols	2
4.2	Verification requirements	3
4.2.1	Methods of verification	3
4.2.2	Verification tools	3
4.2.3	Bounded vs unbounded verification	3
4.3	Cryptographic protocol model	4
4.3.1	Description of a model	4
4.3.2	Formal specification	4
4.3.3	Adversarial model	5
4.3.4	Submitting a model	5
4.3.5	Security properties	5
4.3.6	Self-assessment evidence	6
5	Verification process	6
5.1	General	6
5.2	Duties of the submitter	6
5.3	Duties of the evaluator	6
5.3.1	Main duties	6
5.3.2	Evaluating the prover	6
5.3.3	Evaluating the model	6
5.3.4	Evaluating the evidence	7
5.3.5	Example evaluation	7
Annex A (informative)	The Needham-Schroeder-Lowe public key protocol	8
Annex B (informative)	Example submission	9
Annex C (informative)	Example evaluation	10
Annex D (informative)	Dolev-Yao model	11
Annex E (informative)	Security properties	12
Bibliography		14