

ISO/IEC 18014-2:2021-09 (E)

Information security - Time-stamping services - Part 2: Mechanisms producing independent tokens

Contents		Page
Foreword		iv
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Notation, symbols and abbreviated terms	4
5	Time-stamp tokens	5
5.1	5
5.2	Generation	5
5.3	Verification	5
5.4	Renewal	6
5.5	Renewal verification	6
6	Protection mechanisms	7
7	Independent time-stamp tokens	8
7.1	Core structure	8
7.2	Extensions	8
7.3	Protection mechanisms	9
7.3.1	Digital signatures using SignedData	9
7.3.2	Message authentication codes using AuthenticatedData	9
7.3.3	Archival	10
7.3.4	Digital signatures using SignerInfo	11
7.4	Protocols	12
Annex A (normative) ASN.1 Module for time-stamping		13
Annex B (informative) Cryptographic syntax		19
Bibliography		22