ISO/IEC 18014-2:2009-12 (E)

Information technology - Security techniques - 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 5

5 Time-stamping services 5

6 Time-stamp tokens 6
6.1 Contents 6
6.2 Notation 7
6.3 Verification 7
6.4 Renewal 8
6.5 Renewal verification 8

7 Protection mechanisms 9

8 Independent time-stamp tokens 10
8.1 Core structure 10
8.2 Extensions 10
8.3 Protection mechanisms 11
8.3.1 Digital signatures using SignedData 11
8.3.2 Message authentication codes using AuthenticatedData 11
8.3.3 Archival 13
8.3.4 Digital signatures using SignerInfo 13
8.4 Protocols 15

Annex A (normative) ASN.1 Module for Time-Stamping 16

Annex B (informative) Cryptographic Syntax 22

Bibliography 28