ISO/IEC 18014-3:2009-12 (E)

Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 General discussion 3

5 Operations specific to TSAs producing linked tokens 3
5.1 Linking operation 3
5.2 Aggregation operation 4
5.3 Publishing operation 5
5.4 Extend operation 5

6 Message formats 5
6.1 Time-stamp request 5
6.2 Time-stamp response 6
6.3 Verify request 6
6.4 Verify response 7
6.5 Extend request 7
6.6 Extend response 7

7 Data types 8
7.1 Object identifiers 8
7.2 TSTInfo 8
7.3 TimeStampToken 9
7.4 BindingInfo 10
7.5 Chain 11
7.6 Link 11
7.7 Node 12
7.8 PublicationInfo 12
7.9 Extensions 13

8 Generating a time-stamp token 15
8.1 General 15
8.2 DigestedData encapsulation 16
8.3 SignedData encapsulation 16
8.4 Security considerations 17

9 Verifying a time-stamp token 17
9.1 General 17
9.2 DigestedData encapsulation 18
9.3 SignedData encapsulation 18
9.4 Security considerations 18

10 Extending a time-stamp token 18

11 Renewing a time-stamp token 19
11.1 General 19
11.2 Renewal and verify operation 19
11.3 Renewal and extend operation 19

Annex A (normative) ASN.1 Module for time-stamping 21

Annex B (informative) Additional discussion 29

Annex C (informative) Data structures 33

Bibliography 37