ISO 22376:2023-08 (E)

Security and resilience - Authenticity, integrity and trust for products and documents - Specification and usage of visible digital seal (VDS) data format for authentication, verification and acquisition of data carried by a document or object

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 General concepts 5

5 Structures and resources 6
5.1 General 6
5.2 Trust service list and extensions 6
5.2.1 General 6
5.2.2 Extensions 6
5.2.3 TSO identity 6
5.2.4 TSO manifest location 6
5.2.5 CA reference 6
5.2.6 Public certificate directory 7
5.2.7 XML security 7
5.2.8 Example and verification 7
5.3 Manifest 7
5.3.1 General 7
5.3.2 Information section 7
5.3.3 Schema section 8
5.3.4 Extensions section 10
5.3.5 XML security 11
5.3.6 Example and verification 11
5.4 Manifest extensions 11
5.4.1 General 11
5.4.2 Policies extension 11
5.4.3 Authorized usage policy 11
5.5 VDS 11
5.5.1 General 11
5.5.2 Binary encoding 12
5.5.3 Header section 12
5.5.4 Payload section 14
5.5.5 Signature section 15
5.5.6 Auxiliary data section 16
5.5.7 Example 16
5.6 Signing certificate 16
5.6.1 General 16
5.6.2 Usage list extensions 17

6 Production process 17

7 Verification process 18

7.1 General concepts 18
7.2 Acquisition of VDS data 18
7.3 Header structure analysis 18
7.4 Reference retrieval and verification 18
7.4.1 General 18
7.4.2 TSL 18
7.4.3 Manifest 19
7.4.4 Signing certificate and certificate revocation list 19
7.5 Payload processing 19
7.6 Extensions processing 19
7.7 Signature verification 19
7.8 Document data presentation 19

Annex A (informative) VDS encoding example 20

Annex B (informative) TSL example 22

Annex C (informative) Manifest example 26

Annex D (informative) TSL XML schema definition example 28

Annex E (informative) Manifest XML schema definition example 29

Bibliography 40