ISO/IEC 20248:2022-06 (E)

Information technology - Automatic identification and data capture techniques - Digital signature data structure schema

Contents

Page

Foreword ..... **v**

Introduction ..... **vii**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Field and data definitions, abbreviated terms, symbols, and binary data **4**
4.1 Field and data definitions 4
4.2 Abbreviated terms 4
4.3 Symbols 5
4.4 Binary data 5

5 Conformance **5**
5.1 Specification version 5
5.2 Claiming conformance 6
5.3 Test authority 6
5.4 Test specification 6

6 DigSig use architecture **6**
6.1 General 6
6.2 DigSig identification and ownership 7
6.3 DigSig certificate process 8
6.4 DigSig generation process 9
6.5 DigSig verification process 9
6.6 Error codes 10

7 DigSig certificate **10**
7.1 General 10
7.2 ISO/IEC 20248 Object Identifier 10
7.3 DigSig certificate parameter use 10
7.4 DigSig cryptography 11
7.4.1 General 11
7.4.2 Digital signatures 11
7.4.3 Private containers 11
7.5 DigSig Domain Authority identifier (DAID) 11
7.5.1 Binary encoding 11
7.5.2 Referenced DAID 13
7.5.3 GS1 Company Prefix (GCP) 13
7.6 DigSig certificate identifier (CID) 13
7.7 DigSig validity 13
7.8 DigSig certificate management 14
7.9 DigSig revocation 14
7.10 Online verification 15

8 DigSig Data Description (DDD) **15**
8.1 General 15
8.2 DDD derived data structures 16
8.2.1 General 16
8.2.2 DDDdata 16
8.2.3 SigData 17
8.2.4 DDDdataTagged 17

8.2.5 DDDdataDisplay 18
8.3 DigSig format 18
8.3.1 General 18
8.3.2 Snips 18
8.3.3 Envelope format 19
8.3.4 AIDC specific construction of a DigSig 19
8.4 The DigSig physical data path 20
8.5 DDD syntax 21
8.6 DigSig information fields 22
8.7 Data fields 23
8.7.1 General 23
8.7.2 Compulsory data fields 23
8.7.3 Application data fields 23
8.8 Data field object syntax 24
8.9 DDD field types and associate settings 25
8.9.1 General 25
8.9.2 Special field values 25
8.9.3 Field types 26
8.10 DigSig data presentation 35
8.10.1 General 35
8.10.2 displaystring 36
8.10.3 displayformat 36
8.10.4 DDDdataDisplay generation 39
8.11 Structured document processing 40
8.12 Application field specification by codebook 41

9 Pragmas (field directives) 42
9.1 General 42
9.2 entertext 42
9.3 structjoin 43
9.4 readmethod 43
9.5 privatecontainer 44
9.6 startonword 45

Annex A (normative) **Test methods 46**

Annex B (informative) **Example DigSigs 49**

Annex C (informative) **DigSig use in IoT 57**

Annex D (informative) **Typical DigSig EncoderGenerator device architecture 60**

Annex E (informative) **Typical DigSig DecoderVerifier device architecture 69**

Annex F (normative) **DigSig error codes 75**

Annex G (informative) **Digital Signature use considerations 76**

Annex H (informative) **Example of a DigSig certificate 77**

Annex I (informative) **Example DDD for a physical certificate 79**

Annex J (normative) **DigSig revocation specifications 84**

Annex K (informative) **ISO/IEC 15434-based message DigSig examples 89**

Annex L (informative) **DigSig URI envelope discussion 93**

Annex M (informative) **ISO/IEC 18000-63 and GS1 EPC Gen2 RFID DigSig examples 94**

Annex N (informative) **Typical DigSig support infrastructure 98**

Annex O (informative) **Example structured document 103**

Bibliography 105