ISO/IEC 20248:2018 (E)

Information technology — Automatic identification and data capture techniques — Data structures — Digital signature meta structure

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Field and data definitions, abbreviations and symbols

4.1 Field and data definitions
4.2 Abbreviations
4.3 Symbols

5 Conformance

5.1 Specification version
5.2 Claiming conformance
5.3 Test authority
5.4 Test specification

6 DigSig use architecture

6.1 General
6.2 DigSig Certificate process
6.3 DigSig generation process
6.4 DigSig verification process
6.5 Error codes

7 DigSig Certificate

7.1 General
7.2 ISO/IEC 20248 Object Identifier
7.3 DigSig Certificate parameter use
7.4 DigSig cryptography
7.4.1 General
7.4.2 Digital Signatures
7.4.3 Private containers
7.5 DigSig Domain Authority identifier
7.6 DigSig Certificate identifier (CID)
7.7 DigSig validity
7.8 DigSig Certificate management
7.9 DigSig revocation
7.10 Online verification

8 DigSig Data Description (DDD)

8.1 General
8.2 DDD derived data structures
8.2.1 General
8.2.2 DDDdata
8.2.3 SigData
8.2.4 DDDdataTagged
8.2.5 DDDdataDisplay
8.3 DigSig format
8.3.1 General

8.3.2 Snips
8.3.2.1 Snip types
8.3.2.2 Snip encoding
8.3.3 Envelope format
8.3.3.1 General
8.3.3.2 RAW Envelope
8.3.3.3 URI Envelope
8.3.4 AIDC specific construction of a DigSig
8.4 The DigSig physical data path
8.5 DDD syntax
8.6 DigSig information fields
8.7 Data fields
8.7.1 Compulsory data fields
8.7.2 Application data fields
8.8 Data field object syntax
8.9 DDD field types and associate settings
8.9.1 General
8.9.2 Special field values
8.9.2.1 The DDD field value “null”
8.9.2.2 Array of field values - cardinality
8.9.3 Field types
8.9.3.1 boolean
8.9.3.2 unsignedint
8.9.3.3 number
8.9.3.4 string
8.9.3.5 bstring
8.9.3.6 digsigenv
8.9.3.7 date
8.9.3.8 enum
8.9.3.9 struct
8.9.4 Special types
8.9.4.1 General
8.9.4.2 displaystring

9 Pragmas

9.1 General
9.2 entertext
9.3 structjoin
9.4 readmethod
9.5 privatecontainer
9.6 startonword
9.7 cidsniptext

Annex A (normative) Test methods

A.1 DigSig Certificate format
A.1.1 General
A.1.2 Test configuration
A.1.3 Test method
A.1.4 Test report
A.2 DigSig Data
A.2.1 General
A.2.2 Test configuration
A.2.3 Test method
A.2.4 Test report
A.3 DigSig DecoderVerifier
A.3.1 General
A.3.2 Test configuration
A.3.3 Test method
A.3.3.1 Test by inspection
A.3.3.2 Test by execution against a norm data set
A.3.4 Test report
A.4 DigSig EncoderGenerator
A.4.1 General
A.4.2 Test configuration

A.4.3 Test method
A.4.3.1 Test by inspection
A.4.3.2 Test by execution against a norm data set
A.4.3.3 Test report

Annex B (informative) Example DigSigs

B.1 General
B.2 DigSig shorthand syntax
B.3 A simple timestamp
B.4 Barcode DigSigs for mobile phones
B.5 A RFID example
B.6 A simple file system
B.7 A sequence of DigSigs
B.8 Selective struct
B.9 Multiple DigSigs using the same base data
B.10 Null encryption — Trusted data definition
B.11 Simple data error detection

Annex C (informative) DigSig use in IoT

Annex D (informative) Typical DigSig EncoderGenerator device architecture

Annex E (informative) Typical DigSig DecoderVerifier device architecture

Annex F (normative) DigSig error codes

Annex G (informative) Digital Signature use considerations

Annex H (informative) Example of a DigSig Certificate

Annex I (informative) Example DDD for a physical certificate

I.1 General
I.2 Example university course certificate
I.3 Example DDD
I.4 Example Snips
I.5 Example DDDdata input
I.6 Example DDDdata
I.7 Example SigData
I.8 Example DDDdataTagged
I.9 Example DDDdataDisplay

Annex J (normative) DigSig revocation specifications

J.1 General
J.2 Revocation response rules
J.3 DigSig revocation lists
J.4 DigSig revocation list download
J.5 Online DigSig revocation check

Annex K (normative) 2D bar code symbologies — Encoding and decoding the DigSig

K.1 Symbologies capable of supporting DigSigs
K.2 Requirements and constraints
K.2.1 Symbology encoder requirements and constraints
K.2.2 Symbology decoder and reader requirements and constraints
K.3 Common RAW envelope encoding and decoding rules
K.3.1 RAW envelope encoding
K.3.2 RAW envelope decoding
K.4 URI envelope encoding and decoding rules
K.4.1 URI envelope encoding
K.5 Symbology specific rules
K.5.1 Common rules for all symbologies
K.5.2 ISO/IEC 15438 PDF417
K.5.2.1 Common rules for PDF417
K.5.2.2 PDF417 and RAW envelopes
K.5.2.3 PDF417 and URI envelopes

K.5.3 ISO/IEC 16022 Data Matrix
K.5.3.1 Common rules for Data Matrix
K.5.3.2 Data Matrix and RAW envelopes
K.5.3.3 Data Matrix and URI envelopes
K.5.4 ISO/IEC 18004 QR Code
K.5.4.1 Common rules for QR code
K.5.4.2 QR Code and RAW envelopes
K.5.4.3 QR Code and URI envelopes
K.5.5 ISO/IEC 24728 MicroPDF417
K.5.5.1 Common rules for MicroPDF417
K.5.5.2 MicroPDF417 and RAW envelopes
K.5.5.3 MicroPDF417 and URI envelopes
K.5.6 ISO/IEC 24778 Aztec Code
K.5.6.1 Common rules for Aztec Code
K.5.6.2 Aztec Code and RAW envelopes
K.5.6.3 Aztec Code and URI envelopes
K.6 Examples

Annex L (normative) ISO/IEC 18000#3 Mode 1 RFID protocol and DigSigs

L.1 General
L.2 RFID air interface protocol requirements and constraints
L.2.1 General
L.2.2 Declaring memory parameters
L.2.3 AFI memory
L.2.4 DSFID memory
L.2.5 Required air interface commands
L.2.6 Air interface conformance and performance
L.3 Designing a DigSig for ISO/IEC 18000#3 Mode 1 tags
L.4 Encoding and decoding rules
L.4.1 Overview
L.4.2 Data capture considerations
L.4.2.1 AFI
L.4.2.2 Data format
L.4.2.3 DSFID
L.4.3 The OID structure for data sets
L.4.4 Data set for Relative-OID value 1 to 14
L.4.4.1 Overview
L.4.4.2 Compaction code
L.4.4.3 The data set for Relative-OID 1
L.4.4.4 The data set for Relative-OID 2 to 14
L.4.4.5 Locking a data set
L.5 Device interface

Annex M (normative) ISO/IEC 18000#63 RFID protocol and DigSigs

M.1 General
M.2 RFID air interface protocol requirements and constraints
M.2.1 General
M.2.2 Declaring memory parameters
M.2.3 AFI memory
M.2.4 DSFID memory
M.2.5 Required air interface commands
M.3 Designing a DigSig for ISO/IEC 18000#63 tags
M.4 Encoding and decoding rules
M.4.1 Overview
M.4.2 Data capture considerations
M.4.2.1 AFI
M.4.2.2 Data format
M.4.2.3 DSFID
M.4.3 The OID structure for data sets
M.4.4 Data set for Relative-OID value 2 to 14
M.4.4.1 Overview
M.4.4.2 Compaction code
M.4.4.3 The data set for Relative-OID 2 to 14
M.4.4.4 Locking a data set

M.4.5 Additional 18000-63 considerations
M.5 Device interface

Page count: 81