INTERNATIONAL STANDARD

ISO/IEC 20248

Second edition
2022-06

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

Technologies de l'information — Techniques d'identification automatique et de capture de données — Schéma de structure de données de signature numérique

Reference number
ISO/IEC 20248:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see

This document was prepared by joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 20248:2018), which has been technically revised.

The main changes are as follows:

— The relationship between the Domain Authority (data owner) and the Domain Authority ID (DAID) is clarified to be one-to-many. The DAID has been extended to cater for the GS1 Company Prefix longer than 10 digits (see 7.5.3), and a method to use the primary data carrier DAID, if present (see 7.5.2).

— The data types and specifications have been updated for easier implementation and completeness, especially to support the practice of using the data type specifications to achieve optimized schema-based data encoding. A codebook method forms part of this update.

— The `date` field type has been found to be limiting. A new human readable `isodate` has been specified to replace `date` (see 8.9.3.7).

— The format of binary data is explicitly defined to be `HexString` or `Base64String` ensuring interoperability and ease of use.

— The `bstring` DDDdata has been limited to `HexString` since Base64 decoding can be done in more than one way which may cause a valid DigSig to be rejected.

— The `digsigenv` type has been changed from `bstring` to `string` with a range of `Base64String`, which is technically the same, but explicit and clear.

— The `cidsniptext` pragma (field directive) has been removed since it is not practical, not used, and redundant. It is also difficult and convoluted to use and implement.

© ISO/IEC 2022 – All rights reserved

— ISO/IEC 9899, *Information technology — Programming languages — C* has been removed as a normative reference. Common current coding language methods replaced the C methods.

— Example cryptography methods are provided in B.4.

— Example interfaces to potential code blocks are provided in D.3.3 and E.3.3.

— Revocation has been harmonized with conventional best practices. The CID requirement to be 0 and 1 has been removed (see Annex J).

— An example implementation architecture description has been added as Annex N.

— The structured document function (see 8.11) has been enhanced to support multiple languages. An example structured document is discussed as Annex O.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2022 – All rights reserved

Introduction

This document specifies a data structure framework and data specification method for domain-authority-specified, schema-based item identification data. A domain authority is typically a brand owner, a data authority, or a data owner.

ISO/IEC 21778 (JSON) is used as the data message format for both the schema and the data, ensuring interoperability with modern Internet systems and services. The data message encapsulates both data syntax and semantics, providing meaning to the data message.

The data source, data schema and data are both offline and online verifiable using ISO/IEC 9594-8 (public key infrastructure (PKI) digital signatures and certificates), with its implementation environment. The data message format allows for the verification of the data message anywhere within the data-stack.

Data capacity and/or data transfer capacity of automated identification data carriers (barcode labels and RFID tags) are limited. This restricts the normal use of a digital signature, as specified in ISO/IEC 9594-8, within automated identification services. This limitation is overcome by the methods specified in this document, which recognizes the three classes of item; data carrier data (any combination of barcodes and RFID tags), generic data which applies to a group of items, and item specific data which may be static for that item, or volatile. Only item specific data are carried by the tag. Generic data are carried by the digital certificate associated with the tag. This method allows additional (comprehensive) data about a group of items to be readable and verifiable.

Adding additional data, especially authenticity data, to tags are often challenging for existing systems resulting in high costs and system/services unavailability. This document provides a method whereby data may be added with limited impact to incumbent systems, facilitating an interoperable add-on rather than a system redesign.

This document specifies an effective and interoperable method to specify, read, decode, and verify data stored in automated identification, independent from real-time remote control. Meta parameters included in a digital certificate are used to achieve:

— offline integrity verification of the data source and data originality,

— a verifiable data structure description to enable interoperability of deployment, domain authority and automated identification data carriers,

— a verifiable data encoding method to achieve compact data to be stored in data constrained automated identification data carriers (the JSON data format is used for both input and output of the encoder and decoder),

— a verifiable automated identification data carrier read method description, allowing for the data of a read event to be distributed over more than one carrier of the same and of different technologies, and

— a verifiable method to support key management of cryptographically-enabled automatic identification data carriers.

A successful verification of the DigSig signifies:

— the data was not tampered with;

— the source of the data is as indicated on the DigSig certificate used to verify the DigSig with;

— if a secured unique identifier of the data carrier is included in the signature of the DigSig stored on data carrier, then the DigSig stored on the data carrier can be considered unique and original.

The choice of cryptography method should be considered carefully. It is advised that only internationally recognized or standardized methods, e.g. FIPS PUB 186-4 and IEEE P1363, be used.

© ISO/IEC 2022 – All rights reserved

This document should be used in conjunction with standard risk assessments of the use-case and environment.

NOTE Many applications rely on a secure non-transferable unique data carrier identifier to tag an item uniquely. ISO/IEC 29167 gives more information on such functionality for RFID tags. This specification provides a mechanism to ensure the integrity and authenticity of the data carrier data and an irrefutable link of the data carrier data with the unique data carrier identifier. As such, alterations or insertion of false data into data carriers are detectable. It also provides a means to detect tampered data carrier data stored and communicated within systems. It does not provide any means to defend against replay attacks. As a counter the data carrier reader can use this specification to sign the read data, effectively providing integrity and authenticity to the read-transaction. A third party can then verify that the read-transaction happened at a given place and time, as well as verify the data read from the carrier. Likewise, the signed data carrier data can contain data describing unique features and security marks of the item establishing a verifiable link between the data carrier data and the physical item.

© ISO/IEC 2022 – All rights reserved

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

1 Scope

This document is an ISO/IEC 9594-8 [public key infrastructure (PKI) digital signatures and certificates] application specification for automated identification services. It specifies a method whereby data stored within a barcode and/or RFID tag are structured, encoded and digitally signed. ISO/IEC 9594-8 is used to provide a standard method for key and data description management and distribution. The data capacity and/or data transfer capacity of automated identification data carriers are restricted. This restricts the normal use of a digital signature as specified in ISO/IEC 9594-8 within automated identification services.

The purpose of this document is to provide an open and interoperable method, between automated identification services and data carriers, to read data, verify data originality and data integrity in an offline use case.

This document specifies

— the meta data structure, the DigSig, which contains the digital signature and encoded structured data,

— the public key certificate parameter and extension use, the DigSig certificate, which contains the certified associated public key, the structured data description, the read methods, and private containers,

— the method to specify, read, describe, sign, verify, encode, and decode the structured data, the DigSig Data Description,

— the DigSig EncoderGenerator which generates the relevant asymmetric key pairs, keeps the private key secret, and generates the DigSigs, and

— the DigSig DecoderVerifier which, by using to the DigSig certificate, reads the DigSig from the set of data carriers, verifies the DigSig and extracts the structured data from the DigSig.

This document does not specify

— cryptographic methods, or

— key management methods.

2 Normative references

The following documents are referred to in the text in such a way that some or all their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 8601 (all parts), *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/IEC 8824-1[1)], *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

1) ITU-T X.680 is equivalent to ISO/IEC 8824-1.

© ISO/IEC 2022 – All rights reserved

ISO/IEC 9594-1[2], *Information technology — Open Systems Interconnection — The Directory — Part 1: Overview of concepts, models and services*

ISO/IEC 9594-8[3], *Information technology — Open Systems Interconnection —The Directory — Part 8: Public-key and attribute certificate frameworks*

ISO/IEC/IEEE 9945, *Information technology — Portable Operating System Interface (POSIX®) Base Specifications, Issue 7*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*

IETF RFC 5646[4], *Tags for Identifying Languages*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
authenticity
quality or condition of being authentic, trustworthy, or genuine

3.2
base64url
Base64 encoding with the URL and Filename Safe Alphabet

Note 1 to entry: See IETF RFC 4648.

3.3
CIDSnip
continuous binary sequence starting with the DAID and CID encoded field values

Note 1 to entry: See 8.3.2.

3.4
DataSnip
continuous binary or text sequence of encoded field values

Note 1 to entry: See 8.3.2.

3.5
digital certificate
certificate
data construct that contains the public key, integrity parameters and use parameters of the DigSig

Note 1 to entry: The data construct shall be as specified in ISO/IEC 9594-8.

2) ITU X.500 is equivalent to ISO/IEC 9594-1, and is the commonly used reference for standard and terminology.

3) ITU X.509 is equivalent to ISO/IEC 9594-8, and is the commonly used reference for standard and terminology.

4) IEFT RFC 5646 is the reference specification of the IETF BCP 47.

© ISO/IEC 2022 – All rights reserved

3.6
digital signature
signature
result of an asymmetric encryption method on a data construct

Note 1 to entry: The asymmetric encryption method and data construct shall be as specified in ISO/IEC 9594-8.

Note 2 to entry: In typical legal terminology, this term is the equivalent of an advanced electronic signature.

3.7
DigSig
data construct assembled according to this document which contains verifiable information obtained from one or more AIDC

3.8
DigSig envelope
envelope
data construct assembled according to this document by the EncoderGenerator

3.9
Domain Authority
entity, operating as a trusted third party, responsible for the digital signature integrity of a jurisdiction

3.10
integrity
reliability of data that are as they were created according to the required verification parameters

3.11
jurisdiction
independent domain of control in terms of the business or legal (or both) scope of the parties concerned

Note 1 to entry: Examples are independent countries, separate ministries or departments of a government, or independent companies each with their own legal or business (or both) framework.

3.12
nibble
four-bit aggregation

3.13
pragma
field directive

Note 1 to entry: See Clause 9.

3.14
Private key
key that is kept in secret and is used to generate a digital signature by encrypting data that will be verified by its associated public key

3.15
Public key
key that is publicly available and is used to verify data that were encrypted by its associated private key

3.16
Snip
continuous binary or text sequence

Note 1 to entry: See 8.3.2.

© ISO/IEC 2022 – All rights reserved

3.17
UTF-8
8 bit variable-width encoding as specified by ISO/IEC 10646 of the Unicode Graphic code points

Note 1 to entry: See ISO/IEC 10646.

3.18
WORD
media physical memory grouping of bits

4 Field and data definitions, abbreviated terms, symbols, and binary data

4.1 Field and data definitions

Field and data objects are defined in Clause 8 and 8.10.3.

4.2 Abbreviated terms

AFI	Application Family Identifier
AIDC	Automatic Identification data capture
BRE	Basic Regular Expression
CA	Certification Authority
CID	DigSig certificate ID
DA	Domain Authority
DAID	Domain Authority identifier
DDD	DigSig Data Description
DI	Data Identifier (see ISO/IEC 15434)
DigSig IA	DigSig Issuing Authority
ERE	Extended Regular Expressions
ID	Identification number
IoT	Internet of Things
JSON	Data description construct (see ISO/IEC 21778)
MSB	Most significant bit
OID	Object identifier as specified in ISO/IEC 8824-1
PKI	Public key infrastructure
RFID	Radio-frequency identification
UID	Unique ID
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time

© ISO/IEC 2022 – All rights reserved