International Standard

ISO/IEC 20248

Second edition
2022-06

AMENDMENT 1
2024-10

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

AMENDMENT 1: Domain authority identifier (DAID) specification for the GS1 legal entity identifier and encoding clarifications

Reference number
ISO/IEC 20248:2022/Amd. 1:2024(en)

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

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 document 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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

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.

Clause 2, Normative references

Add the reference:

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

AMENDMENT 1: Domain authority identifier (DAID) specification for the GS1 legal entity identifier and encoding clarifications

GS1 General Specifications Standard

7.5.3

Replace the entire subclause with:

7.5.3 DAID for GS1 legal entity(ies)

GS1 General Specifications Standard shall be used to specify the GS1 Party Global Location Number (PGLN), corresponding to GS1 Application Identifier (417), as the GS1 identifier for legal entity(ies).

The DAID shall be "GS1 <PGLN>". The PGLN is a 13-character base 10 (digits 0 to 9) number.

The DAID for GS1 shall be encoded as follows:

— DAID encoding type identifier: 0xFE.

— PGLN encoding: 44-bit binary number.

EXAMPLE The PGLN 9506000151540 is the DAID "GS1 9506000151540" encoded as ":FE:8A549C323F4".

8.2.3

Delete the second bullet: "Empty fields and arrays shall be pruned."

Replace the forth bullet

Base64 shall be in the format when encoded from the binary; it shall contain the padding characters.

with:

The binary value presentations shall be as follows: bstring uses HexString, digsigenv uses Base64String and privatecontainer uses HexString.

8.10.2

Replace the third paragraph

The language tag shall be constructed in accordance with IETF RFC 5646. The use of ISO 639-1, 2-character language tag is compulsory. The IETF RFC 5646 sub-tags are optional.

with:

The language tag shall be constructed in accordance with IETF RFC 5646. The language subtag is compulsory. The other sub-tags are optional.

B.4.6, fourth paragraph

Add the following sentence at the end of the paragraph:

The following example FP256BNwithSHA256 implementation steps was created using the MIRACL Core: Apache License, Version 2.0 library dated 2020 (https://github.com/miracl/core -snapshot date: 2023-12-08).

B.4.6, a)

Replace the Extracted SigData with:

```
["ISO/IEC 20248:2022","https://www.dept-edu.com","QC DGSG",110,"2024-02-11T12:02:01","John
Doe","612209498902",["2021","2022","2023"],"Bachelors in Administration","Business
School","2024-03-04",[["Structures 101","degree","B"],["Accounting
112","degree","A"],["Statistics 159","extra","A"]]]
```

B.4.6, b)

Replace the generated signature with:

```
0x03FAA57BE23549FE02E584B9F14CAEFE2BD5404A8D4165A3CCB5427262D2566AE2
```

Replace the compressed signature with:

```
0xFAA57BE23549FE02E584B9F14CAEFE2BD5404A8D4165A3CCB5427262D2566AE2
```

Replace the encoded the DDDdata after adding the signature with:

```
0xC098099640006EC96C081A129BDA1B8811BBD9621B0DA130B1B432B637B9399034B71020B236B4B734B9BA39
30BA34B7B75E84EAE6D2DCCAE6E640A6C6DCDEDED96BBBBBB9730B1319730B1973D30B3245729BA393AB1BA3AB
932B9901898188DC82C6C6DEEADCE8D2DCCE406262641729BA30BA34B9BA34B1B990189A9CC0
```

Replace the URI Envelope with:

```
https://www.dept-edu.com/verify?wJgJlkAAbslsCBoSm9obiBEb2WIbDaEwsbQytje5OZA0txAgsja0tzS5uj
kwujS3t16E6ubS3Mrm5kCmxtDe3tlru7u5cwsTGXMLGXPTCzJFcpujk6sbo6uTK5kBiYGI3ILGxt7q3OjS3M5AYmJk
Fym6MLo0ubo0sbmQGJqcwA
```

B.4.6, c)

Replace the Extracted SigData with:

```
["ISO/IEC 20248:2022","https://www.dept-edu.com","QC DGSG",110,"2024-02-11T12:02:01","John
Doe","612209498902",["2021","2022","2023"],"Bachelors in Administration","Business
School","2024-03-04",[["Structures 101","degree","B"],["Accounting
112","degree","A"],["Statistics 159","extra","A"]]]
```

Replace the extracted signature with:

```
0xFAA57BE23549FE02E584B9F14CAEFE2BD5404A8D4165A3CCB5427262D2566AE2
```