INTERNATIONAL STANDARD

**ISO/IEC 20248**

First edition
2018-03

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

*Technologies de l'information — Techniques d'identification automatique et de capture de données — Structures de données — Méta-structure de signature numérique*



Reference number
ISO/IEC 20248:2018(E)



ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.



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

# Introduction

This document specifies a “language” which is used to specify data constructs with; how the data constructs can be read from one or more AIDC; and how to decode and verify such data.

This document is an ISO/IEC 9594-8 (Public Key Infrastructure: digital signatures and certificates) application specification for automated identification services. Data capacity and/or data transfer capacity of Automated Identification Data Carriers are limited. This restricts the normal use of a digital signature as specified in ISO/IEC 9594-8 within automated identification services.

This document specifies an effective and interoperable method to specify, read, decode and verify data stored in automated identification data carriers, 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 automated identification data carriers.



The user of this document may use any suitable hashing and asymmetric cryptography method. The choice of cryptography method should be considered carefully and it is advised that only internationally recognized or standardized methods, for example FIPS PUB 186-4 and IEEE P1363, be used.



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

NOTE Many transport applications rely on a secure non-transferable unique identifier to ensure that the data are bound to the tag and/or the vehicle. For such functionality, please refer to ISO/IEC 29167. This specification provides a mechanism to ensure the integrity and authenticity of the data themselves in order to protect against alterations or insertion of false data into the system. It does not provide any means to defend against replay attacks. Including the secure non-transferable unique identifier of a tag, as signed data, allows for the unrefutable link between the tag and the data and provides a means to determine if the data were read from the tag. The reader can place the read DigSig in another DigSig, effectively signing the read transaction. A third party can then verify that the read transaction happened at a given place and time, as well as the data read.

 

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

## 1 Scope

This document is an ISO/IEC 9594-8 (Public Key Infrastructure: 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. It is worth noting that 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.

A successful verification of the DigSig signifies the following:

— 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 identifier of the data carrier is included in the DigSig it contains, then the data stored on the data carrier can be considered as the original issued copy of the data; the secure identifier will be able to guarantee that the data carrier is authentic.

This document does not specify

— cryptographic methods, nor

— key management methods.

This document is used in conjunction with standard risk assessments of the use environment.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of 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/IEC 8824-1[1)], *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

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 9899, *Information technology — Programming languages — C*

ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*

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

IETF 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 following terms and definitions apply.



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

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

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

**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**
singular continuous bit or text stream portion of a Data Carrier transmission which contains the CID as the first part

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

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.

**3.4**
**Data Carrier**
device used to store data as a relay mechanism in an AIDC system

EXAMPLE Barcodes, RFID tags and even human memory.

**3.5**
**Data Carrier construct rule**
process to prepare the DigSig Envelope for encoding in a particular Data Carrier

**3.6**
**DataSnip**
singular continuous bit or text stream portion of a Data Carrier transmission containing data for DDD fields

**3.7**
**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.

**3.8**
**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.



**3.9**
**DigSig**
data construct assembled according to this document which contains verifiable information obtained from one or more AIDC

**3.10**
**DigSig Envelope**
**envelope**
data construct assembled according to this document by the EncoderGenerator

**3.11**
**Domain Authority**
entity, operating as a trusted third party, responsible for the Digital Signature integrity of a jurisdiction

**3.12**
**integrity**
reliability of data that are as they were created according to the required verification parameters

**3.13**
**jurisdiction**
independent domain of control in terms of the business or legal (or both) scope of the parties concerned

EXAMPLE Independent countries, separate ministries or departments of a government, or independent companies each with their own legal or business (or both) framework.

**3.14**
**nibble**
four-bit aggregation

**3.15**
**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

**3.16**
**protocol**
communication specification

**3.17**
**Public Key**
key that is publicly available and is used to verify data that were encrypted by its associated Private Key

**3.18**
**Snip**
singular continuous bit or text stream portion of a Data Carrier transmission

**3.19**
**Time Zone**
time zone code

Note 1 to entry: See ISO 8601.

**3.20**
**UTF-64**
64 bit variable-width encoding

Note 1 to entry: See ISO 10646.



**3.21**
**WORD**
media physical memory grouping of bits



# 4 Field and data definitions, abbreviations and symbols

## 4.1 Field and data definitions

Field and data objects are defined in Clause 8.

## 4.2 Abbreviations

| | |
|---|---|
| AFI | Application Family Identifier |
| AIDC | Automatic Identification Data Carrier |
| AutoID | Automated Identification |
| BRE | Basic Regular Expressions |
| 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 |
| X.509 | ISO/IEC 9594-8 |



## 4.3 Symbols



| | |
|---|---|
| \|\| | concatenate or join |
| … | repeat the previous, as required |
| {…} | parameters that form one structure/grouping |
| [x] | x is optional. |
| <x> | x is compulsory. |
| **Bold** | a tag to be used as is |
| x \|= y | y is a description of x. |
| x ⇐ y | x takes the value of y. |
| # x | x is a comment until the end of the line. |
| F(x,y) | the function F that takes as input two parameters, x and y, to produce an output |
| xx:..xx | depicts an hexadecimal string “0” to “9” and “A” to “F” |
| $XXX_2$ | “XXX” is binary. |

# 5 Conformance

## 5.1 Specification version

The specification version is used by data structures defined in this document. Other systems use the specification version to identify the data structures of this document and to determine the version of the specification.

The specification version shall be set as follows:

**specificationversionvalue** ⇐ "ISO/IEC 20248:yyyy" with "yyyy" the year of publication of this document.

## 5.2 Claiming conformance

In order to claim conformance, a service shall comply with the requirements of this document.

AIDC conformance standards, as specified in Annex K, Annex L and Annex M, shall apply.

## 5.3 Test authority

The tests shall be performed by a software test authority using a norm application or by code inspection. The norm application used in this test shall be independent from the person who requests the test.

## 5.4 Test specification



The test specification specifies the conformance test methods for this document.

The full test methods in Annex A shall be applied.



The test specification is independent of:

— cryptography conformance and performance;

— AutoID Data Carrier conformance and performance.

The following components shall be tested:

— DigSig Certificate format;

— DigSig Data;

— DigSig DecoderVerifier;

— DigSig DecoderGenerator.

# 6 DigSig use architecture

## 6.1 General

This document specifies a DigSig EncoderGenerator and a DigSig DecoderVerifier system component. The DigSig EncoderGenerator is typically an application dedicated implementation and the DigSig DecoderVerifier an application independent implementation.

A DigSig is a structured set of AIDC data. A DigSig may be stored over more than one AIDC device of different types. A DigSig is cryptographically verifiable. The DigSig data structure, read method and cryptographic functions are specified by a Domain Authority (DA) published in a DigSig Certificate (an X.509 method). The DigSig Certificate is cryptographically verifiable as certified by an X.509 Certification Authority. Each DigSig Certificate has a unique identifier (Clause 7) called the Certificate

 

Identifier (CID). The {DA, CID} is unique and contained in every DigSig as the first data of the DigSig. A reader of a DigSig uses the {DA, CID} of the specific DigSig to reference the relevant DigSig Certificate, from which the reader acquires the read methods, data structure specification and cryptographic functions to read the full DigSig, decode the DigSig and verify the DigSig.

The DigSig EncoderGenerator is used to generate a DigSig, on request from a Data Carrier programming application. The DigSig EncoderGenerator does not include the method to create or program a Data Carrier. See Annex D for a typical DigSig EncoderGenerator use architecture.

The DigSig DecoderVerifier is used by a local application to instruct a Data Carrier reader/interrogator how to read the DigSig from a set of Data Carriers and other sources in order to decode and verify the data. See Annex E typical DigSig DecoderVerifier use architecture.

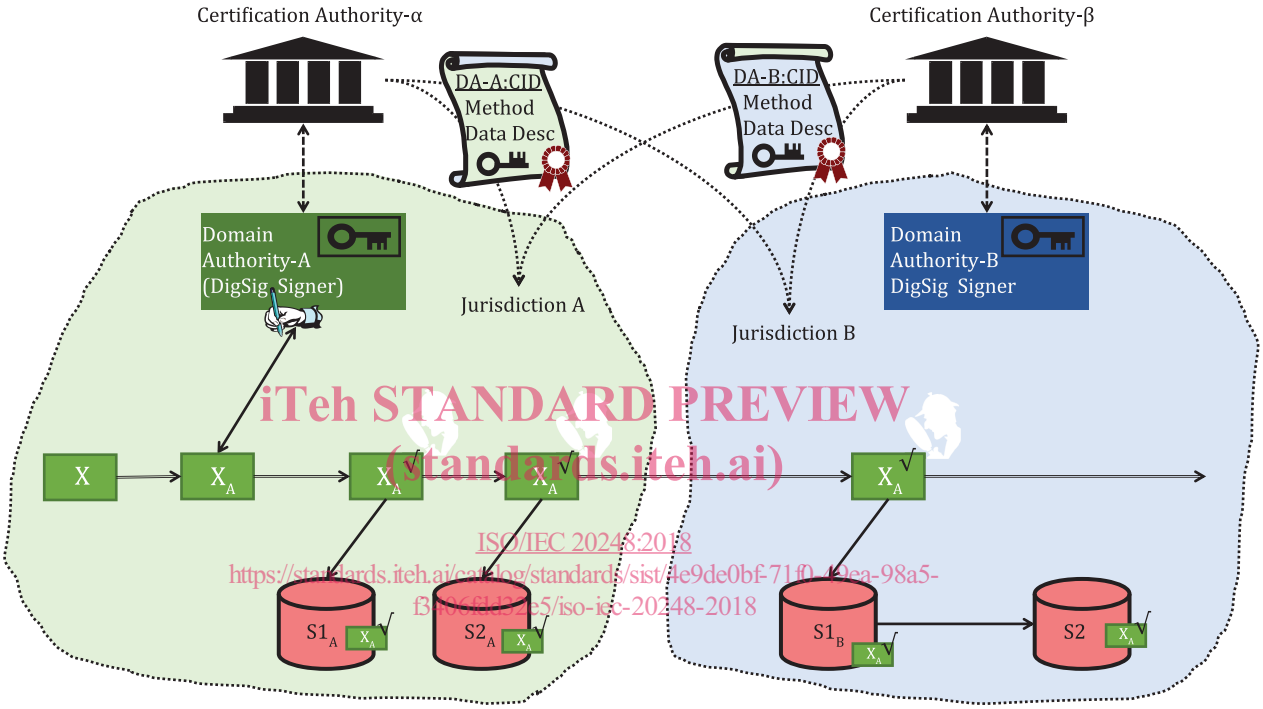




**Figure 1 — DigSig use architecture**

The general method and properties of ISO/IEC 20248 are illustrated in Figure 1. With reference to Figure 1:

a) Domain Authority A (DA-A) provides DigSig issuing services for Jurisdiction A. Similarly, Domain Authority B (DA-B) provides DigSig issuing services for Jurisdiction B. “Issuing” entails the validation of the data for a DigSig, the validation of the DigSig requestor's credentials, and the generation of the DigSig. The DigSig requestor may be a human and/or an application.

b) The DigSig Certificates issued by DA-A, each containing a DigSig Data Description (DDD) as applicable to Jurisdiction A applications/services, are certified by the Certification Authority α (CA-α) for a specific signing and certificate validity period in accordance with a Certification Practice Statement as specified in X.509. Similarly, Certification Authority β certifies DigSig Certificates issued by DA-B. Certification Authorities α and β may be the same entity.

c) The DigSig Certificates are published in a manner to allow systems $S1_A$, $S2_A$, $S1_B$, $S2_B$... to acquire them in advance or on demand. The DigSig Certificates are used by the systems to read, decode and verify DigSigs generated and stored on Data Carriers by the Domain Authorities; for example:

   Data X is used by DA-A to generate a DigSigN $X_A$ as specified by a DigSig Certificate N.

   The systems of both jurisdictions use the DigSig Certificates to read, decode, verify and use the data without the need to connect to any other system.

AIDC data fulfil an important role in IoT by providing physical objects a digital identity and optional attributes. Annex C provides more information on DigSig use in IoT.

Annex G provides more information on Digital Signature use.

## 6.2 DigSig Certificate process

Figure 2 describes the process that shall be followed to issue a DigSig Certificate in accordance with X.509.

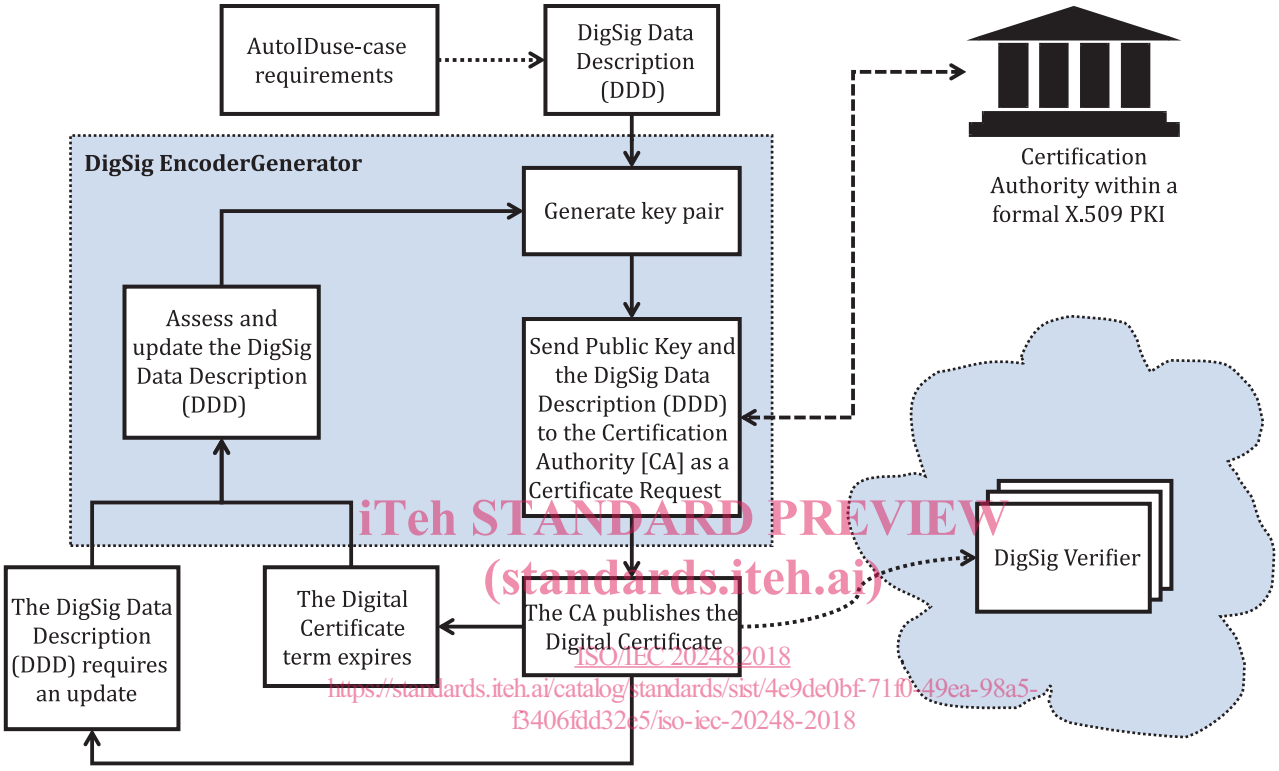




**Figure 2 — DigSig Certificate process**

Figure 3 illustrates how data structure changes can be achieved seamlessly by allowing DigSig Certificates — and therefore the data structure validity — to overlap.

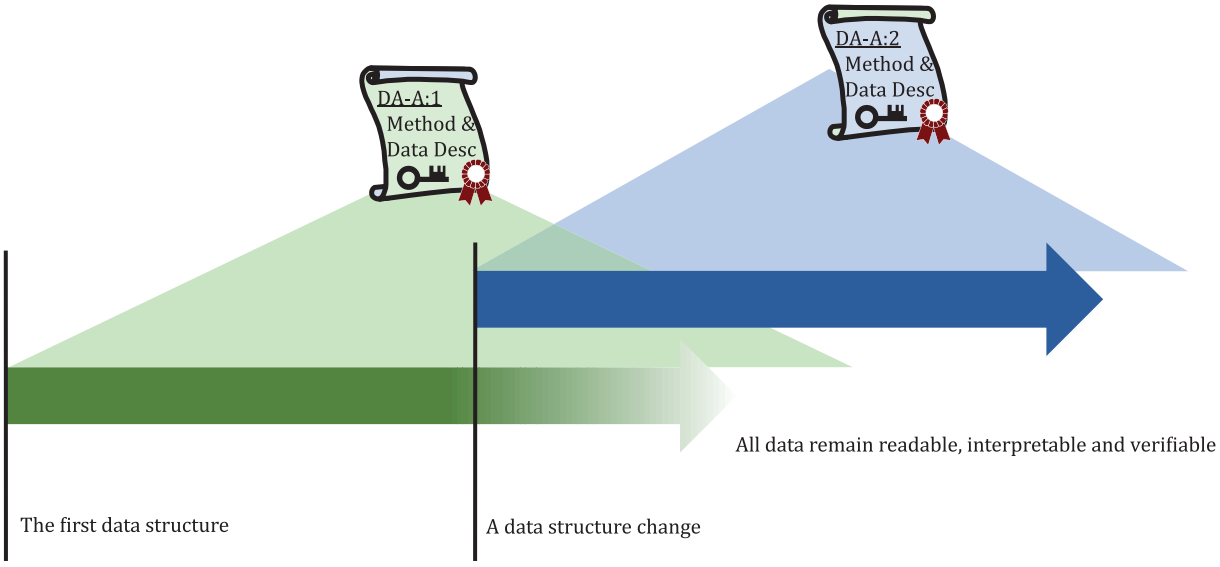


**Figure 3 — DigSig data structure rollover**

### 6.3 DigSig generation process

The DigSig is generated by the DigSig EncoderGenerator.

a) The applicable CID referenced DigSig Certificate shall be used to generate SigData from DDDdata.

b) SigData shall be digitally signed using the DigSig Certificate specified Digital Signature algorithm resulting in Signature and Timestamp.

c) The **signature** and **timestamp** DDDdata fields shall be assigned the values Signature and Timestamp.

d) The required DigSig shall be generated from DDDdata.

### 6.4 DigSig verification process

The DigSig verification shall be performed by a DigSig DecoderVerifier application. The application has the ability to read the Data Carriers as required by its primary function in its use case. It has also the ability to obtain the referenced DigSig Certificate.

The steps to verify a DigSig shall be as follows:

a) Read the DigSig Envelope;

b) Extract the {DA, CID} from the DigSig Envelope. The DA is determined from the DAID. It may be derived from the URI Envelope encoding;



Use the {DA, CID} DigSig Certificate after it was verified to:

c) Read the remainder of the DigSig using the **readmethod pragma**;



d) Decode the DigSig and prepared DDDdata and SigData;

e) Perform the verification on SigData.

### 6.5 Error codes

The DigSig error codes shall be in accordance with Annex F.

## 7 DigSig Certificate

### 7.1 General

The DigSig Certificate consists of a X.509 version 3 certificate with the DDD included in a X.509 version 3 extension.

DigSig Certificate |= <X.509V3 certificate> || <DDD in a X.509V3 extension>

NOTE 1 A non-hierarchical certification path is valid when the same DigSig is used by more than one DA.

NOTE 2 The desired CA might not be familiar with the specific requirements of this document as these differ from the standard requirements of X.509. In this case, an intermediate CA, a DigSig Issuing Authority (DigSig IA), can be included in the PKI, with a singular function of validating the DigSig extension. The desired CA can incorporate the DigSig IA or be the parent of the DigSig IA. X.509 recommends the inclusion of the DigSig IA function into the respective Certification Practice Statement.

### 7.2 ISO/IEC 20248 Object Identifier

The ISO/IEC 20248 OID shall take the value: ISO.standard.“the number of this standard”; this results in the OID: “1.0.20248”.