BS ISO/IEC 20248:2018

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20248:2018

National foreword

This British Standard is the UK implementation of ISO/IEC 20248:2018.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 89419 0

ICS 35.040.50

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20248:2018

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)

Documents
Document Sharing Hub
© ISO/IEC 2018

Full document details: BS ISO/IEC 20248:2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20248:2018

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **2**

3 Terms and definitions ... **2**

4 Field and data definitions, abbreviations and symbols ... **4**
4.1 Field and data definitions ... 4
4.2 Abbreviations ... 4
4.3 Symbols ... 5

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

6 DigSig use architecture ... **6**
6.1 General ... 6
6.2 DigSig Certificate process ... 7
6.3 DigSig generation process ... 8
6.4 DigSig verification process ... 9
6.5 Error codes ... 9

7 DigSig Certificate ... **9**
7.1 General ... 9
7.2 ISO/IEC 20248 Object Identifier ... 9
7.3 DigSig Certificate parameter use ... 9
7.4 DigSig cryptography ... 10
7.4.1 General ... 10
7.4.2 Digital Signatures ... 10
7.4.3 Private containers ... 10
7.5 DigSig Domain Authority identifier ... 10
7.6 DigSig Certificate identifier (CID) ... 12
7.7 DigSig validity ... 12
7.8 DigSig Certificate management ... 12
7.9 DigSig revocation ... 12
7.10 Online verification ... 13

8 DigSig Data Description (DDD) ... **13**
8.1 General ... 13
8.2 DDD derived data structures ... 14
8.2.1 General ... 14
8.2.2 DDDdata ... 14
8.2.3 SigData ... 15
8.2.4 DDDdataTagged ... 15
8.2.5 DDDdataDisplay ... 15
8.3 DigSig format ... 16
8.3.1 General ... 16
8.3.2 Snips ... 16
8.3.3 Envelope format ... 17
8.3.4 AIDC specific construction of a DigSig ... 17
8.4 The DigSig physical data path ... 18
8.5 DDD syntax ... 20
8.6 DigSig information fields ... 20
8.7 Data fields ... 21

© ISO/IEC 2018 – All rights reserved

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 20248:2018

8.7.1 Compulsory data fields ... 21
8.7.2 Application data fields ... 21
8.8 Data field object syntax ... 22
8.9 DDD field types and associate settings ... 23
8.9.1 General ... 23
8.9.2 Special field values ... 23
8.9.3 Field types ... 24
8.9.4 Special types ... 29

9 Pragmas ... 29
9.1 General ... 29
9.2 entertext ... 29
9.3 structjoin ... 30
9.4 readmethod ... 31
9.5 privatecontainer ... 32
9.6 startonword ... 33
9.7 cidsniptext ... 33

Annex A (normative) **Test methods ... 34**

Annex B (informative) **Example DigSigs ... 37**

Annex C (informative) **DigSig use in IoT ... 43**

Annex D (informative) **Typical DigSig EncoderGenerator device architecture ... 46**

Annex E (informative) **Typical DigSig DecoderVerifier device architecture ... 48**

Annex F (normative) **DigSig error codes ... 50**

Annex G (informative) **Digital Signature use considerations ... 52**

Annex H (informative) **Example of a DigSig Certificate ... 53**

Annex I (informative) **Example DDD for a physical certificate ... 54**

Annex J (normative) **DigSig revocation specifications ... 60**

Annex K (normative) **2D bar code symbologies — Encoding and decoding the DigSig ... 62**

Annex L (normative) **ISO/IEC 18000-3 Mode 1 RFID protocol and DigSigs ... 70**

Annex M (normative) **ISO/IEC 18000-63 RFID protocol and DigSigs ... 75**

Bibliography ... 80

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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*.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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.

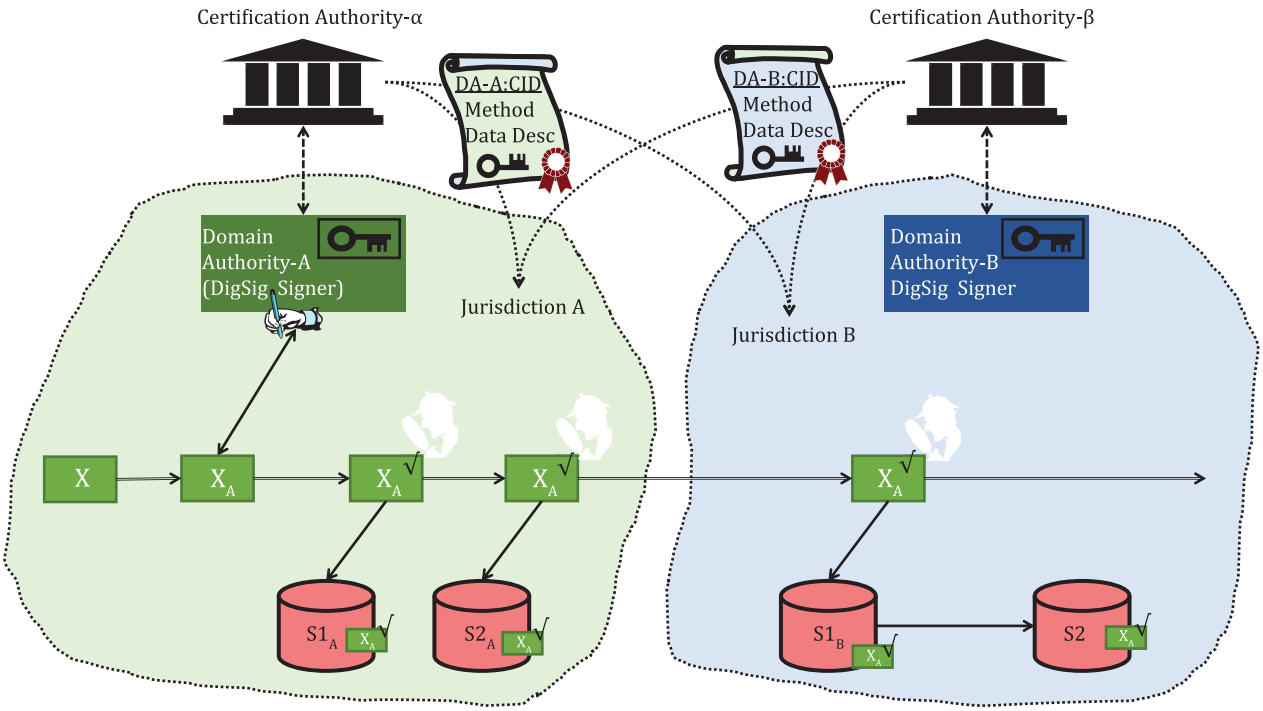

Figure 1 — DigSig use architecture

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.

© ISO/IEC 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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.

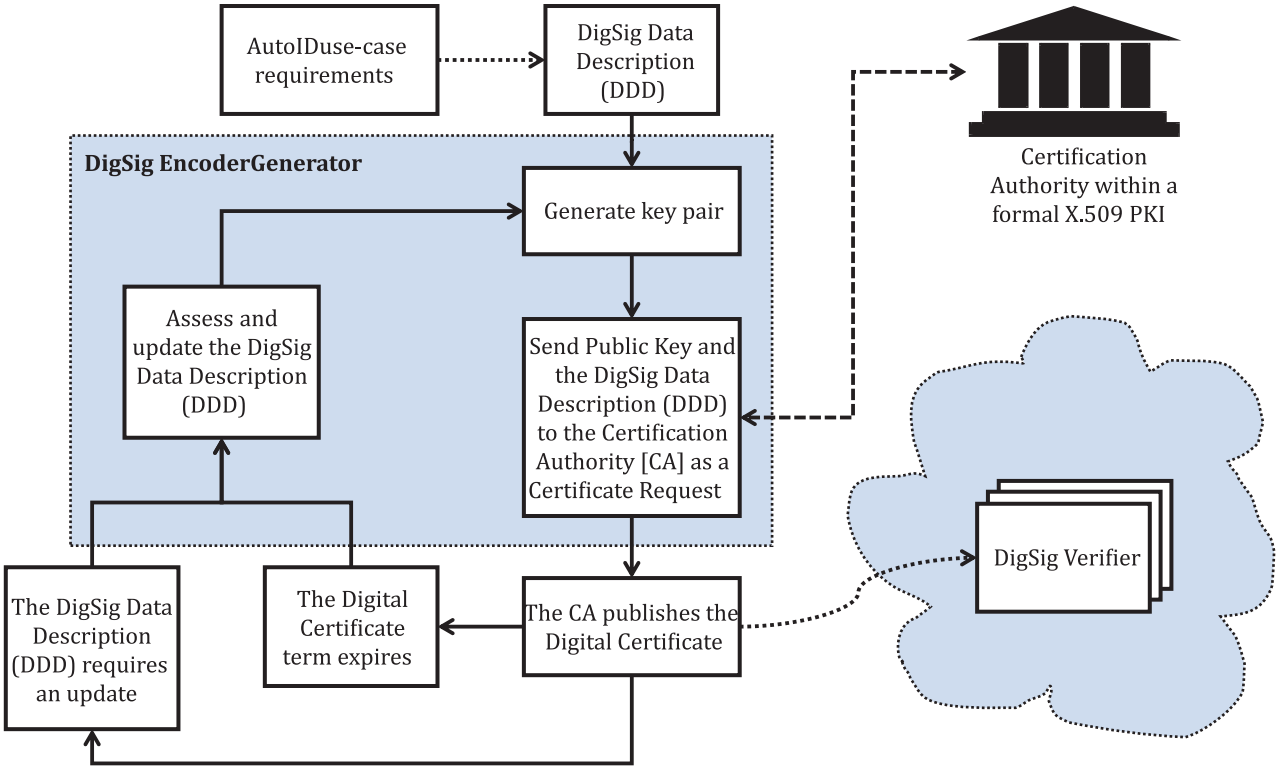

Figure 2 — DigSig Certificate process

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

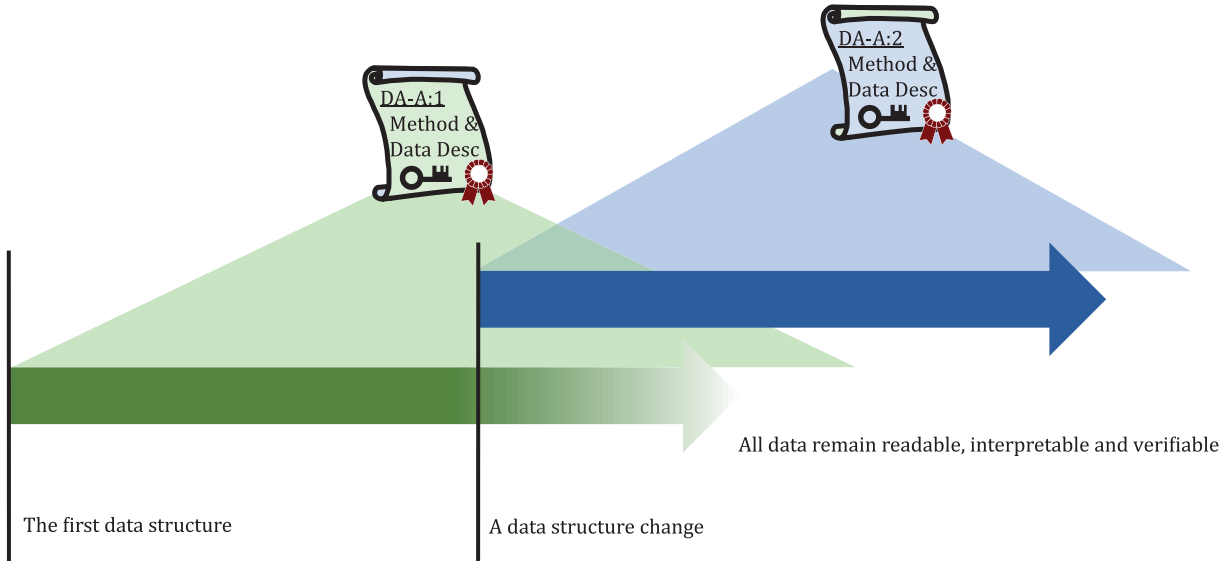

Figure 3 — DigSig data structure rollover

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

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”.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

The object identifier format to be used in X.509 shall be as specified in ISO/IEC 8824-1.

7.3 DigSig Certificate parameter use

The X.509 version 3 parameters (in X.509 specification notation) shall be used as follows:

```
certificateContent::= SEQUENCE {
   version                  set to the value 2 indicating certificate version 3
   serialNumber             set in accordance with X.509
   signature                set in accordance with X.509
   issuer                   set in accordance with X.509
   validity                 set in accordance with X.509 and 7.7
   subject                  {DA, CID} using distinguished names as specified in
                            ISO/IEC 9594-1 and this clause.
   subjectPublicKeyInfo     set in accordance with X.509
   issuerUniqueIdentifier   set in accordance with X.509
   Extensions::= SEQUENCE {
      extnId                ISO/IEC 20248 OID
      critical              shall have the value "non-critical"
      extnValue             DDD; see Clause 8
   }
}
```

EXAMPLE 1 See Annex H.

The common name of the subject shall have the following format:

CN = <DA URI> || "/cid/" || <CID>

EXAMPLE 2 “CN = https://DomainAuthority.com/cid/12345”

NOTE A DigSig aware digital certificate validator processes the extension and accepts or rejects the DigSig Certificate depending on the content of the DigSig Certificate, the extension and the conditions under which processing occurs (e.g. the current values of the path-processing variables).

7.4 DigSig cryptography

7.4.1 General

This document specifies the use of two types of cryptography:

— for the Digital Signatures;

— for the private containers.

This document does NOT specify the specific cryptographic algorithms, key or hash lengths. Only recognized cryptographic methods shall be used.

NOTE The choice of cryptography is closely linked to the use case risk profile, the size of memory available on the Data Carriers to be used, the time available to read/interrogate the Data Carrier reliably, the scope of the application services (i.e. open vs close loop) and the desired validity period of the DigSig.

7.4.2 Digital Signatures

The Digital Signature cryptography methods (i.e. asymmetric encryption, key length and hash algorithm) shall be specified within the DigSig Certificate in compliance with X.509.

7.4.3 Private containers

The private container cryptography shall be specified by the **privatecontainer pragma** in 9.5.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

7.5 DigSig Domain Authority identifier

The DigSig Domain Authority identifier shall be uniquely constructed in the following manner:

DAID |= <IAC> || " " || <CIN> (see ISO/IEC 15459-2).

An ISO/IEC 20248 Domain Authority shall be registered with a Company Identifying Number (CIN).

a) The Domain Authority identifier (DAID) shall be encoded from the ISO/IEC 15459-2 Issuing Agency Code (IAC) and CIN as specified in Table 1.

Table 1 — Domain Authority identifier bit encoding

IAC indicator	CIN indicator	IAC code	CIN code
1 bit	2 bits	5 or 13 bits	24 or 32 bits

b) The rules in Table 2 shall be used to assign a unique identifier to each IAC:

Table 2 — ISO/IEC 15459-2 IAC encoding

IAC indicator	IAC range	IAC code	Encoding bits
0_2	0-9	0-9	5
0_2	A-J	10-19	5
1_2	LA-UZ	20-279	13
1_2	KAA-KZZ	280-955	13
1_2	VAA-ZZZ	956-4335	13

The numerical code is converted to binary with the necessary leading zeros.

c) The rules in Table 3 shall be used to calculate a unique identifier for each CIN:

Table 3 — ISO/IEC 15459-2 CIN encoding

CIN indicator	CIN type	CIN length	Encoding bits
00_2	Numeric	1-7 digits	24 bits
01_2	Numeric	8-9 digits	32 bits
10_2	Alphanumeric	1-4 char.	24 bits
11_2	Alphanumeric	5-6 char.	32 bits

1) Numeric CIN: The numeric value is used as is.

2) Alphanumeric CIN: Base 36 conversion from the CIN to a numeric value:

   i) "0" to "9" takes the character values 0 to 9.

   ii) "A" to "Z" takes the character values 10 to 35.

   iii) Leading spaces takes the character value 0.

$A_n \ldots A_2 A_1 A_0 \Leftarrow A_n{*}36^n \ldots + A_2{*}36^2 \ldots + A_1{*}36 \ldots + A_0$

NOTE ISO/IEC 15459-3 specifies that a CIN is limited to capital letters and numerals; see the Invariant Character Set of ISO/IEC 646.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

EXAMPLE

15459–2 Example IAC CIN	IAC indicator	CIN indicator	IAC Code	CIN Code	DAID calculated from IAC || CIN Example
C ZZZZ	0_2	10_2	01100_2	19:A0:FF	4C:19:A0:FF
B 999999999	0_2	01_2	01011_2	3B:9A:C9:FF	2B:3B:9A:C9:FF
QC ZZZZ	1_2	10_2	0000010011000_2	19:A0:FF	C0:98:19:A0:FF
QC ZZZZZZ	1_2	11_2	0000010011000_2	81:BF:0F:FF	E0:98:81:BF:0F:FF
UN 999999999	1_2	01_2	0000100001011_2	3B:9A:C9:FF	A1:0B:3B:9A:C9:FF

7.6 DigSig Certificate identifier (CID)

The CID is a 16 bit unsigned integer reference number to a DigSig Certificate. The Domain Authority manages the CID and its associated DigSig Certificate.

The tuple {DA, CID} shall be unique within its validity lifespan.

The CID values 0 and 1 are reserved for revocation, see Annex J.

7.7 DigSig validity

The Time Zone of the validity period shall be UTC.

DigSigs are issued within an issuing period. DigSigs are typically valid for a much longer period: the DigSig validity period. The validity period of the DigSig Certificate shall be at least as long as the sum of the issuing period and the DigSig validity period.

From a security and risk analysis viewpoint, X.509 allows periodic re-issuing of a new certificate to extend a certificate validity period.

EXAMPLE A re-issue period is discussed in the following use-case:

A university selects a one year issuing period; they generate a new key pair annually and publish a new DigSig Certificate with a new CID annually.

The university determines that the risk profile indicates that the DigSig Certificate should be valid for 10 years. They therefore issue the DigSig Certificate with a validity period of 10+1 years (to include the issuing period).

University certificates need to be verifiable for many years. The university therefore re-issues the DigSig Certificate, with the same CID, DDD and key pairs, every decade. Both the DigSig and the current DigSig Certificate remain therefore verifiable.

NOTE Encryption strength is measured in the brute-force attack duration. The DigSig lifespan is limited by this duration. Re-issuing of the DigSig with new key pairs extends the lifespan of a DigSig.

7.8 DigSig Certificate management

DigSig Certificate management and DigSig Certificate revocation shall comply with ISO/IEC 9594-1.

The revocation of a DigSig Certificate shall also revoke all DigSigs issued with it. The DigSigs need not be individually revoked.

7.9 DigSig revocation

The revocation of DigSigs is a recommended service typically performed by a Trust Service (see Annex E).

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

The Domain Authority of a DigSig shall be the authority of the revocation of the DigSig.

The DigSig revocation shall be as provided in Annex J.

NOTE A chain of trusted Digital Signatures can be compromised in several possible ways (e.g. exposure of a private key, innovations in the mathematics of hashing algorithms, or availability of greater computing power). Any implementation of this document which does not implement revocation services for Digital Signatures assumes some risk of wrongly trusting a Digital Signature.

7.10 Online verification

Online verification, using commonly available browsers, may be performed by submitting the URI Envelope (see 8.3.3.3) to a Trust Service (see Annex E).

The Trust Service shall perform the **entertext pragma** (see 9.2) through its user interface.

The Trust Service uses App services to perform the **readmethod pragmas**.

NOTE The primary goal of this document is to provide an offline method, whereby a Data Carrier reader/interrogator reads, decodes and verifies Data Carrier data in an open and interoperable manner. The data read passed on to another application, as in IoT, remain verifiable.

8 DigSig Data Description (DDD)

8.1 General

The DDD is a hierarchical specification of the data fields contained or directly associated with an item; the DDD data. The DDD data are structured, signed, verified, encoded, decoded, stored and read from Data Carriers as specified by the associated DDD. The encoded form of the DDD data are called a DigSig.

AutoID Data Carriers data storage and data transfer is limited. This limitation should be considered when developing the DDD.

The DDD is a JSON construct. It has the following format:

DDD |= {<digsiginfo> || <datafields>}

digsiginfo |= an object with management definition fields.

datafields |= an array of compulsory and application definition fields.

The DDD is a tree structure. The leaves are the DDD data containers and the branches are the structuring of the containers.

Figure 4 illustrates the use of a DDD.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

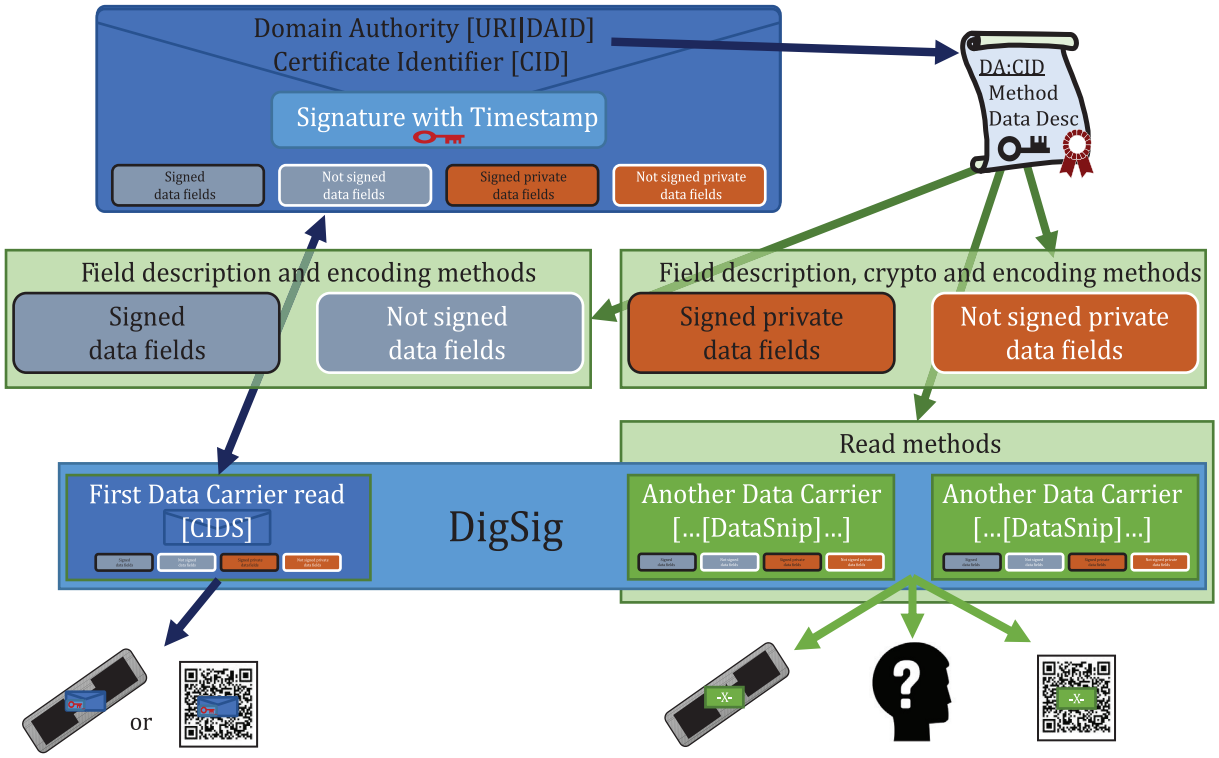

Figure 4 — Use of a DigSig Data Description (DDD)

8.2 DDD derived data structures

8.2.1 General

DDD derived data structures are JSON constructs.

DDD derived data structures shall follow the DDD syntax as specified in 8.5.

The specified field order and hierarchy shall be maintained between a DDD and all its derived data structures.

EXAMPLE For DDD, see I.3.

8.2.2 DDDdata

DDDdata shall only contain the values of the DDD leaf fields called the field values.

DDDdata shall be a JSON array of arrays following the structure of the DDD **datafields**.

DDDdata of a **struct** shall be contained in a JSON array.

DDDdata shall NOT contain JSON objects.

A field value shall be:

a) When cardinality is NOT specified for the field: a JSON string, number, true, false or null;

b) When cardinality is specified for the field: a JSON array of strings, numbers, trues, falses or nulls.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

The values Signature and Timestamp of DDDdata^{input} shall be ignored.

NOTE DDDdata are used as an input and output structure: see in Figure 4 and 8.3.4. The values Signature and Timestamp are generated by the DigSig EncoderGenerator; the input values of Signature and Timestamp are ignored.

EXAMPLE For DDDdata^{input}, see I.5. For DDDdata, see I.6.

8.2.3 SigData

SigData shall be a subset of DDDdata.

SigData shall only contain the data fields specified to be signed and verified.

SigData shall be generated by deleting all field values of which the field descriptor **bsign** equals false. Empty branches shall be pruned.

SigData shall NOT contain white spaces or any other formatting.

EXAMPLE See I.7.

8.2.4 DDDdataTagged

DDDdataTagged shall be a JSON object whereby each array and field value of DDDdata is tagged with its **fieldid** value as set in the DDD to become a JSON pair.

EXAMPLE 1 This example is abbreviated for readability purposes.

DDD: {"fieldid":"id-A", "fieldid":"id-B", {"fieldid":"id-C", "cardinality":"{2}"},

{“ fieldid":"id-D","fields":{"fieldid":"id-D^1","fieldid":"id-D^2"}}}

DDDdata: [val-A, val-B, [val-C^1, val-C^2], [val-D^1, val-D^2]]

DDDdataTagged: {id-A:val-A, id-B:val-B, id-C:[val-C^1, val-C^2], id-D:{id-D^1:val-D^1, id-D^2:val-D^2}}

EXAMPLE 2 See I.8.

8.2.5 DDDdataDisplay

DDDdataDisplay is used to display DDDdata in the desired language and Time Zone. DDDdataDisplay shall only contain information for display purposes. All other information shall be purged.

DDDdataDisplay ⇐ GenerateDDDdataDisplay(DDD, DDDdata, Language Code, Time Zone)

DDDdata shall be generated by:

a) Adding the DDDdata field values as JSON pairs to the DDD fields in the format as specified by the DDD. The value pair shall have the format:

“displayvalue”: <field value formatted for display - JSON string >

b) Changing all **displayStrings** to singular strings; for example:

```
"postverify":
   {"en":"For more information contact the Department of Education.",
    "af":"Vir meer inligting kontak die Department van Opleiding."
   }
```

Based on the selection of “af” the value of “postverify” becomes:

```
"postverify":"Vir meer inligting kontak die Department van Opleiding."
```

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

c) Changing all **date**s to the selected Time Zone and display format.

d) Purging all field members excluding: **fieldname, description** and **displayvalue**.

e) If a field member does not contain a **fieldname** pair, the **fieldid** shall be used for display purposes.

EXAMPLE See I.9.

8.3 DigSig format

8.3.1 General

See Figure 4. The encoded form of the DDD data is called a DigSig. A DigSig may be stored over more than one Data Carrier. It contains fields which are signed or not signed and open or private.

The DigSig Envelope is the encapsulation of the {DA, CID} and the data fields as specified to be stored on the Data Carrier containing the {DA, CID}.encoded format of the DDDdata. The DigSig Envelope is the first part of the DigSig read.

{DA, CID} references the DigSig Certificate, which contains the DDD, which in turn defines methods to read, decode and verify data of the DigSig.

NOTE Human memory is also a Data Carrier. Data are provided from human memory as a TEXT Snip.

8.3.2 Snips

8.3.2.1 Snip types

A Snip is a singular continues part of a Data Carrier memory as specified by the DDD. It contains one or more fields.

The following Snips shall be used:

a) CIDSnip: The CIDSnip is the head, the first Snip, of the DigSig. It shall contain the DAID, CID and all data fields without a **readmethod pragma**.

b) DataSnips: The additional Snips as specified by the DDD **readmethod pragma**. Each **readmethod** shall map to a DataSnip.

The DataSnips shall be in the order of reference in the DDD.

NOTE Data Carrier typically will provide a CIDSnip in an automated manner; for example when reading a barcode, the content of the barcode will be the CIDSnip as a singular read. In contrast, inventory of an ISO/IEC 18000-63 will only provide the UII. It is possible for the UII to contain the complete DigSig, though it is expected that the TID and some user memory can also be read. In the latter case, the TID and user memory are provided as separate DataSnips.

8.3.2.2 Snip encoding

A CIDSnip shall be encoded in BINARY. A DataSnip shall be encoded as either BINARY or TEXT:

a) BINARY encoding shall be packed as a bit stream with the most significant bit first in network byte order.

b) TEXT encoding shall be UTF.

The following shall apply to padding a Snip:

— The head of a Snip shall NOT be padded.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

— The tail of a Snip may be padded.

EXAMPLE See I.4.

8.3.3 Envelope format

8.3.3.1 General

The Envelope specification contains fields specified in 8.5.

8.3.3.2 RAW Envelope

A Raw Envelope is the CIDSnip.

8.3.3.3 URI Envelope

The URI Envelope shall be the CIDSnip encoded in Base64url preceded with a URI in accordance with IETF RFC 3986. The URI Envelope shall have the following format:

URI Envelope |= <verificationuri> || "?" || Base64url_encoding(CIDSnip) [|| "~" <cidsniptextvalue>]...

The **cidsniptextvalue** shall be in the order of reference in the DDD; see 9.7.

NOTE The URI Envelope is useful for online verification where a Data Carrier is read using a hand-held device with generic Data Carrier readers; e.g. a smart phone with a barcode and/or RFID reader.

8.3.4 AIDC specific construction of a DigSig

Each Snip of a DigSig shall be specifically constructed for insertion into the desired Data Carrier allowing the DigSig to be read correctly from such Data Carrier.

This international standard defines a process, as depicted in Figure 5, for encoding a DigSig in data carriers. Rules are explicitly specified for:

— 2 D barcodes (see Annex K for details), specifically:

  — Aztec Code, as defined in ISO/IEC 24778;

  — DataMatrix, as defined in ISO/IEC 16022;

  — MicroPDF417, as defined in ISO/IEC 24728;

  — PDF417, as defined in ISO/IEC 15438;

  — QR Code, as defined in ISO/IEC 18004.

— RFID tags to these protocols:

  — ISO/IEC 18000-3 Mode 1, operating at 13.56MHz (see Annex L for details);

  — ISO/IEC 18000-63, operating at 860 MHz to 960 MHz (see Annex M for details).

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

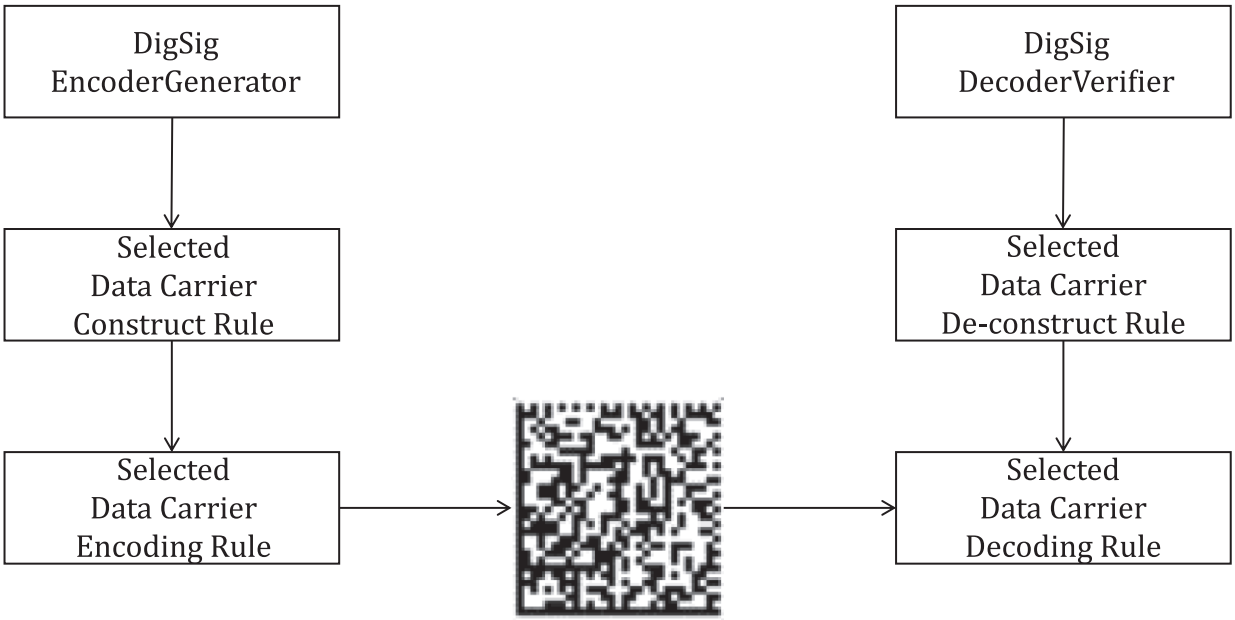

Figure 5 — Encoding and decoding a DigSig in AIDC data carriers

The data carrier construct rule addresses the following features.

— The data carriers need to declare that the encoding complies with the International Standard. There are different ways of doing this in RFID and bar code data carrier.

— The Domain Authority and CID need to be processed in a manner specific to the data carrier. For example, these are encoded in different memory areas in the different RFID protocols, while all the 2D symbols share common features.

— RFID tags support selective locking.

— ISO/IEC 18000-63 supports addressable partitioned memory and these memory areas may require the DigSig to be distributed between these memory areas.

— The 2D symbologies support error correction, sometimes with a choice of correction level.

— The 2D symbologies require print parameters to be defined, including defining the format of the symbol.

A similar inverse process is required to de-construct the data carrier. Additionally, the DigSig DecoderVerifier may call for additional processes to be carried out based on the content of the data carrier, e.g. to use the unique chip id in an RFID tag.

8.4 The DigSig physical data path

The physical data path of a DigSig is depicted in Figure 6.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

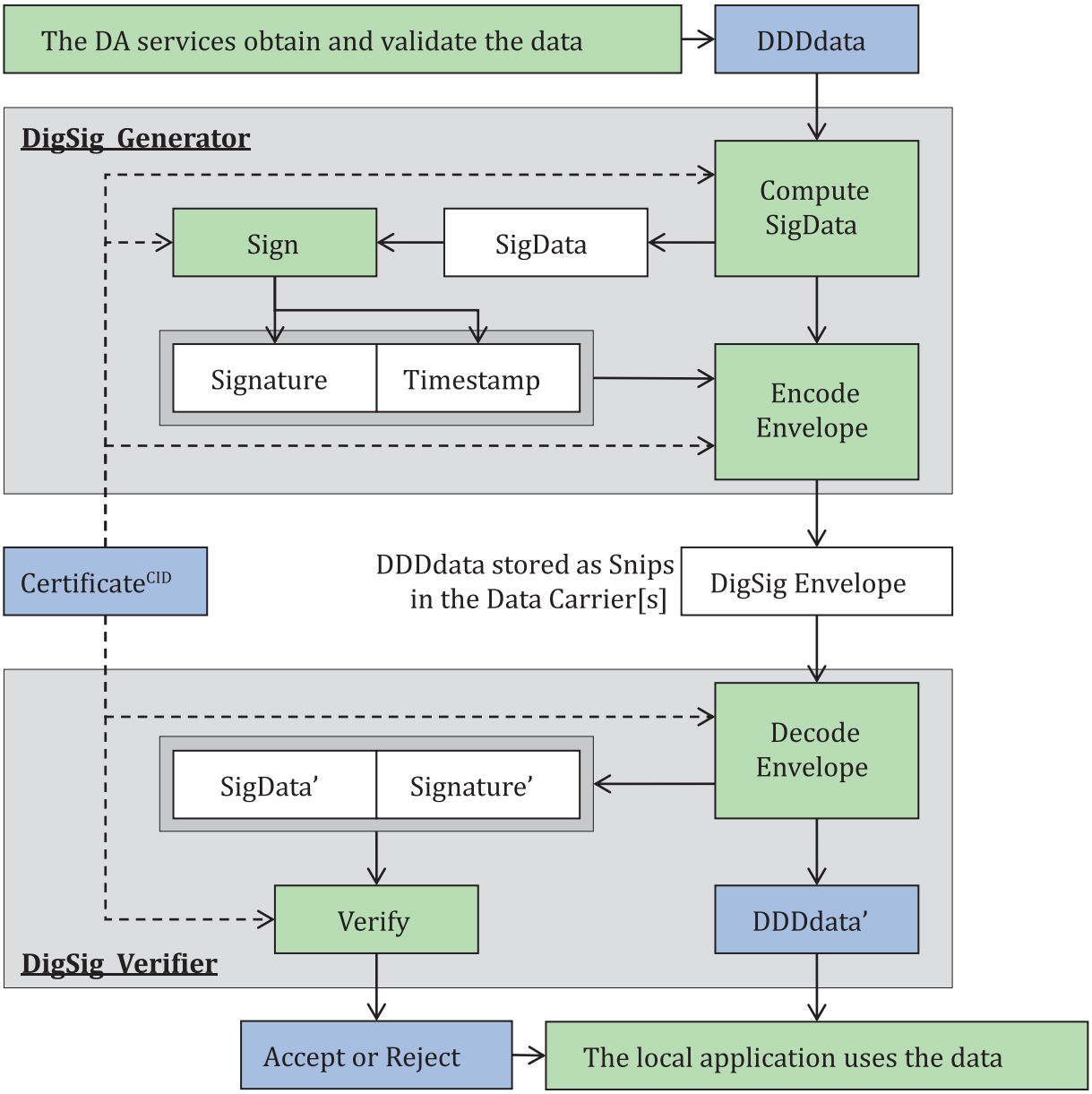

Figure 6 — Physical data path

a) $DDDdata^{input} \Leftarrow LocalApplicationGenerateDDDdata(Certificate^{CID}, ApplicationData)$

b) $SigData \Leftarrow ExtractSigData(Certificate^{CID}, DDDdata^{input})$

c) $\{Signature, Timestamp\} \Leftarrow Sign(Certificate^{CID}, SigData)$

d) $DigSig \Leftarrow EncodeDigSig(Certificate^{CID}, DDDdata^{input}, \{Signature, Timestamp\})$

e) $Programmed\ Data\ Carrier... \Leftarrow WriteDigSig(DigSig)$

f) $\{CID', DigSig'\} \Leftarrow ReadDigSig(Data\ Carrier...)$

g) $\{DDDdata', SigData', Signature'\} \Leftarrow DecodeDigSigCertificate^{CID'}, DigSig')$

h) $VerificationOutcome \Leftarrow Verify(Certificate^{CID'}, SigData', Signature'\}$

i) $ApplicationData \Leftarrow TranslateFromLocalApplication(Certificate^{CID'}, DDDdata', VerificationOutcome)$

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018

8.5 DDD syntax

The DDD shall have the following syntax:

```
{"digsiginfo":
  {"specificationversion":<specificationversionValue>,
   "dauri":<dauri>,
   "daid":<DAID>,
   "cid":<CID>,
   "verificationuri":<verification URI>,
   "revocationuri":<revocation URI>,
   "preverify":<display string before verification>,
   "acceptverify":<display string on verification accept>,
   "rejectverify":<display string on verification reject>,
   "postverify":<display string after verification>,
   "structureddocuri":<structured document URI>,
   "custom":<JSON member with custom DDD information>
   },
  "datafields":
   [{"fieldid":"specificationversion",    # Shall be the first field description
     "type":"string",
     "bsign":true
    },
    {"fieldid":"dauri",                   # Shall be the second field description
     "type":"string",
     "bsign":true
    },
    {"fieldid":"daid",                    # Shall be the third field description
     "bsign":true
    },
    {"fieldid":"cid",                     # Shall be the fourth field description
     "type":"unsignedint",
     "bsign":true
    },
    {"fieldid":"signature",               # This field may be placed elsewhere
     "type":"bstring",                    # Fixed length as per DigSig Certificate
     "bsign":false
    },
    {"fieldid":"timestamp",               # This field may be placed elsewhere
     "type":"date",                       # The Time Zone shall be UTC
     "binaryformat":<dateformat>,         # The default is tepoch
     "bsign":true
    },
    …                                     # Optional application fields
   ]
}
```

specificationversion, **dauri**, **cid**, **signature** and **timestamp** are compulsory **datafields**. The compulsory fields shall only use the field descriptors with its specified value as specified in this clause. The field descriptors may be omitted from the DDD.

8.6 DigSig information fields

The DigSig information fields describe the use environment of the DigSig and DDD.

digsiginfo is a JSON object. It shall contain only the fields specified in Table 4. These fields shall not contain DDDdata values.

Table 4 — digsiginfo fields

Name	Purpose and value	Type	Inclusion
specificationversion	Set according to 5.1.	JSON string	compulsory
dauri	The Domain Authority URI for reference purposes.	JSON string	compulsory
daid	The Domain Authority identifier.	JSON string	compulsory

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 20248:2018