Technical Specification

ISO/IEC TS 23220-2

First edition
2024-11

Cards and security devices for personal identification — Building blocks for identity management via mobile devices —

Part 2: Data objects and encoding rules for generic eID systems

Cartes et dispositifs de sécurité pour l’identification des personnes — Blocs fonctionnels pour la gestion des identités via les dispositifs mobiles —

Partie 2: Objets de données et règles d'encodage pour les systèmes eID génériques

Reference number
ISO/IEC TS 23220-2:2024(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

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.

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 17, *Cards and security devices for personal identification*.

A list of all parts in the ISO/IEC 23220 series can be found on the ISO and IEC websites.

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.

Introduction

Electronic ID-Applications (eID-Apps) are today commonly used in badges and ID cards with integrated circuits and allow users to complete electronic identification, authentication, or optionally, to create digital signatures. Many different application areas have an essential need for these mechanisms and use different means to provide these features (e.g. health system with health assurance cards or health professional cards, financial sector with payment cards, governmental ID with national ID cards, electronic passports or driver's licenses, educational systems with student cards or library cards, in the company sector with employee cards and in the private sector with any kind of member cards).

Mobile devices (e.g. mobile phones or smart phones, wearable devices) are a central part of the daily life for many individuals. They are not only used for communication, but also for emailing, access to social media, gaming, shopping, banking, and storing of private content such as photos, videos and music. They are used today as a personal device for business and private applications. With the ubiquity of mobile devices in day-to-day activities there is a strong demand from users to have eID-Apps or services with identification/ authentication mechanisms on their mobile equipment, i.e. an mdoc app.

An mdoc app can be deployed to provide a number of different digital ID-documents. Additionally, it can reside among other eID-Apps on a mobile device. Moreover, users can possess more than one mobile device holding an mdoc app, which leads to enhanced mechanisms for the management of credentials and attributes.

The technical preconditions for the deployment of mdoc apps exist and they are partly standardized to support security and privacy on a mobile device. Examples for containers of eID-App solutions are the software-based Trusted Execution Environment (TEE), hardware-based secure elements such as universal integrated circuit card (UICC), embedded or integrated UICC (eUICC or iUICC), embedded secure elements, secure memory cards with cryptographic module or other dedicated internal security devices residing on the mobile device, as well as solutions with server-based security means.

As mdoc apps can be located on different forms of mobile devices featuring different security means, being as generic as possible helps them to be adoptable to different variants of trusted eID-Management. This diversity leads also to different levels of security, trust and assurance. Trusted eID-Management thereby implies the (remote) administration and use of one or several security elements (e.g. in form of an intelligent network), credentials and user attributes with different levels of security suitable to their capability and power.

Access to the mdoc app by the external world is performed by the available transmission channels. Typical local communication channels are Bluetooth Low Energy (BLE), Near Field Communication (NFC) and Wi-Fi aware, whereas remote communication is typically an internet connection over mobile networks and Wi-Fi networks. The way of identification and choice of the transmission interface and protocols is an essential part for a trusted eID-Management.

Those mdoc apps are used in different areas of daily life and are the focus of different standardization activities. This document aims at delivering mechanisms and protocols usable by other standards to provide interoperability and interchangeability. With these basics in mind, future mdoc apps can be derived and extend the ISO/IEC 23220 series.

The ISO/IEC 23220 series builds upon existing standards comprising four main subjects:

a) secure channel establishment;

b) API call serialization method;

c) data element naming convention; and

d) payload transport over communication channel protocols, which are constitutive of the interoperability pillars.

In addition, it adds means to establish Trust on First Use (TOFU).

NOTE The ISO/IEC 23220 series inherits and enhances the functionality that was adopted by mobile driving licence (mDL) applications whereby ensuring backward compatibility with ISO/IEC 18013-5.

Cards and security devices for personal identification — Building blocks for identity management via mobile devices —

Part 2: Data objects and encoding rules for generic eID systems

1 Scope

This document specifies data objects and encoding rules of generic eID-Systems in terms of building blocks for mobile document system infrastructures, and standardizes generic data models for data exchanges between mdoc apps and verification applications.

This document is applicable to entities involved in specifying, architecting, designing, testing, maintaining, administering, and operating a mobile eID-System in parts or as a whole.

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 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

ISO 3166-2, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*

ISO/IEC 5218, *Information technology — Codes for the representation of human sexes*

ISO/IEC 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 10646, *Information technology — Universal coded character set (UCS)*

ISO/IEC 18013-2:2020, *Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 18013-5:2021, *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application*

ISO/IEC 19785-3, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-4, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5, *Information technology — Biometric data interchange formats — Part 5: Finger image data*

ISO/IEC 39794-4, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*

ISO/IEC 39794-5, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*

RFC 4648, *The Base16, Base32, and Base64 Data Encodings, October 2006*

RFC 7165, *Use Cases and Requirements for JSON Object Signing and Encryption (JOSE)*

RFC 7515, *JSON Web Signature*

RFC 8949, *Concise Binary Object Representation (CBOR)*

ITU-T E.123, *Notation for national and international telephone numbers, e-mail addresses and web addresses*

ITU-T E.164, *The international public telecommunication numbering plan*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
alphabetic character
A
hexadecimal ranges '41' – '5A' (Latin capital letters), '61' – '7A' (Latin small letters), 'C0' – 'D6', 'D8' – 'F6' and 'F8' – 'FF' of ISO/IEC 8859-1

3.2
boolean
logical values, TRUE and FALSE

3.3
byte string
bstr
sequence of bytes

3.4
label
identifier that is attached to a data element

3.5
numeric character
N
hexadecimal range '30' – '39' (digits 0 to 9) of ISO/IEC 8859-1

3.6
special character
S
hexadecimal ranges '20' – '2F' (<space> ! “ # $ % & ‘ ( ) * + , - . /), '3A' (:), '3C' – '40' (< = > ? @), '5B' – '60' ([\]^_`),'7B'–'7E'({|}~),'A1'–'AC'(¡¢£¤¥¦§¨©a«¬),'AE'–'A5'(®¯°±2 3´µ), and'A7'–'BF'(·¸ 1 ° » 1/4 1/2 3/4 ¿) of ISO/IEC 8859-1

3.7
text string
tstr
string of characters

3.8
unsigned integer
uint
binary value of a number of consecutive bits

4 Symbols and abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

BCD	Binary Coded Decimal
CBEFF	Common Biometric Exchange Formats Framework
CBOR	Concise Binary Object Representation
CDDL	Concise Data Definition Language
eID	electronic IDentification
F	Fixed length
JSON	JavaScript Object Notation
JWS	JSON Web Signature
mDL	mobile driving license
mdoc	mobile document
URI	Uniform Resource Identifier
V	Variable length

5 General

ID documents are issued by binding an applicant with a real-life identity. An issuer collects evidence to verify the attributes provided by the applicant, and this process is called identity proofing. An applicant provides his or her attributes in specific application form. In such an application form, character formats of each data element are taken into account in order to avoid a mismatch with the ID document format. The issuer of the ID document verifies the attributes provided by the applicant with evidence and confirms the value of each attribute. ID documents issued by authoritative organisations are usually used as evidence.

Figure 1 illustrates an example of the issuing process of an eID document. An applicant provides an application form and evidence (e.g. ID cards issued by Authority) to the issuer. The issuer collects other evidence if needed and proves his or her identity and binds his or her identity with the holder and confirms the applicant by photo ID or by person of authority. As a result, his or her eID card is issued as "something you have", optionally together with "something you are (e.g. portrait)" and "something you know (e.g. password)", as defined in ISO/IEC TS 23220-5[1].

[1] Under preparation. Stage at the time of publication: ISO/IEC CD TS 23220-5

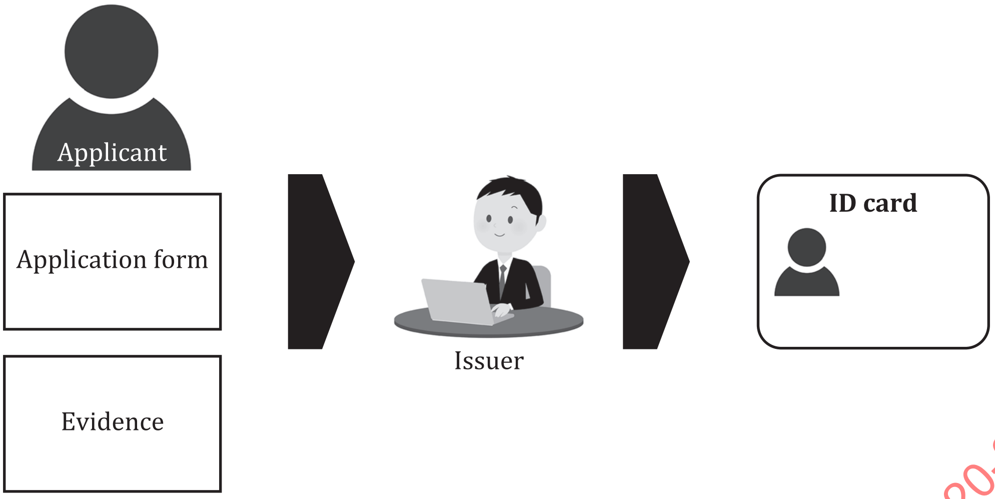

Figure 1 — Identity data collection and confirmation of its values

According to digitalisation of the issuing process, attributes used for application form and evidence are described as digital data. The specification of data elements and encoding rules for application form can be identical to that of Mobile eID. In case eID card or Mobile eID is used as evidence, a set of data elements and encoding rule is not always identical to Mobile eID. Character format, type and length are not always identical, and are out of scope of this document because they are specified by the issuer.

Figure 2 describes an example which shows a difference of attribute name between application form evidence and Mobile eID. Attributes for "Date of birth" and "Place of birth" are expressed by different attribute names in a different entity. The attribute "Date of birth" is expressed as "birth_date" in ISO/IEC 18013-5, whereas it is expressed as "birthdate" in OpenID connect standard claims.

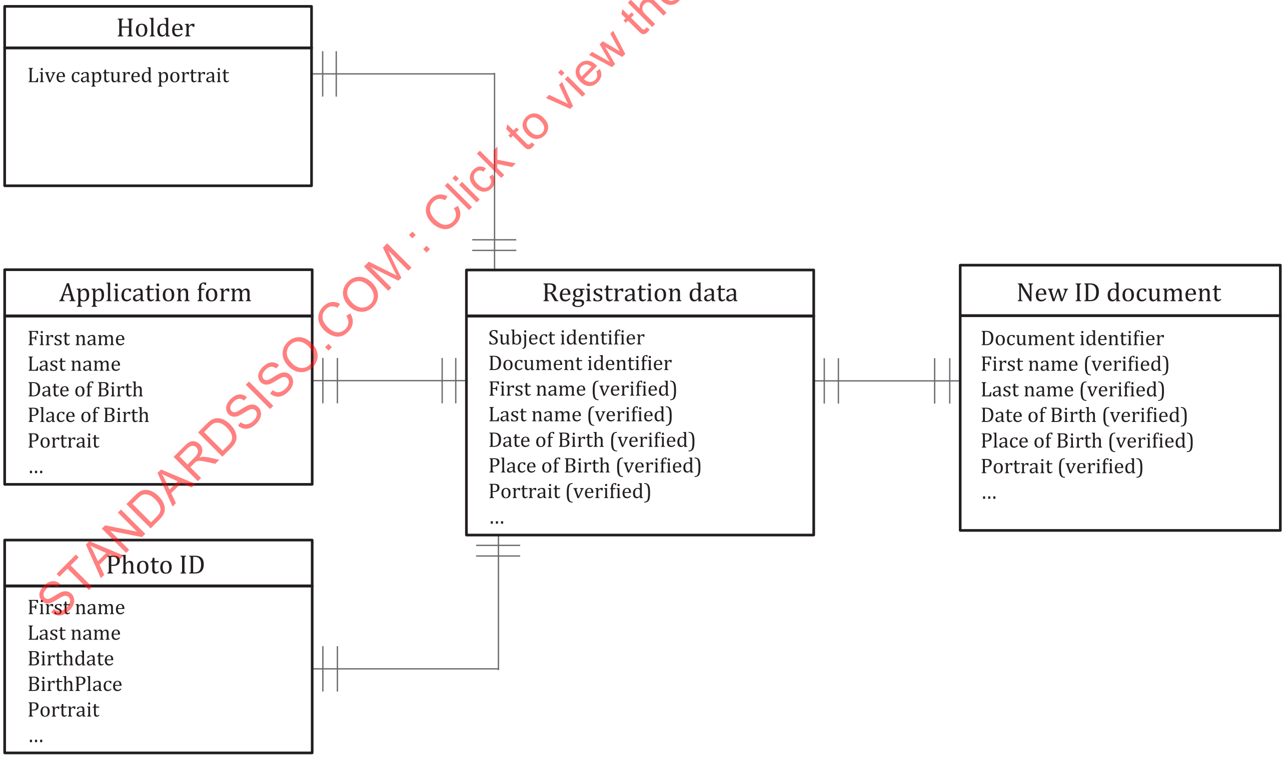

Figure 2 — Comparison of attribute names (example)

In this document, meta attributes are defined to clarify the same attributes with different identifiers to be used as a reference, supporting comparison and re-use of attribute name between two standards of eID data elements.

This document also specifies the requirement of ISO/IEC TS 23220-3[2] and ISO/IEC TS 23220-4[3] data elements as a generic extension of ISO/IEC 18013-5 specified for mDL. The data model for each ID document is specified by issuing authority and out of scope of this document.

6 Data model

6.1 General

Issuing authority should select data element identifiers from this document for interoperability if applicable. It makes it difficult for authorities to change such a specification because it sometimes requires an amendment of regulations. It results in a difference of document format, vocabulary and encoding rule.

In general, content of an eID document consists of four kinds of entities: person, document, issuer and proof. Each entity has attributes which are used to identify an instance of entity. Regardless of vocabulary, some attributes are commonly used for identifying an instance of entity. In this document, such attributes are defined as "meta-attribute".

Figure 3 shows an example of a basic data model and how an instance of an entity is identified by values for a set of attributes. In this document, such attributes are defined as personal attributes.

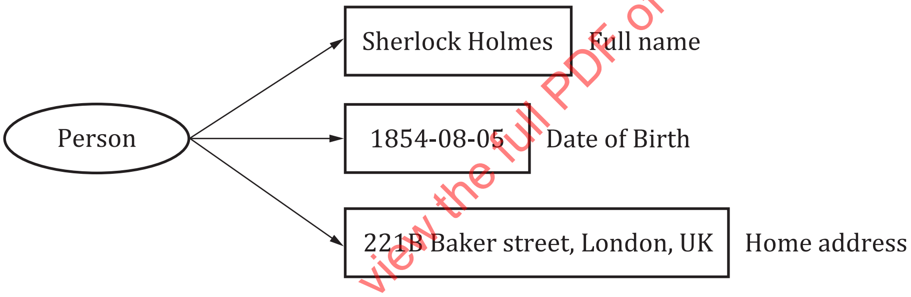

Figure 3 — Example of basic data model for identifying a person

Relationships with other persons (e.g. parental authority, proxy) can also be expressed with attributes. In this document, Figure 4 shows a relation between entity and attribute.

[2] Under preparation. Stage at the time of publication: ISO/IEC CD TS 23220-3.

[3] Under preparation. Stage at the time of publication: ISO/IEC CD TS 23220-4.

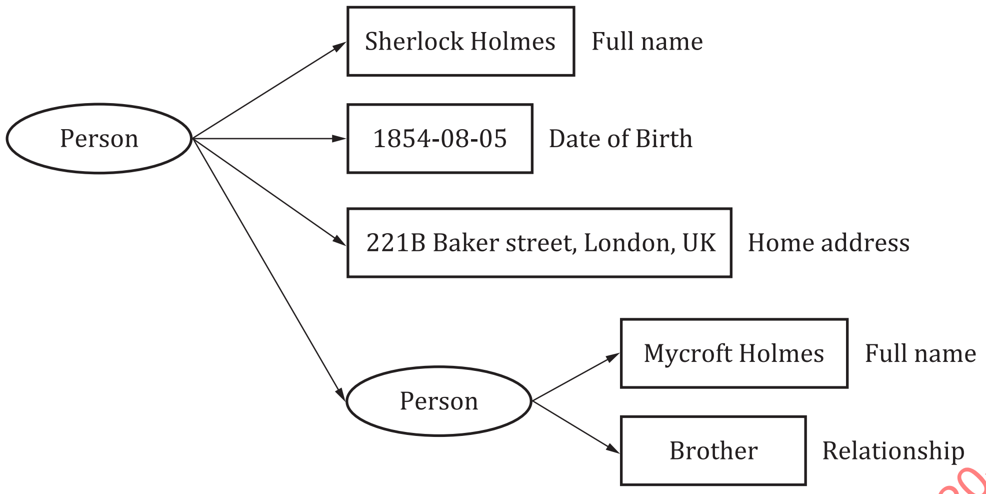

Figure 4 — Example of data model including relationship attribute

In eID documents, such attributes are described as data elements. In this subclause, this document specifies a set of data elements to identify a person.

6.2 Data format and encoding rules

6.2.1 Identifier

The “Identifier” is assigned to identify a data element. The value of “Identifier” can be a tag, an address (URI), a name, an identifier or else according to the definition language employed. The value type can be also determined by the definition language employed.

6.2.2 Field format

The field format of data elements is specified with:

- flexibility of length (F/V);
- integer denoting a length of the field;
- character format [alphabetic character (A), numeric character (N) and special character (S)].

EXAMPLE V150AS indicates Variable length, maximum 150 characters with alphabetical characters and special characters.

6.2.3 Encoding

The following encoding types are used for each data element:

- text string (tstr)
- byte string (bstr)
- uint
- tdate
- boolean (true/false)
- full-date

Text string shall be encoded by unicode as specified in ISO/IEC 10646. If binary data is encoded as text string, Base64URL encoding as specified in RFC 4648 shall be used. There are no length restrictions for the encoding of the elements, unless otherwise indicated.

Data elements shall be encoded and serialised according to CBOR as specified in RFC 8949.

RFC 8949:2020, section 4.2.1 describes the “core deterministic encoding requirements” for CBOR. The requirements regarding preferred serialization and indefinite-length shall be implemented. The requirements regarding sorting of map keys may be implemented.

Table 1 describes a list of Tag values of CBOR major type applied for each encoding type.

Table 1 — Tag value of CBOR major type

Encoding types	Tag value of CBOR major type	Remarks
text string	type 3	unicode encoding
byte string	type 2	
uint	type 0	Unsigned integer
tdate	type 6	See below
boolean	type 7	true; value 21, false; value 20

Field format of date and time is date-time or full-date as specified in ISO 8601-2. Unless otherwise indicated. date-time shall be encoded according to RFC 8949:2020, 3.4.1 and uses Tag value 0 of major type 6, described as tdate (tdate = #6.0(tstr)).

6.2.4 namespace

A namespace defines a data element identifier and specifies the encoding of the format of its value. A document may have multiple namespaces. The meaning of data elements is dependent on which namespace it belongs to.

The namespace field follows the following general format:

[Reverse Domain].[Domain Specific Extension].

EXAMPLE The namespace for the mdoc data defined in this document is “org.iso.23220.1”. The last number “1” in the namespace will be replaced by the edition number of this document.

In case the subdivision of issuing country or issuing authority specifies an extension of the namespace, the structure of namespace shall add its subdivision code (see 6.3.3) as a suffix.

6.3 Standard meta-attributes

6.3.1 Meta attributes for person entity — personal attributes

6.3.1.1 Data element identifier for personal attributes

This subclause specifies data element identifiers which express attributes for describing a natural or legal person and requirements for values of each data element. This subclause specifies data element identifiers and their meaning is namespace specific.

Table 2 describes a set of data elements to express personal attributes. When an implementation of this document uses a data element from Table 2 under the “org.iso.23220.1” namespace, these shall implement the definition and encoding as defined in Table 2. For JSON data model, claims as defined in the IANA JOSE elliptic curves registry [4] shall be used.

[4] https://www.iana.org/assignments/jose/jose.xhtml

If an implementation of this document wants to use a data element from Table 2 that changes the definition or the encoding, it shall be used with a different namespace.

More than two images/biometrics template can be used according to the issuer's policy, if more than two values can be supported for a data element.

Table 2 — Data elements for personal attributes

Data element	Data element identifier	Description	Encoding
Family name	family_name_unicode	Last name, surname, or primary identifier, of the holder	tstr
	family_name_latin1	Last name, surname, or primary identifier, of the holder, Latin1 characters	tstr
Given names	given_name_unicode	First name(s), other name(s), or secondary identifier, of the holder	tstr
	given_name_latin1	First name(s), other name(s), or secondary identifier, of the holder. Latin1 characters	tstr
Date of birth	birth_date	Day, month and year on which the holder was born. Unknown parts (i.e., year, month, day) are masked with 1	See birth_date structure (6.3.1.3)
Sex	sex	Holder's sex using values as defined in ISO/IEC 5218. (0 = Not Known, 1 = Male, 2 = Female, 9 = Non-applicable)	uint
Height (cm)	height	Holder's height in centimetres	uint
Weight (kg)	weight	Holder's weight in kilograms	uint
Place of birth	birthplace	Country and municipality or state/province where the holder was born	tstr
Normal place of residence	resident_address_unicode	The place where the holder resides and/or may be contacted (street/house number, municipality etc.)	tstr
	resident_address_latin1	The place where the holder resides and/or may be contacted (street/house number, municipality etc.), Latin 1 characters	tstr
Residence city	resident_city_unicode	The city/municipality (or equivalent) where the holder lives	tstr
	resident_city_latin1	The city/municipality (or equivalent) where the holder lives, Latin 1 characters	tstr
Postal code	resident_postal_code	The postal code of the holder	tstr
Resident country	resident_country	The country where the holder lives as a two letter country code (alpha-2 code) defined in ISO 3166-1	
Biometric template (face image)	biometric_template_face	A reproduction of the holder's portrait. See 6.3.1.1.2	bstr
Portrait	portrait	Portrait data as specified in ISO/IEC 18013-2:2020, C.4.5.	bstr
Portrait image timestamp	portrait_capture_date	Date when portrait was taken	tdate
Fingerprint data	fingerprint	A reproduction of the holder's fingerprint data (TBC)	bstr
Nationality	nationality	Nationality of the Holder as two letter country code (alpha-2 code) or three letter code alpha-3 code) defined in ISO 3166-1[a]	tstr
Business name	business_name_unicode	Business name of the holder	tstr
	business_name_latin1	Business name of the holder, Latin1 characters	tstr
Organization name	organization_name_unicode	Name of legal person	tstr
	organization_name_latin1	Name of legal person, Latin1 characters	tstr
Name at birth	name_at_birth	The name(s)which holder was born	tstr

[a] For persons without a defined nationality, the data model should be encoded as the values specified in ICAO Doc 9303-3 8th edition Clause 5, Part E.

Table 2 *(continued)*

Data element	Data element identifier	Description	Encoding
Telephone number(s)	telephone_number	Telephone number of the holder, including country code as specified ITU-T E.123 and ITU-T E.164	tstr
e-mail address(es)	email_address	E-mail address of the holder	tstr
Profession	profession	Profession of the holder	tstr
Academic title	title	Academic title of the holder	tstr

[a] For persons without a defined nationality, the data model should be encoded as the values specified in ICAO Doc 9303-3 8th edition Clause 5, Part E.

NOTE 1 Some major eID applications, such as ePassport defined in ICAO Doc 9303-10 and driving licence, defined in ISO/IEC 18013-2 define two different face image data elements, e.g. portrait image and biometric. The latter is used for both visual inspection and biometric comparison, but the former is not usually used. This document defines one face image in a biometric information template.

NOTE 2 Biometric information record structure defined in CBEFF (ISO/IEC 19785 series) consisting of standard biometric header and biometric data block are encapsulated in ASN.1 constructed data object such as biometric information template. This ASN.1 constructed data object is binary string.

6.3.1.2 Portrait image

The portrait image shall be encoded as follows (see Figure 5):

- Application specific identifier, e.g. DG2 with tag '75' as defined by ICAO 9303-10.
- Biometric information template as defined in ISO/IEC 19785-3 (and Biometric information template Group defined in ISO/IEC 7816-11, if the multiple biometric information templates are supported) encapsulating CBEFF (Common Biometric Exchange Formats Framework) structure defined in ISO/IEC 19785-3 (see Table 3).
- CBEFF structure contains biometric data block in accordance with ISO/IEC 19794-5 or ISO/IEC 39794-5 (see Table 4).

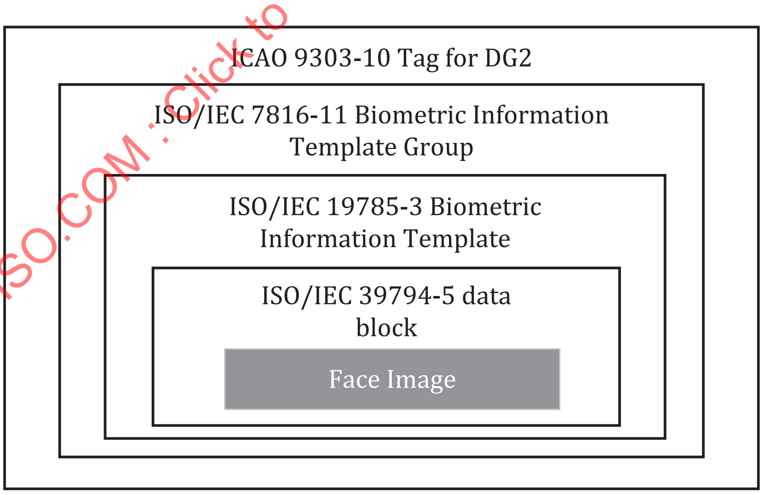
ICAO 9303-10 Tag for DG2
ISO/IEC 7816-11 Biometric Information Template Group
ISO/IEC 19785-3 Biometric Information Template
ISO/IEC 39794-5 data block
Face Image

Figure 5 — Encoding of portrait image

This structure is also applicable to fingerprint, and then shall support ISO/IEC 19794-4 or ISO/IEC 39794-4.

Table 3 — Parameter of Group biometric information table

Element	Parameter	Value	Description
Biometric information template Group	number of biometric information template	<variable>	Number of the supported instance of biometric information templates Mandatory, if the multiple biometric information templates are supported)
biometric information template	CBEFF_patron_header_version	'0101'	Version of CBEFF patron format header (Optional)
	CBEFF_BDB_biometric_type	As specified in ISO/IEC 19785-3	Optional
	CBEFF_BDB_biometric_subtype	As specified in ISO/IEC 19785-3	Optional for face image, mandatory for fingerprint
	CBEFF_BDB_creation_date	As specified in ISO/IEC 19785-3	creation date and time of biometric reference data: fourteen BCD digits (YYYYMMDDHHMMSS) Optional
	CBEFF_BDB_validity_period	As specifies in ISO/IEC 19785-3	A pair of dates (not before, not after): sixteen BCD digits (YYYYMMDDYYYYMMDD) Optional
	CBEFF_BIR_creator	<variable>	Optional
	CBEFF_BDB_format_owner	JTC 1/SC 37	Mandatory
	CBEFF_BDB_format_type	ISO/IEC 19794-4 (for fingerprint) ISO/IEC 19794-5 (for face image)	Mandatory
	CBEFF_BDB	biometric reference data	Mandatory

Table 4 — Parameters for biometric data

Element	Parameter	Value	Description
versionBlock	Generation	3	
	Year	2019	
representationBlocks-> RepresentationBlock	imageRepresentationBlock-> imageRepresentation2DBlock-> representationData2D	<variable>	The face image data in JPEG2000 format
	imageRepresentationBlock-> imageRepresentation2DBlock-> ca ptureDeviceTechnology2DBlock-> classOfDeviceTechnology	Static photograph from scanner	
	imageRepresentationBlock-> imageRepresentation2DBlock-> imageInformation2DBlock-> faceImageKind2D-> faceImage2DType	mrtd	
	imageRepresentationBlock-> imageRepresentation2DBlock-> imageInformation2DBlock-> postAcquisitionProcessingBlock -> multiplyCompressed	TRUE	
	imageRepresentationBlock-> imageRepresentation2DBlock-> imageInformation2DBlock-> imageDataFormat -> imageDataFormat	JPEG2000Lossy	

Table 4 *(continued)*

Element	Parameter	Value	Description

	`imageRepresentationBlock->`
	`imageRepresentation2DBlock->`
	`imageInformation2DBlock->`
	`imageSizeBlock`
		width = 413 height = 531	

	`representationId`	<variable>	

	`captureDateTimeBlock`	year = <var>
		month = <var>
		day = <var>	

	`qualityBlocks-> QualityBlock -> organisation`	<variable>	
	`qualityBlocks-> QualityBlock -> identifier`	<variable>	
	`qualityBlocks-> QualityBlock -> scoreOrError -> score`	<variable>	
	`identityMetadataBlock -> eyeColour`	<variable>	

6.3.1.3 Date of birth as either uncertain or approximate, or both

If date of birth includes an unknown part, the following birth_date structure may be used.

```
birth_date = {
 "birth_date" : full-date,
 ? "approximate_mask": tstr
}
```

`approximate_mask` is an 8 digit flag to denote the location of the mask in YYYYMMDD format. 1 denotes mask.

NOTE 1 `"approximate_mask"` is not intended to be used for calculation.

NOTE 2 The `birth_date` structure is always used, not just when the mask is present.

6.3.2 Attribute statement

6.3.2.1 Data elements for attribute statements

This subclause specifies data elements which express statement attributes for describing an attribute statement of a holder and requirements for values of each data element.

Table 5 describes a set of data elements to express an attribute statement. When an implementation of this document uses a data element from Table 5 under the "org.iso.23220.1" namespace, these shall implement the definition and encoding as defined in Table 5.

If an implementation of this document wants to use a data element from Table 5 that changes the definition or the encoding, it shall be used with a different namespace.

Table 5 — Data elements for attribute statement

Data element	Data element identifier	Description	Encoding
Age attestation: How old are you (in years)?	age_in_years	The age of the holder	uint
Age attestation: In what year were you born?	age_birth_year	The year when the holder was born	uint
Age attestation: Nearest "true" attestation above request	age_over_NN	See 6.3.2.2	bool

6.3.2.2 Age attestation: Nearest “true” attestation above request

This set of elements is used to convey to a verifier, in a data-minimized fashion, if the holder is as old or older than a specified age, or if the holder is younger than a specified age. To achieve this, the mdoc contains age attestation identifiers. An age attestation identifier has the format age_over_NN where NN is a value from 00 to 99. The value of an age attestation identifier can be TRUE or FALSE.

If a verifier includes age_over_NN in a request, it has the meaning of “provide the nearest age attestation equal to or larger than NN with value TRUE, or smaller than NN with value FALSE”. More specifically, after receiving an age_over_NN request, the logic to determine the appropriate response shall be equivalent to the following:

a) For all age attestations of the form age_over_NN stored on the mdoc, consider all the attestations with value TRUE. From among these attestations, check if an attestation exists where nn is equal to or larger than NN. If one and only one such attestation exists, this is the response. If more than one such attestation exists, the response shall be the attestation with the smallest difference between nn and NN.

b) If step 1 does not produce a response, for all age attestations of the form age_over_NN stored on the mdoc, consider all the attestations with value FALSE. From among these attestations, check if an attestation exists where nn is equal to or smaller than NN. If one and only one such attestation exists, this is the response. If more than one such attestation exists, the response shall be the attestation with the smallest difference between NN and nn.

c) If step 2 does not produce a response, no age_over_NN data element shall be returned.

In case of device retrieval, the value of an age_over_NN data element shall be calculated by the issuing authority infrastructure to be valid at the value of the timestamp in the `validFrom` element in the mobile security object (MSO) from 8.2.2.4.

In case of server retrieval, the value of an age_over_NN data element shall be valid at the value of the `iat` timestamp as defined in 8.2.3.3.2.

For the use of age_over_NN data element, see ISO/IEC TS 23220-4.

6.3.2.3 Relationship attributes

This subclause specifies data elements which express attributes for describing a relationship with another person entity and requirements for values of each data element. Legal definitions of these data elements are up to the profile.

Table 6 describes a set of data elements to express relationship attributes. When an implementation of this document uses a data element from Table 6 under the “org.iso.23220.1” namespace, these shall implement the definition and encoding as defined in Table 6.

If an implementation of this document wants to use a data element from Table 6, encoding of values shall be specified in each namespace.

Table 6 — Data elements for relationship attribute

Data element	Data element identifier	Description	Encoding
Father	father	The father of the holder	tstr
Mother	mother	The mother of the holder	tstr
Parent	parent	A parent of the holder	tstr
Son	son	The son of the holder	tstr
Daughter	daughter	The daughter of the holder	tstr
Brother	brother	The brother of the holder	tstr
Sister	sister	The sister of the holder	tstr
Sibling	sibling	The sibling of the holder	tstr

Table 6 *(continued)*

Data element	Data element identifier	Description	Encoding
Spouse	spouse	The spouse of the holder	tstr
Father-in-Law	father_in_law	The father-in-law of the holder	tstr
Mother-in-Law	mother_in_law	The mother-in-law of the holder	tstr
Parent-in-Law	parent_in_law	The parent-in-law of the holder	tstr
Son-in-Law	son_in_law	The son-in-law of the holder	tstr
Daughter-in-Law	daughter_in_law	The daughter-in-Law of the holder	tstr
Child-in-Law	child_in_law	The child-in-law of the holder	tstr
Parental authority	parental_authority	The parental authority of the holder	tstr
Legal representative	legal_representative	The legal representative of the holder	tstr
Agent	agent	The voluntary agent of the holder	tstr

6.3.3 Meta-attribute for issuer entity

This subclause specifies data elements which express attributes for describing an issuer and requirements for values of each data element.

Table 7 describes a set of data elements to express attributes for issuer. When an implementation of this document uses a data element from Table 7 under the "org.iso.23220.1" namespace, these shall implement the definition and encoding as defined in Table 7.

If an implementation of this document wants to use a data element from Table 7 that changes the definition or the encoding, it shall be used with a different namespace.

Table 7 — Data elements for issuer entity

Data element	Data element identifier	Description	Encoding
Issuing country	issuing_country	Country code as alpha 2 and alpha 3 code, defined in ISO 3166-1, which issued the mobile eID document or within which the issuing authority is located	tstr
Issuing subdivision	issuing_subdivision	Subdivision code as defined in ISO 3166-2, which issued the mobile eID document or within which the issuing authority located	tstr
Issuing authority	issuing_authority_unicode	Name of issuing authority	tstr
	issuing_authority_latin1	Name of issuing authority, Latin1 characters	tstr

6.3.4 Data elements for document entity

This subclause specifies data elements which express attributes for describing a document and requirements for values of each data element.

Table 8 describes a set of data elements to express attributes for document. When an implementation of this document uses a data element from Table 8 under the "org.iso.23220.1" namespace, these shall implement the definition and encoding as defined in Table 2.

If an implementation of this document wants to use a data element from Table 8 that changes the definition or the encoding, it shall be used with a different namespace.

Table 8 — Data elements for document entity

Data element	Data element identifier	Description	Encoding
Date of Issue	issue_date	Date mobile eID document was issued	full_date
Date of Expiry	expiry_date	Date mobile eID document expires	full_date
Type of document	document_type	The document type	tstr
Document number	document_number	The number assigned or calculated by the issuing authority	tstr

The validUntil element determines the validity period of the MSO and therefore, the mdoc cannot be validated after this date. mdoc data elements can provide further information on the administrative validity of the mdoc. For example, if the mdoc has an expiry date data element, this date can be later than the validUntil date of the MSO (see 8.2.2.4).

6.3.5 Data elements for document authenticity

This subclause specifies data elements that shall be used as a proof for:

- authenticating the origin of mobile eID data;
- verifying mdoc data has not changed from issuance;
- verifying how up to date the mobile eID data is.

If mobile eID data is retrieved from mobile device, the proof of the mobile eID data shall be generated as specified in ISO/IEC 18013-5:2021, 9.1.2.

If mobile eID data is retrieved from issuer infrastructure via internet, the proof of eID data shall be generated as JWS as specified in ISO/IEC 18013-5:2021, 9.2.2.

6.4 Data element for level of confidence

This subclause specifies identifier of a data element for expressing confidence level as specified in ISO/IEC TS 23220-5. This document only specifies data element identifier, and detailed CDDL structure of Level of Confidence data elements are specified in ISO/IEC TS 23220-5.

```
LevelOfConfidence ; See ISO/IEC TS 23220-5:2023, Annex E
```

7 Cipher suites

7.1 General

This clause defines the following cipher suite identifiers which are used in the ISO/IEC 23220 series:

- elliptic curves;
- TLS;
- digest algorithms;
- digital signature algorithms.

7.2 Elliptic curves

The ISO/IEC 23220 series supports multiple cipher suites for elliptic curve as specified in Table 9. Curve identifiers and key types are defined in the IANA COSE Registry.

Table 9 — Curve identifiers of elliptic curves

Definition	Specification	COSE Curve identifier	Key type	Purpose
Curve P-256	FIPS PUB 186-4	1	EC2	ECDH/ECDSA
Curve P-384	FIPS PUB 186-4	2	EC2	ECDH/ECDSA
Curve P-521	FIPS PUB 186-4	3	EC2	ECDH/ECDSA
X25519	RFC 7748	4	OKP	ECDH
X448	RFC 7748	5	OKP	ECDH
Ed25519	RFC 7748	6	OKP	EdDSA
Ed448	RFC 7748	7	OKP	EdDSA
secp256k1	RFC 8812	8	EC2	ECDSA
brainpoolP256r1	RFC 5639	256	EC2	ECDH/ECDSA
brainpoolP320r1	RFC 5639	257	EC2	ECDH/ECDSA
brainpoolP384r1	RFC 5639	258	EC2	ECDH/ECDSA
brainpoolP512r1	RFC 5639	259	EC2	ECDH/ECDSA
Others		RFU		

7.3 TLS

The ISO/IEC 23220 series supports TLS cipher suites as specified in Table 10.

Table 10 — TLS cipher suites

Cipher suite	References
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	RFC 8422
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	RFC 8422
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	RFC 7905

7.4 Digest algorithms

The ISO/IEC 23220 series supports digest algorithms as specified in Table 11.

Table 11 — Digest algorithm identifiers

Digest algorithm	Digest algorithm identifier	COSE algorithm identifier
SHA-256	“SHA-256”	-16
SHA-384	“SHA-384”	-43
SHA-512	“SHA-512”	-44

7.5 Signature algorithms

The ISO/IEC 23220 series supports digest algorithms as specified in Table 12.

Table 12 — Signature algorithm identifiers

Digital signature algorithm	Digital signature identifier	COSE digital signature identifier
ECDSA with SHA-256	“ES256”	-7
ECDSA with SHA-384	“ES384”	-35
ECDSA with SHA-512	“ES512”	-36
ECDSA secp256k1 with SHA-256	“ES256K”	-47
EdDSA	“EdDSA”	-8

7.6 HMAC algorithm

The ISO/IEC 23220 series shall use “HMAC 256/256” (HMAC with SHA-256) value for identifying mdoc authentication algorithm.

8 Generic data models

8.1 General

This clause specifies generic data models used for the ISO/IEC 23220 series. mdoc data model is the data model used for mdoc response message specified in ISO/IEC TS 23220-4, which is derived from ISO/IEC 18013-5.

Two encoding rules are used for mdoc data model. The CBOR encoded model with MSO (8.2.2) can be used for device retrieval method defined in ISO/IEC 18013-5. For a CBOR encoded model, selective disclosure functionality is supported by the usage of MSO. In addition to selective disclosure, MSO also serves a purpose to prove legitimate possession of the mdoc.

NOTE 1 JSON converted model without MSO (8.2.3) can be used for the server retrieval method defined in ISO/IEC 18013-5.

NOTE 2 For a JSON encoded model, MSO is not required when issuing Identity or Attributes Service Provider returns, only claims requested by the verifier device and consented to by the user in that particular transaction.

JSON data model (8.3) can be used for transport both device retrieval and server retrieval defined in ISO/IEC TS 23220-4 and ISO/IEC TS 18013-7. It can be expressed as a Verifiable Credential and Verifiable Presentation as defined by W3C VC-DATA-MODEL specification encoded as a JWT and signed as a JWS.

Usage of SD-JWT is defined in ISO/IEC TS 23220-4.

NOTE Selective Disclosure functionality is supported by using SD-JWT (Selective Disclosure for JWTs).

8.2 mdoc data model

8.2.1 General

This subclause describes CBOR encoding and JSON conversion of mdoc data model initially defined in ISO/IEC 18013-5.

a) In this document CDDL is used to define data structures to express mdoc data model in CBOR and JSON. CDDL as used in this document as specified in RFC 8610. JSON is standardized in RFC 8259.

b) mdoc data model can be used in both device retrieval and server retrieval defined in ISO/IEC 18013-5.

For an informative example, see A.1.1.

8.2.2 CBOR encoding

8.2.2.1 docType

docType is the document type of the document. doctype is specified by each issuing authority.” The docType “org.iso.23220.1.mID” is reserved for future use.

NOTE There is no requirement for the docType format. To avoid collisions the following general format can be used: [Reverse Domain].[Domain Specific Extension]. It can be used to define other docTypes.

8.2.2.2 namespace

See 6.2.4.

8.2.2.3 Data elements

See 6.3.

8.2.2.4 Mobile Security Object (MSO)

The MSO is specified in ISO/IEC TS 23220-4.

The MSO includes digests of the data elements intended to be returned as issuer signed items and the authorizations for the data elements intended to be returned as device signed items. Even if the holder selects only some of the data elements for disclosure, the verifier can verify integrity and authenticity of selected data by:

- verifying signature of DS certificate with IACA public key;
- verifying signature of MSO with DS signer public key for issuer signed data elements compare the hash values with corresponding digest values;
- compare the hash values with corresponding digest values or device signed data elements perform mdoc authentication, see ISO/IEC TS 23220-4.

8.2.3 JSON conversion

8.2.3.1 General

Data elements may be converted from CBOR to JSON as specified in RFC 8259.

If data elements are converted from CBOR to JSON, "bstr" data elements shall be encoded as base64url-without-padding string as specified in RFC 8949:2020, 6.1.

JWT is a claim representation format supporting JWS to prove the integrity of claims. JWT is specified in RFC 7519.

This subclause specifies requirements on JWT structure compliant to this document. The usages of JWT are out of scope of this document and are described in ISO/IEC TS 23220-4.

JWT consists of the following three components:

- JSON Object Signing and Encryption (JOSE) Header;
- JWT claims;
- JWS.

For signing of JWT, JOSE as specified in RFC 7165 shall be applied.

For an informative example, see A.1.2.

8.2.3.2 JOSE Header

JOSE header describes the cryptographic operations applied to JWS. JOSE header shall support at least the following two header parameters, “typ” header parameter and “alg” header parameter.

“typ” header parameter is used to declare the media type of the JWT. The value of “typ” header parameter for JWT is “JWT” as defined in RFC 7519.

“alg” header parameter is used to declare the algorithm for JWS. If a digital signature is used for JWS, the value shall be one from signature algorithm identifiers defined in 7.5, Table 12. If the MAC is used for JWS, the value shall be HMAC algorithm identifier HS256 (see 7.6).

The example of JOSE Header which uses ECDSA with SHA-256 is as follows.

```
{“typ”:”JWT”,
“alg”:”ES256”}
```

8.2.3.3 JWT claims

8.2.3.3.1 General

The JWT claims Set represents a JSON object whose members are the claims conveyed by the JWT. The following JWT claims can be used for the JWT compliant to this document. The choice of claims is at the discretion of Issuer.

8.2.3.3.2 “iat” (Issued At) claim

The “iat” (Issued At) claim identifies the time at which the JWT was issued. The value of “iat” claim is expressed in UNIX time. Use of “iat” claim is optional.

EXAMPLE

```
“iat”:1611543618 (issued at 25th January 2021, 03:00:18 UTC)
```

8.2.3.3.3 “exp” (Expiration Time) claim

The “exp” (Expiration Time) claim identifies the expiration time on or after which the JWT shall not be accepted for processing. The value of “exp” claim is expressed in UNIX time. Use of “exp” claim is optional.

EXAMPLE

```
“exp”: 1611543918 (expired at 25th January 2021, 03:05:18 UTC)
```

8.2.3.3.4 “aud” (audience) claim

The “aud” (audience) claim identifies the recipients that the JWT is intended for. The recipient intended to process the JWT shall identity itself with a value in the audience claim (e.g. Reader Authentication). If the recipient does not identify itself with a value in the “aud” claim, then the JWT shall be rejected. The “aud” value is a case-sensitive string containing a StringOrURI value or an array of them. Use of the “aud” claim is OPTIONAL.

EXAMPLE

```
“aud”: “https://utopiadot.gov/resources”
```

8.2.3.3.5 “nonce” claim

“nonce” claim is a string value used to associate a session with a JWS, and to mitigate replay attacks.

EXAMPLE

```
“nonce”: “343s$FSFDa-”
```

8.2.3.3.6 “mdoc” (mdoc) claim

The “mdoc” (mdoc) claim is a JSON object that shall include doctype, namespace, user claims.

JWT allows to use private claims names according to the agreement between producer and consumer as specified in RFC 7519:2015, 4.3.

EXAMPLE

```
   “mdoc”: {
   “docType”: “org.iso.23220.1.mID”,
   “namespace”: {
      “org.iso.23220.1”
      “family_name_latin1”: “family_name formatted as IssuedSignedItemBytes”,
      “portrait”: "portrait formatted as IssuedSignedItemBytes”,
   }
}
```

The following rules shall be applied to support mdoc data elements:

a) “docType” claim: The “docType” claim is a string identifying requested document type.

EXAMPLE

```
“docType”: “org.iso.23220.1.mID”
```

b) “namespace” claim: The “namespace” claim identifies requested data elements and the namespace they belong to.

EXAMPLE

```
“namespace”: “org.iso.23220.1”
```

c) User claims: Each user claim shall be formatted as IssuerSignedItemBytes as defined in ISO/IEC 18013-5 mDL.

EXAMPLE User claims as IssuedSignedItemBytes:

```
“family_name”: “family_name formatted as IssuedSignedItemBytes”,
“portrait”: "portrait formatted as IssuedSignedItemBytes”,
"driving_privileges": “driving_privileges formatted as
IssuedSignedItemBytes”,
```

8.2.3.4 JWS

A JWT shall be protected using a JSON Web Signature (JWS). JWS is specified in RFC 7515. The JWS shall be signed with the JWS certificate, and this certificate shall be provided in the JWS header in the registered x5c attribute in accordance with RFC 7515. The digital signature algorithm expressed in JOSE Header shall be used.

8.3 JSON data model

8.3.1 General

This subclause defines a general JSON data model and how it can be Issuer-signed and Holder-signed. Holder can perform proof of possession by signing over an Issuer-signed JSON data model. JSON data model is expressed as a JWT and shall be signed as a JWS.

8.3.2 Issuer-signed

8.3.2.1 JOSE Header

See 8.2.3.2

8.3.2.2 JWT claims

JWT claims applies 8.2.3.3 with the following changes:

— User claims shall be

  — included in an `“mdoc”` claim to indicate that a JWT is compliant to this document;

  — expressed by value instead of as IssuedSignedItemBytes;

— Use of `“aud”` claim is not recommended;

— `“iss”` claim defined in 8.3.2.2.1 shall be present;

— `“sub”` claim defined in 8.3.2.2.2 shall be present.

EXAMPLE `mdoc` claim in a JSON data model

```
“mdoc“: {
   “docType”: “org.iso.23220.1.mID”,
   “namespace”: “org.iso.23220.1”
```