ISO/IEC JTC 1/SC17/WG4-WG10 JAG on ISO-compliant mdoc for eHealth

Release Candidate 2, 2021-09-14

Please provide feedback by 2021-10-16 to arjan.geluk@ul.com

White Paper

Guidelines for developing an ISO-compliant mdoc for eHealth

Executive summary

Vaccination certificates are proposed as one of the instruments to recover society from the Coronavirus pandemic. Several technology propositions have been put forward to enable vaccination certificates. Most of these lack globally interoperable protocols for identification of the certificate holder and verification and authentication of their credentials in a privacy-preserving manner.

Over the last five years, a task force under ISO/IEC JTC1/SC17 (security devices for personal identification) has developed a standard for mobile documents (mdocs). This standard, ISO/IEC 18013-5, provides a generic data model and protocols for mobile credentials, enabling secure wireless communication, user control over what data is released, and electronic authentication of that data. Although originally initiated as a standard for mobile driving licences, it can be applied for health credentials. It addresses relevant security and privacy issues, such as binding a holder to a credential, binding a credential to a mobile device, data minimisation and selective data release, and offline operation. It furthermore addresses non-traceability and availability, even if holder and verifier are without internet connectivity. The ISO/IEC 18013-5 standard is currently being generalised as a multi-part standard for identity management via mobile devices, ISO/IEC 23220. The contributors to this paper (a selection of the ISO/IEC task force members) believe that vaccination, test, and recovery certificates can benefit from these technologies.

This white paper introduces the mdoc concept as specified in ISO/IEC 18013-5 — ISO/IEC 23220, and provides guidelines for applying this concept to vaccination, test, and recovery certificates. Apart from the mentioned standards, this paper is based on:

— WHO International Certificate of Vaccination or Prophylaxis, 2005;
— WHO Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021;
— WHO Digital Documentation of COVID-19 Certificates: Vaccination Status – Web Annex A. DDCC:VS core data dictionary, 27 August 2021
— eHealth Network Technical Specifications for Digital COVID Certificates, Volume 1, V1.0.5, 2021-04-21;
— eHealth Network Guidelines on Value Sets for Digital COVID Certificates, Version 1.2, 2021-07-07;
— eHealth Network Technical Specifications for EU Digital COVID Certificates, JSON Schema Specification, Version 1.3.0, 2021-06-09.

As part of the preparation of this whitepaper, a doctype has been defined for a ‘mobile international certificate of vaccination’; “org.micov.1”. Likewise, a namespace was defined covering vaccination, test, and recovery certificates: “org.micov.vtr.1”. In addition, this paper provides another namespace to enable attestation of a person’s health status without or with minimal disclosure of medical details, and with various options for binding the credential to an individual: “org.micov.attestation.1”. The intent of this namespace is to maximize the privacy benefits that the ISO/IEC 18013-5 standard offers.

In addition to the request/response protocols provided in ISO/IEC 18013-5, support for paper-based credentials is also defined in this white paper.

Acknowledgements

This white paper has been prepared by the ISO/IEC JTC 1/SC17/WG4-WG10 joint action group on ISO-compliant mdoc for eHealth, whose members include:

Arjan Geluk (UL, NL)

Mourad Faher (Thales, FR)

Fabrice Jogand-Coulomb (HID, FR)

Brandon Gutierrez (TSA, US)

Kristina Yasuda (Microsoft, US)

Nuno Ponte (Multicert, PT)

Martijn Haring (Apple, NL)

Anthony Nadalin (US)

David Zeuthen (Google, US)

Jens Urmann (Veridos, DE)

Kenichi Nakamura (Panasonic, JP)

Loffie Jordaan (AAMVA, US)

Adam DeFranco (FAST Enterprises, US)

Jesse Dyer (FAST Enterprises, US)

Jean-Marc Desperrier (Idemia, FR)

Jeff Quarrington (CBN, CA)

David Chadwick (University of Kent, UK)

Xiangying Yang (Apple, US)

Sebastian Zehetbauer (Younix, AT)

Mindy Stephens (AAMVA, US)

David Bakker (UL, NL)

Evangelos Sakkopoulos (Scytales/ University of Piraeus, GR)

Bas van den Berg (RDW, NL)

Matthias Schwan (Bundesdrückerei, DE)

Gilles Roux (Google, US)

David Jencel (Thales, FR)

Andrew Hughes (Idemia, CA)

Ketan Mehta (NIST, US)

Mike McCaskill (AAMVA, US)

Contents

List of abbreviations

BLE	Bluetooth Low Energy
CA	Certificate Authority
CBOR	Concise Binary Object Representation
COSE	CBOR Object Signing and Encryption
CWT	CBOR Web Token
DCC	Digital COVID Certificate
DDCC:VS	Digital Documentation of COVID-19 Certificates: Vaccination Status
EC	Elliptic Curve
eHN	eHealth Network
JSON	JavaScript object notation
MAC	message authentication code
mDL	mobile Driving Licence
mdoc	mobile document
Micov	mobile international certificate of vaccination
MSO	Mobile Security Object
PKI	Public Key Infrastructure
TLS	Transport Layer Security
VICAL	Verified Issuer Certificate Authority List
WHO	World Health Organization

1 Introduction

Vaccination against COVID-19 is considered by many experts to be a key enabler for ending a devastating pandemic. However, reaching a sufficiently high percentage of vaccinated people will take time. While the pandemic is still ongoing, accurate vaccination information may help authorities to manage public health and to get societies back on their feet. Such information may include proof of vaccination, a negative test result or proof of recovery from COVID-19. The authors of this document acknowledge that the pros and cons of "vaccination and test passports" are being actively debated in many jurisdictions around the world and involve difficult questions concerning (among others) freedom of movement, discrimination, and public health. This white paper does not imply a position in these debates.

There are several initiatives for vaccination certificates. Some are focused on the exchange of vaccination details for medical purposes, while others are focused on providing attestation that a person has been vaccinated. These initiatives are proposing, or still evaluating, appropriate enabling technologies.

Whether used for conveying medical details or for attestation, during the actual use of a vaccination certificate, there should be no doubt to whom the data in the certificate pertains. Uncertainty about whether the data actually concerns the person presenting it could lead to incorrect medical or safety-related decisions. Therefore, technology enabling the operational use of vaccination certificates should facilitate verification of the identity of the holder of the certificate, and authentication of the certificate data. And if vaccination certificates are to be used across sectors and geographies, technologies used should be interoperable (work everywhere) and robust (always available, regardless of internet connectivity). Moreover, as sensitive personal data is involved, technologies should be privacy-preserving.

Over the last five years, ISO/IEC has developed a standard that, to our knowledge, complements existing approaches for vaccination certificates. This standard is ISO/IEC 18013-5. Although developed for mobile driving licences, the protocols in this standard have been explicitly designed to be usable for other types of documents, such as health cards, vehicle registration cards, etc. The standard was approved for publication on 18 August 2021 and will be published soon. It has passed several rounds of ISO/IEC's rigorous process for international commenting and balloting, and has been informed by multiple rounds of international interoperability testing on several continents.

ISO/IEC 18013-5 will form the basis for Part 4 of the new multi-part ISO/IEC 23220 standard on "Building blocks for identity management via mobile devices". Part 4 will deal with "Protocols and services in the operational phase". ISO/IEC 23220 will be applicable for any mobile document, not just for mDLs.

ISO/IEC 18013-5 allows any data model for credentials, from any applicative domain, to be represented in a mobile document (mdoc). An mdoc can be present on a mobile device, and/or on a server of the issuing authority. An mdoc allows an mdoc holder to share one or more data elements with an mdoc reader. From the very start of the standardisation process, the ISO/IEC work group has focused on empowering trust in mobile credentials, practising privacy-by-design, designing security in, and achieving international interoperability.

The standard was designed to support:

— a protocol for two devices to engage, establish a secure offline wireless communication channel, and subsequently exchange mdoc data, using structured request and response messages. The standard calls this 'device retrieval'. This protocol facilitates availability and non-traceability;

— an optional protocol to retrieve mdoc data from the issuing authority. The standard calls this 'server retrieval';

— a mechanism by which an mdoc reader is able to establish that the mdoc was truly issued by a valid issuing authority, and is unchanged. The standard calls this 'issuer data authentication';

— a mechanism by which an mdoc reader is able to establish that the mdoc data is bound to the device on which it is resident. The standard calls this ‘mdoc authentication’, and it allows device-binding and anti-cloning;

— a mechanism allowing the selective release of single data elements by the mdoc holder, as well as other measures for data minimisation;

— the exchange of data elements that allow identification of the mdoc holder and thus enable user binding.

2 Scope

This white paper introduces the mdoc concept as standardized in ISO/IEC 18013-5 and ISO/IEC 23220-4, and demonstrates how the standard is ready to be used for vaccination certificates, without any adaptation.

In addition, this whitepaper describes provisions to enable

— optional inclusion of HL7 FHIR bundles for medical purposes[1], e.g. in a clinical context, directly retrievable from the holder's device using the ISO-compliant mdoc request/response protocol.

— the optional issuance and verification of paper-based credentials, using the same namespace, protocols for electronic signing and enabling a common public key infrastructure (PKI);

We invite our audience to provide feedback to this paper, especially regarding integration with various vaccination certificate initiatives.[2]

1 See https://www.hl7.org/fhir/index.html
[2] Please provide feedback by email to arjan.geluk@ul.com

3 Introduction to the ISO/IEC 18013-5 — ISO/IEC 23220 mdoc concept

3.1 Security, privacy, and interoperability for mobile credentials

Following the trend toward contactless and mobile interactions, credential issuers around the world are preparing for the introduction of mobile driving licences and similar types of mobile documents.

To facilitate secure, privacy-preserving and globally interoperable mobile credentials, stakeholders from around the world (see Annex D for details) have collaborated to develop an international standard with protocols for mobile documents (mdocs). The result is ISO/IEC 18013-5, a standard that enables the deployment of mobile credentials with the same level of integrity and authenticity of the electronic data in biometric passports. Credentials based on this standard are available offline, even if neither the holder nor the verifier of the credential has internet connectivity. This facilitates non-traceability. Moreover, such credentials are more privacy preserving than biometric passports, as they support selective disclosure of data.

A critical difference between a physical document and an mdoc is that the latter can be verified electronically and cryptographically. A verifier uses an mdoc reader to obtain mdoc data from the mdoc through secure wireless communication. Both the mdoc and the mdoc reader can be implemented as an app on a mobile device.

3.2 mdoc interfaces

Figure 1 shows the interfaces in the scope of the ISO/IEC 18013-5 standard:

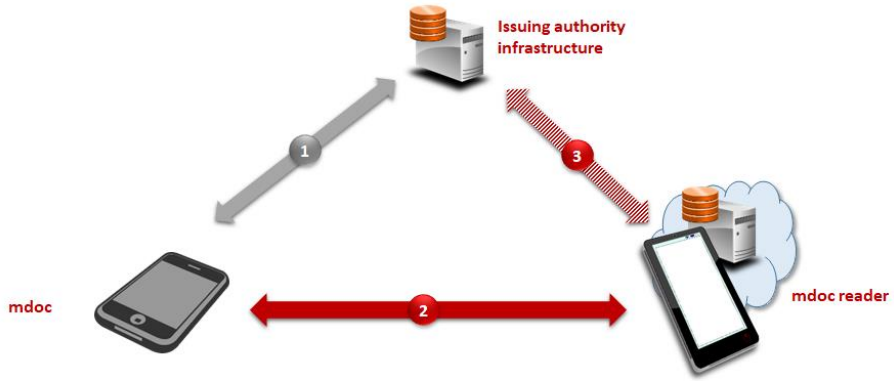

Figure 1 - ISO/IEC 18013-5 mdoc interfaces

Interface 1: issuing authority infrastructure ↔ mdoc. This provisioning interface is recognized in ISO/IEC 18013-5, and subject to standardisation in ISO/IEC TS 23220-3.[3]

Interface 2: mdoc ↔ mdoc reader. This interface can be used for establishing a secure channel between the mdoc and the mdoc reader and for exchanging mdoc data.

Interface 3: mdoc reader ↔ issuing authority infrastructure. This optional interface can be used to retrieve mdoc data directly from the issuer, e.g. if the mdoc data does not reside on the mobile device.

[3] ISO/IEC TS 23220-3 — Building blocks for identity management via mobile devices — Part 3: Protocols and services for the issuing phase.

3.3 mdoc functional requirements

Key stakeholders, such as issuers and verifiers, provided the ISO/IEC work group with the following minimum functional requirements for a standard for mdocs:

— an mdoc verifier with an mdoc reader will be able to request, receive and verify the integrity and authenticity of an mdoc, whether online connectivity is present or not for either the mdoc or the mdoc reader;

— an mdoc verifier not associated with the mdoc issuer will be able to verify the integrity and authenticity of the mdoc;

— the mdoc verifier will be able to confirm the binding between the person presenting the mdoc and the person identified in the mdoc (i.e., the mdoc holder);

— the interface between the mdoc and the mdoc reader will support the selective release of mdoc data to an mdoc reader.

3.4 mdoc data model, data elements, doctype and namespace

The mdoc data model, which is illustrated in Figure 2, is based on elements with unique identifiers within a namespace. The number of elements can vary, and the model is indifferent to the value and data format of each element. As such the data model is generic and can apply to any kind of document.

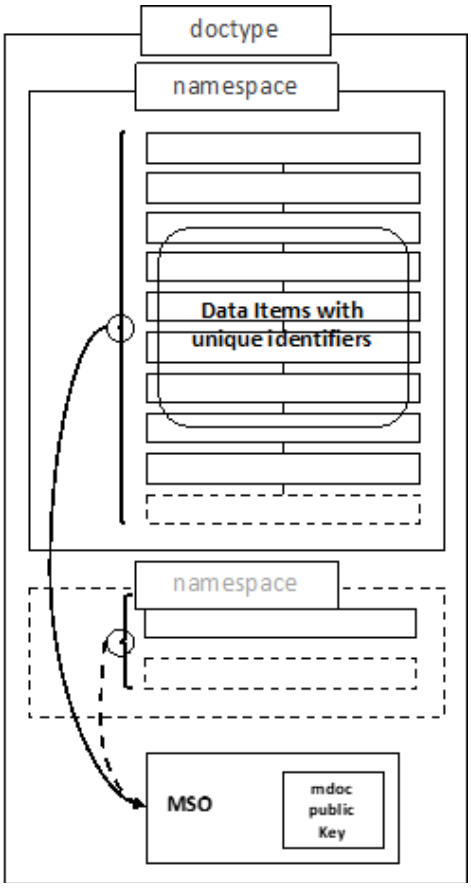

Figure 2 - mdoc data model

(source: contribution to ISO/IEC 18013-5)

mdoc data consists of individual data elements that can be requested and returned independently from each other. An mdoc is addressed by its doctype, and may include data elements from one or more namespaces.

ISO/IEC 18013-5 enables the definition of any doctype and/or namespace for mdocs, whether completely new or in support of an existing data model. The standard defines a first mdoc: a mobile driving licence (mDL), based on the data model for domestic and international driving permits regulated in the UN conventions on road traffic.

Authenticity and integrity validation is enabled by a mobile security object (MSO), which includes (1) a hash value for each data element of the mdoc it pertains to, (2) an mdoc public key, enabling binding of the mdoc to a mobile device, and (3) the electronic signature of the document signer, whose signature is placed under the responsibility of the issuing authority.

3.5 Trust model

ISO/IEC 18013-5 uses public key cryptography and a public key infrastructure for authenticating mdoc data.

At transaction time, the mdoc shares (1) zero or more data elements and (2) the MSO, which includes the document signer (DS) public key certificate. Each data element is accompanied by a digestID, which identifies the applicable hash value in the MSO. Instead of a single DS certificate, the MSO may contain an X.509 certificate chain, if the mdoc is trusted under a multi-level PKI.

The mdoc reader obtains the issuer's Certification Authority (CA) public key[4] out-of-band. At transaction time, the mdoc reader validates (1) the integrity of each data element, by verifying the identified hash value in the MSO, (2) the signature on the MSO, using the document signer certificate, and (3) the document signer certificate (chain), using the CA public key obtained out-of-band.

The trust model in ISO/IEC 18013-5 assumes that each issuing authority has its own root CA. To enable mdoc verifiers to establish trust in mdocs issued by multiple issuing authorities, a verified issuer CA list (VICAL) is standardized. This leaves the freedom for issuers to not necessarily subject themselves to a higher certification authority in a PKI, and provides verifiers with the ability to decide for themselves which issuers' mdocs to accept. VICALs could also be published by (inter)national organisations.

3.6 Adoption

Already in 2019, 30 implementations of a draft version of ISO/IEC 18013-5 participated in an interoperability test event. At present, several issuing authorities around the world (Australia, Europe, North America) are introducing driving licence and vehicle registration mdocs. Since Android 11, Google made the Android IdentityCredentialAPI[5] available, which implements ISO/IEC 18013-5, facilitating uniform hardware security for mdocs. In 2021, Apple announced ISO/IEC 18013-5 support for mobile driving licence and mobile ID in Wallet[6].

[4] Or the public key of the highest CA, in case of a multi-level PKI.
[5] https://developer.android.com/reference/androidx/security/identity/IdentityCredential
[6] https://www.apple.com/newsroom/2021/09/apple-announces-first-states-to-adopt-drivers-licenses-and-state-ids-in-wallet/

4 ISO/IEC 18013-5 — ISO/IEC 23220 mdoc for vaccination certificates

4.1 Existing harmonization: international certificate of vaccination

The International Certificate of Vaccination or Prophylaxis[7], harmonized and published by the World Health Organization, notes that *"The only disease specifically designated in the International Health Regulations (2005) for which proof of vaccination of prophylaxis may be required as a condition of entry to a State Party, is yellow fever. … This same certificate will also be used in the event that these Regulations are amended or a recommendation is made by the World Health Organization to designate another disease."*

The international certificate of vaccination contains information identifying the holder of the certificate, and information pertaining to the individual vaccinations administered to the holder of that certificate.

4.2 Applying ISO/IEC 18013-5 in support of WHO DDCC:VS and eHealth Network DCC

As described above, ISO/IEC 18013-5 allows existing data models for credentials from any applicative domain to be represented in a mobile document (mdoc). Therefore, the benefits of privacy-by-design, designed-in security, and international interoperability can be very straightforwardly made available to vaccination certificates.

To demonstrate the feasibility of applying ISO/IEC 18013-5 for vaccination certificates efficiently and effectively, we took the WHO harmonized Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS) as the basis for a new doctype and namespace: mobile international certificate of vaccination (micov).

To demonstrate the extensibility of this approach, we further added the eHealth Network value sets for Digital COVID Certificates (DCC) for proof of vaccination, test, and recovery to this new namespace. Please refer to Annex A.

4.3 Privacy-preserving attestation of vaccination, test, or recovery

To provide strong, yet privacy-preserving proof that an mdoc holder has been vaccinated, has obtained a negative test result, or has recovered from an infectious disease, Annex A defines specific data elements. These data elements can be used to provide attestation with a simple True/False, without the need to share further details[8].

To support attestation that, for any disease,

— the mdoc holder has been vaccinated;

— the mdoc holder has recovered (and is considered immune);

— the mdoc holder has obtained a negative test result;

— the mdoc holder fulfils set requirements for safe entry in a specific context (leisure or travel),a *"org.micov.attestation.1"* namespace has been added, supplementing the abovementioned "org.micov.vtr.1" namespace.

The namespace definitions are presented in Annex A.

[7] https://www.who.int/ihr/IVC200_06_26.pdf?ua=1

[8] In ISO/IEC 18013-5, the same approach is used for age attestation, using the age_over_NN data element.

Annex A

ISO-compliant mdoc for international certificate of vaccination, test, or recovery

A.1 Basis for this proposal

This proposal for an ISO-compliant mobile international certificate of vaccination (micov) is based on:

— International Certificate of Vaccination or Prophylaxis, International Health Regulations (2005), World Health Organization, https://www.who.int/ihr/IVC200_06_26.pdf?ua=1

— WHO, Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021

— WHO, Digital Documentation of COVID-19 Certificates: Vaccination Status – Web Annex A. DDCC:VS core data dictionary, 27 August 2021

— eHealth Network, Technical Specifications for EU Digital COVID Certificates, Volume 1: formats and trust management, V1.0.5, 2021-04-21,;

— eHealth Network, Value Sets for Digital COVID Certificates, Version 1.2, 2021-07-07.**Error! Hyperlink reference not valid.**;

— eHealth Network, Technical Specifications for EU Digital COVID Certificates, JSON Schema Specification, Version 1.3.0, 2021-06-09.

This proposal is suited to represent vaccination information regarding any disease, and also supports test and recovery certificates.

The WHO published a harmonized international certificate of vaccination or prophylaxis in 2005, based on international health regulations. This certificate contains information identifying the holder of the certificate, and information pertaining to the individual vaccinations administered to the holder of the certificate.

The datasets defined for vaccination certificates in the WHO DDCC:VS and eHN DCC publications largely overlap with the data contained in the internationally regulated WHO Certificate of Vaccination or Prophylaxis. In addition to the Vaccination/Prophylaxis information and Person identification, they provide more options for binding the certificate to the identity of the person, and certificate metadata.

The WHO (2005) provides guidance for linking the vaccination information to a passport or travel document and optionally a national identification document. The WHO DDCC:VS (2021) and eHN DCC (2021) enable linking the vaccination information to more identifiers pertaining to the vaccinated, tested and/or recovered person, such as driving licence number, health registry number, citizen service number, etc.

On top of the information pertaining to individual vaccinations, the eHN publications specify metadata pertaining to the overall certificate, such as certificate issuer, and validity period of the certificate, in addition to the validity of individual claims of vaccination(s), test or recovery.

A.2 Micov document type and namespaces

A.2.1 DocType and NameSpace identifiers

`DocType` and `NameSpace` are used to encapsulate the document type and the namespace in which the data elements are defined. The two concepts are defined in Clause 8.3.1 of ISO/IEC 18013-5.

This white paper introduces a new document type, called the mobile international certificate of vaccination (micov). The document type for a micov shall be "org.micov.1". The number "1" in the document type might be increased in future versions of this paper.

If an mdoc reader wants to retrieve a micov, the `DocType` field in the device retrieval mdoc request or server retrieval mdoc request will contain the micov document type.

This document also introduces three new namespaces:

- A namespace for vaccination, test and/or recovery (VTR) data, which shall be "org.micov.vtr.1". Within this namespace, only data elements defined in Annex A.2.3 may be used.
- A namespace for attestation data, which shall be "org.micov.attestation.1". Within this namespace, only data elements defined in Annex A.2.4 may be used.
- A namespace for Fast Healthcare Interoperability Resources (FHIR) data, which shall be "org.micov.fhir.1". Within this namespace, only data elements defined in Annex A.2.5 may be used.

The source for a number of the data element definitions in these annexes are the eHealth Network DCC and WHO DDCC:VS documents listed in Annex A.1.

`DocType` and `NameSpace` are used within an ISO/IEC 18013-5 compliant mobile document (mdoc). In addition, Annex B to this paper includes provisions to use the same `DocType` and `NameSpace` approach to represent a mobile document on paper (mdop).

A.2.2 Coding provisions

The micov data elements shall be as defined in A.2.3, A.2.4 and A.2.5. Within this Annex A, and in Annex B, the following coding provisions apply[9]:

— CDDL (Concise Data Definition Language) as specified in RFC 8610 is used to express CBOR and JSON-encoded data structures.

— CBOR structures shall be encoded according to RFC 7049. JSON structures shall be encoded according to RFC 8259. RFC 7049, section 3.9 describes four rules for canonical CBOR. Three of those rules shall be implemented for all CBOR structures as follows:

- — integers (major types 0 and 1) shall be as small as possible;
- — the expression of lengths in major types 2 through 5 shall be as short as possible;
- — indefinite-length items shall be made into definite-length items.

— The fourth rule regarding sorting of map keys is not required. Furthermore, maps (major type 5) shall not have multiple entries with the same key.

— The "Identifier" column in Table A.1 and Table A.2 is used for `DataElementIdentifier` in the device retrieval mdoc request or server retrieval mdoc request (see Clause 8.3.1 of ISO/IEC 18013-5).

[9] Note that these coding provisions are consistent with the coding provisions used in ISO/IEC 18013-5.

— The "Presence" column in Table A.1 and Table A.2 indicates whether the presence of the element on a micov is mandatory (M), optional (O) or conditional (C).

NOTE 1: Mandatory presence does not mean that granting access for these elements to an mdoc reader is mandatory.

— The “Format” column in Table A.1 and Table A.2 indicates how the data elements shall be encoded. “tstr”, “uint”, “bstr”, “bool” and “tdate” are CDDL representation types as defined in RFC 8610. This document specifies “full-date” as full-date = #6.1004(tstr), where tag 1004 is specified in RFC 8943.

— In accordance with RFC 8949 Section 3.4.1, a tdate data item shall contain a date-time string as specified in RFC 3339. In accordance with RFC 8943, a full-date data item shall contain a full-date string as specified in RFC 3339.

— The following requirements apply to the representation of dates in micov data elements, unless otherwise indicated:

— Fraction of seconds shall not be used.
— No local offset from UTC shall be used, as indicated by setting the time-offset defined in RFC 3339 to “Z”.

— If data elements are encoded with JSON for the server retrieval methods, the data elements shall be encoded as specified in RFC 8949, Section 6.1.

NOTE 2: This whitepaper is intended to convey the mdoc concepts, and does not pretend to have complete coding provisions. For the encoding of values in individual data fields, WHO DDCC:VS Annex A and eHN DCC value sets and JSON Schema can be leveraged.

A.2.3 namespace: org.micov.vtr.1

This namespace supports vaccination, test or recovery certificate data elements.

Table A.1 - Vaccination, test, or recovery certificate data elements

Identifier	Format	Description	Presence
nam	`Name`	Legal name – Family name, Given name. See clause A.2.3.1.	C[1]
fn	`tstr`	Family name	C[1]
gn	`tstr`	Given name	C[1]
dob	`full-date`	Date of birth	M
pid	`Pid`	Person ID, to be used in case the micov is represented as an mdop as specified in Annex B See clause A.2.3.2.	O
pid_[pty]	`Pid`	Person ID, to be used in case the micov is represented as an ISO-compliant mdoc as specified in this Annex. See clause A.2.3.2.	O
sex	`uint`	Sex, encoded per ISO/IEC 5218	O

v	`Vac`	Vaccination entry, to be used in case the micov is represented as an mdop as specified in Annex B. See Annex A.2.3.3.	O
v_[ICD11DC]_[N]	`Vac`	Vaccination entry, to be used in case the micov is represented as an ISO-compliant mdoc as specified in this Annex. See Annex A.2.3.3.	O
t	`Test`	Test entry, to be used in case the micov is represented as an mdop as specified in Annex B. See clause A.2.3.4.	O
t__[ICD11DC]_[N]	`Test`	Test entry, to be used in case the micov is represented as an ISO-compliant mdoc as specified in this Annex. See Annex A.2.3.4.	O
r	`Rec`	Recovery entry, to be used in case the micov is represented as an mdop as specified in Annex B. See Annex A.2.3.5.	O
r_[ICD11DC]	`Rec`	Recovery entry, to be used in case the micov is represented as an ISO-complicant mdoc as specified in this Annex. See Annex A.2.3.5.	O
[1]) at least either `nam` or `fn` and `gn` shall be present. The `fn` and `gn` elements may be issued instead of, or in addition to the `nam` element, to enable selective disclosure, i.e. sharing of partial name info.			

A.2.3.1 Name encoding

```
Name = {
 ?"fn"        : tstr,       ; Family name
 ?"fnt"       : tstr,       ; Transliterated family name
 ?"gn"        : tstr        ; Given name
 ?"gnt"       : tstr,       ; Transliterated given name
}
```

A Name shall not be an empty map; at least one key-value pair shall be present.

A.2.3.2 Person ID and data element identifier encoding

```
Pid = {
  "pty" : tstr,      ; type of person identifier (value per HL7 FHIR
                     ; https://www.hl7.org/fhir/valueset-identifier-type.html)
  "pnr" : tstr,      ; unique number for the pty/pic or pty/pic/pia combination
  "pic" : tstr,      ; Issuing country of the pty.
 ?"pia" : tstr       ; Issuing authority of the pty (conditional; shall be
                     ; present if pnr is not unique for the combination of
                     ; pty and pic)
}
```

A person ID data element indicates an identification document issued to the legitimate holder of the micov. A verifier can request one or more of these data elements, and subsequently verify that the person presenting the micov indeed possesses the indicated identification document, and that the person identified in that document is indeed the same person as the one presenting the micov.

In case a micov is represented as an mdop as specified in Annex B, a single person ID data element shall be present. Its identifier shall be “pid”.

In case a micov is represented as an ISO-compliant mdoc as specified in this Annex, multiple person ID data elements may be present, each representing a different type of identification document. Each person ID data element shall have the identifier "pid_[pty]", where "[pty]" shall be replaced with the type of identification document , as specified in HL7 FHIR, see https://www.hl7.org/fhir/valueset-identifier-type.html. No "pid" data element shall be present.

EXAMPLE: If both a driving license and a passport are present as a person ID, the PID data elements have identifiers "pid_DL" and "pid_PPN", respectively.

A.2.3.3 Vaccination entry and data element identifier encoding

```
Vac = {
  "tg" : tstr,      ; Disease or agent targeted
 ?"vp" : tstr,      ; Vaccine or prophylaxis
 ?"mp" : tstr,      ; Vaccine medicinal product
 ?"br" : tstr,      ; Vaccine brand
 ?"ma" : tstr,      ; Marketing authorization holder / Manufacturer
 ?"bn" : tstr,      ; Batch number or lot number of the vaccine
 ?"dn" : uint,      ; Dose number
 ?"sd" : uint,      ; Total series of doses
 ?"dt" : full-date, ; Date of vaccination
 ?"co" : tstr,      ; Country of vaccination
 ?"ao" : tstr,      ; Administering organization
 ?"ap" : tstr,      ; Administering professional
 ?"nx" : full-date  ; Due date of next dose, if required
 ?"is" : tstr,      ; Certificate issuer
 ?"ci" : tstr,      ; Unique certificate identifier (UVCI)
 ?"pd" : tstr,      ; Protection duration
 ?"vf" : full-date, ; Valid from
 ?"vu" : full-date  ; Valid until
}
```

In case a micov is represented as an mdop as specified in Annex B, a single vaccination entry data element shall be present. Its identifier shall be "v".

NOTE: If the person holding the health certificate was vaccinated more than once, it is good practice to include the information for the last vaccination in the paper-based micov.

In case a micov is represented as an ISO-compliant mdoc as specified in this Annex, multiple vaccination entry data elements may be present. Each vaccination entry data element shall have the identifier "v_[ICD11DC]_[N]", where "[ICD11DC]" shall be replaced with the ICD-11 Code of the disease targeted, as specified in the WHO's International Statistical Classification of Diseases and Related Health Problems (ICD), see https://icd.who.int/en. [N] shall be replaced with a number starting at 1 for the first vaccination for the disease in question and increased by 1 for every subsequent vaccination. No "v" data element shall be present.

EXAMPLE: If the person holding the health certificate was vaccinated for COVID-19 twice, the vaccination entry data elements have identifiers "v_RA01_1 and "v_RA01_2", respectively.

A.2.3.4 Test entry and data element identifier encoding

```
Test = {
  "tg" : tstr,      ; Disease or agent targeted
 ?"tt" : tstr,      ; Type of test
 ?"nm" : tstr,      ; Test name
 ?"ma" : tstr,      ; Test manufacturer
 ?"dr" : tdate,     ; Date/time of test result
 ?"sc" : tdate,     ; Date/time of sample collection
  "tr" : tstr,      ; Test result (coding per SNOMED CT)
```

```
 ?"tc" : tstr,      ; Testing centre
 ?"co" : tstr,      ; Country where testing was performed
 ?"is" : tstr,      ; Certificate issuer
 ?"ci" : tstr       ; Unique certificate identifier (UVCI)
}
```

In case a micov is represented as an mdop as specified in Annex B, a single test entry data element shall be present. Its identifier shall be "t".

NOTE: If the person holding the health certificate was tested more than once, it is good practice to include the information for the last test in the paper-based micov.

In case a micov is represented as an ISO-compliant mdoc as specified in this Annex, multiple test entry data elements may be present. Each test entry data element shall have the identifier "t__[ICD11DC]_[N]", where "[ICD11DC]" shall be replaced with the ICD-11 Code of the disease targeted, as specified in the WHO's International Statistical Classification of Diseases and Related Health Problems (ICD), see https://icd.who.int/en. [N] shall be replaced with a number starting at 1 for the first test for the disease in question and increased by 1 for every subsequent test. No "t" data element shall be present.

EXAMPLE: If the person holding the health certificate was tested for COVID-19 twice, the test entry data elements have identifiers "t_RA01_1 and "t_RA01_2", respectively.

A.2.3.5 Recovery entry and data element identifier encoding

```
Rec = {
  "tg" : tstr,      ; Disease or agent recovered from
  "fr" : full-date, ; Date of first positive test result
 ?"co" : tstr,      ; Country of Test
 ?"is" : tstr,      ; Certificate Issuer
 ?"df" : full-date, ; Certificate Valid From
 ?"du" : full-date, ; Certificate Valid Until
 ?"ci" : tstr       ; Unique Certificate Identifier
}
```

In case a micov is represented as an mdop as specified in Annex B, a single recovery entry data element shall be present. Its identifier shall be "r".

In case a micov is represented as an ISO-compliant mdoc as specified in this Annex, multiple recovery entry data elements may be present, but at most one for each disease. Each recovery entry data element shall have the identifier "r__[ICD11DC]", where "[ICD11DC]" shall be replaced with the ICD-11 Code of the disease targeted, as specified in the WHO's International Statistical Classification of Diseases and Related Health Problems (ICD), see https://icd.who.int/en. No "r" data element shall be present.

EXAMPLE If the person holding the certificate recovered from both COVID-19 and yellow fever, the recovery entry data elements have identifiers "r_ RA01" and "r_1D47", respectively.

A.2.4 namespace: org.micov.attestation.1

This namespace supports attestation that, for any specified disease (as identified by the ICD-11 Disease Code), the mdoc holder:

— has been vaccinated;

— has recovered (and is considered immune);

— has obtained a negative test result;

— fulfils set requirements for safe entry in a specific context (leisure or travel).

For binding the attestation (or other data from the org.micov.vtr.1 namespace) to the holder, optional identity attributes are provided, including face image, initials, and elements of the holder's date of birth.

Table A.2 - Attestation data elements

Identifier	Format	Description	Presence
`[ICD11DC]_vaccinated`	`bool`	Attest that the holder has been fully vaccinated. Replace "[ICD11DC]" in the data element identifier with the ICD-11 Disease Code of the disease or agent targeted, e.g. "1D47_vaccinated" to reflect a yellow fever vaccination.	O
`[ICD11DC]_recovered`	`Recovered` (see below)	Attest that the holder has recovered (and is considered immune) from the disease identified in the data element identifier, e.g. "RA01_recovered" to reflect recovery from COVID-19.	O
`[ICD11DC]_test`	`Test` (see below)	Attest that the holder obtained a negative test result.	O
`safeEntry_Leisure`	`SafeEntry`	Attest that the holder fulfils certain set requirements for safe entry in a leisure context (without disclosing whether that is based on vaccination, recovery, or negative test). See below.	O
`safeEntry_Travel`	`SafeEntry`	Attest that the holder fulfils certain set requirements for safe entry in a travel context (without disclosing whether that is based on vaccination, recovery, or negative test). See below.	O
`Fac`	`bstr`	Face image of the holder, to confirm binding of the attestation to the holder.	O

		Encoding: JPEG or JPEG2000.[10]	
fni	tstr	Family name initial character – supports attestation using partial ID information	O
gni	tstr	Given name initial character – supports attestation using partial ID information	O
by	date-fullyear	Birth year according to RFC3339 – supports attestation using partial ID information	O
bm	date-month	Birth month according to RFC3339 – supports attestation using partial ID information	O
bd	date-mday	Birthday according to RFC3339 – supports attestation using partial ID information	O

```
Recovered =
{
  "RecovDiseaseAgent" : tstr,      ; Disease or agent the citizen has recovered from
  "FirstPosTest" : full-date       ; Date when the sample for the test was collected that
                                   ; led to positive test
}


Test =
{
  "Result" : tstr,                 ; Test result – coding per SNOMED CT
 ?"TypeOfTest" : tstr,             ; e.g. PCR test
  "TimeOfTest" : tdate             ; consider rounding to the hour in the interest of
                                   ; privacy preservation
}

SafeEntry =
{
  "SeCondFulfilled" : bool,       ; (true/false)
  "SeCondType"      : tstr,       ; "leisure" or "travel". Other condition types may be
                                  ; added in the future. The exact scope and (legal) meaning
                                  ; is out of scope of this document.
  "SeCondExpiry"    : tdate       ; consider rounding to the hour in the interest of
                                  ; privacy preservation; recommended to provide a short
                                  ; validity and refresh regularly, to not leak how the
                                  ; conditions for safe entry are fulfilled (e.g. expiry
                                  ; in a far future suggesting vaccination or recovery)
}
```

[10] Instead of requesting this data element, an mdoc reader could request a pid_[pty] data element specified in clause A.2.3.2, and subsequently confirm the binding of the holder to that person identifier.

A.2.5 namespace: org.micov.fhir.1

Coding provisions:

Identifier:
[Element Id]_[number]:[link]
The [number] element is to support multiple structures of the same element id.
The optional [link] element can be used to indicate certain elements are meant to be linked.

The value of the FHIR structure is the full FHIR structure encoded in CBOR.

Annex B

Direct representation of a micov in a QR code (mdoc on paper, mdop)

B.1 Introduction

For privacy and security reasons, the protocols in ISO/IEC 18013-5 were designed for selective release of individual data elements upon user consent, using a request-response approach. ISO/IEC 18013-5 does therefore not support direct representation of credential data in a QR code. In some situations, however, such a direct representation might be desirable, especially because it can be printed on paper and can therefore exist apart from a mobile device.

To support leveraging the same doctype/namespace approach and trust model for both digital and paper-based mobile international certificates of vaccination (micov), this Annex specifies a representation of a micov that can be conveyed using a QR code and hence can be printed on paper. This representation is referred to as an mdoc on paper (mdop). An mdop uses a signed CBOR Web Token (CWT) instead of a ISO/IEC 18013-5 MSO.

Note that some of the features of a fully ISO/IEC 18013-5 compliant mobile document are not supported by this representation:

— Although the data in an mdop is authenticated, it is not encrypted. This means that anybody with access to the QR code will be able to read the data.
— Data minimization is not possible, since there is no way for a reader to request specific data elements. Instead, all data contained in the certificate is present in the mdop, whether the verifier needs this data or not.
— Selective release of data elements is not possible, since there is no way for the holder to approve the release of the specific data elements.
— User consent can be given only implicitly, by showing the QR code to a verifier.

B.2 Requirements

The following requirements apply for an mdop:

— The contents shall be a CWT according to RFC 8392.

— The CWT shall be of type COSE_Sign1.

— To allow signature verification, the headers of the COSE_Sign1 shall contain the key identifier (kid) element as defined in RFC 8152 or the x5chain element as defined in draft-ietf-cose-x509-08.

— The following claims shall be present in the CWT:

- exp (key value = 4) Expiration Time as defined in RFC 8392
- NameSpaces (key value = -66000) as defined below
- DocType (key value = -66001) as defined below

— The following claims may be present and shall be supported by readers:

- nbf (key value = 5) Not Before as defined in RFC 8392
- iat (key value = 6) Issued At as defined in RFC 8392

— The NameSpaces and DocType claims are defined according to the following CDDL[12]:

[12] Note that these definitions are identical to those in ISO/IEC 18013-5.

```
NameSpaces = {
       + NameSpace => DataElementsValues
}
DataElementsValues = {
       + DataElementIdentifier => DataElementValue
}
DocType = tstr                    ; Doctype identifier
NameSpace = tstr                  ; Namespace identifier
DataElementIdentifier = tstr      ; Data element identifier
DataElementValue = any            ; Data element value
```

As explained in Annex B.1, the `NameSpaces` map shall contain all data elements contained in the certificate. No data minimization or selective release is possible in this representation.

— The CWT shall be encapsulated in the following CBOR structure:

```
mdop = {
       ? -1: bstr, ; raw CWT
       ? -2: bstr, ; zlib compressed CWT
}
```

The key-value pair with key = -1 (if present) shall contain the CWT, without any compression or alteration.
The key-value pair with key = -2 (if present) shall contain the CWT in zlib compressed format as specified in RFC 1950.
At least one of these pairs shall be present in the `mdop` map.

— The mdop structure shall be encoded as a barcode compliant with ISO/IEC 18004. The QR code shall contain a URI with “mdop:” as scheme and the mdop structure encoded using base64url-without-padding, according to RFC 4648, as path.

NOTE The requirements above result in the content of the QR code as “mdop:” followed by the base64url-without-padding encoded mdop structure.

Annex C

Overview of ISO/IEC 18013-5

C.1 Introduction

C.1.1 General

Please note that this Annex quotes from ISO/IEC 18013-5 without always indicating this.

C.2 Overview

This ISO/IEC 18013-5 device retrieval mechanism allows a verifier to request and read any number of data elements from different documents stored on a mobile device, using just one request-response pair. Minimizing the number of necessary request-response messages has a major performance impact. A precondition for this device retrieval mechanism is a device engagement between the mobile device and the reader in order to set up a BLE, NFC or Wi-Fi Aware connection.

Similarly, the ISO/IEC 18013-5 server retrieval mechanism allows to request and read any number of data elements from different documents stored in the issuing authority infrastructure using just one request-response pair.

C.3 Reading an mdoc

Wording: The ISO/IEC 18013-5 standard uses the following terminology:

- **mdoc** – a document / application on a mobile device
- **mdoc reader** – device that can retrieve mdoc data
- **verifier** – person / organization using an mdoc reader to verify an mdoc

During **device engagement**, information required to setup and secure data retrieval is exchanged between the mDL and the mDL reader. Transmission technologies available to transfer the device engagement data are NFC or QR code.

Device retrieval is specified for the following transmission technologies:

- Near Field Communication (NFC)
- Bluetooth Low Energy (BLE)
- Wi-Fi Aware

The mdoc data elements, the device retrieval and other messages are CBOR (Concise Binary Object Representation) data structures according to RFC 7049 / RFC 8949.

Server retrieval makes use of JSON (JavaScript Object Notation) data structures according to RFC 8259.

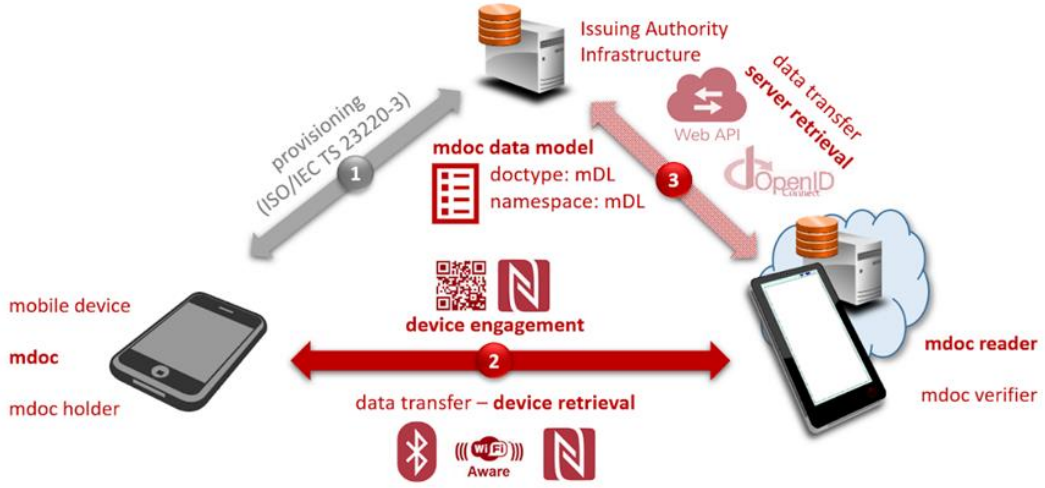

Figure *C*.1 - ISO/IEC 18013-5 mdoc communication protocols

C.3.1 Data Model

According to the ISO/IEC 18013-5 data model, every type of document is identified by a **doctype**. The data elements of an mdoc are identified by unique identifiers which are made up of a **namespace** and an **element identifier** within this namespace. An mdoc may contain data elements from one or more namespaces, see Figure B.2. The data elements of a namespace are all at the same level; there is no nesting, no hierarchy, but just a flat structure (of course the data elements itself may be constructed, i.e. arrays, maps etc.).

Doctypes, namespaces and element identifiers are CBOR text strings. For the mobile security object (MSO), see Clause B.4.2 Issuer data authentication below.

Example: ISO/IEC 18013-5 defines for the mobile Driving Licence:

- the namespace "org.iso.18013.5.1" (the last 1 identifies the edition of the standard) and mandatory and optional data elements within this namespace; these data elements are identified by (self-explanatory) identifiers such as "family_name", "document_number".
- the doctype "org.iso.18013.5.1.mDL". A document of this doctype contains data elements from the org.iso.18013.5.1 namespace and may contain data elements from other (domestic) namespaces to meet issuing authority specific purposes.

NOTE: There is a discussion / work ongoing how this data model can be used / extended for W3C's Verifiable Credentials (https://www.w3.org/TR/vc-data-model/), see the latest ISO/IEC TS 23220-2 draft.

For details on the data model, see ISO/IEC 18013-5 Clause 7.

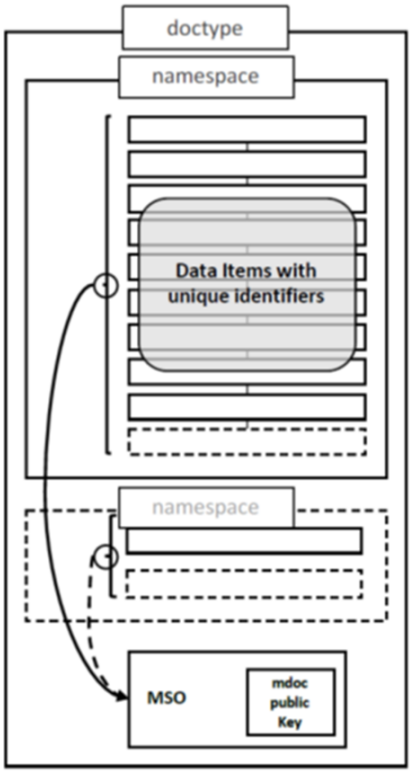

Figure C.2 - mdoc data model (source: contribution to ISO/IEC 18013-5)

C.3.2 Device retrieval method

ISO/IEC 18013 specifies CBOR encoded **mdoc request** and **mdoc response** messages for the so-called device retrieval method. These messages are exchanged encrypted, see Clause B.4.1 Session encryption below. For details see ISO/IEC 18013-5 Clause 8.3.2.1.

C.3.2.1 mdoc request

By means of an mdoc request, an mdoc reader / verifier can ask for data elements from different documents. The documents are identified by their doctypes and the data elements of a doctype by the combination of namespaces and element identifiers within these namespaces.

For each requested data element in the mdoc request the mdoc reader / verifier needs to indicate by means of the **IntentToRetain** variable whether it intends to retain the received data element. The verifier will not retain any data, including digests and signatures, or derived data received from the mdoc, except for data elements for which the IntentToRetain flag was set to true in the request. To retain is defined as "to store for a period longer than necessary to conduct the transaction in realtime".

An optional feature in the mdoc request message is the authentication of the mdoc reader and the mdoc request message (called **mdoc reader authentication** in ISO/IEC 18013-5), see Clause B.4.4 mdoc reader authentication below.

C.3.2.2 mdoc response

By means of an mdoc response message data elements from different namespaces from different documents can be returned to the mdoc reader. This message is also used to authenticate the data elements read, see Clause B.4.2 Issuer data authentication, and the mdoc itself, see Clause B.4.3 mdoc

authentication. As part of this mdoc authentication the mdoc may sign certain data elements that are not subject to issuer data authentication.

C.3.3 Server retrieval method

Similarly to the device retrieval, ISO/IEC 18013-5 mdoc request and response messages can be used for the server retrieval method (WebAPI). The OpenID Connect protocol can also be used.

For the server retrieval the mdoc reader needs to retrieve the issuing authority address as well as an authorization token from the mdoc first. This server retrieval token identifies the mdoc holder and the mdoc to the issuing authority infrastructure and should be a one-time token with a short validity period.

For the server retrieval security mechanisms see Clause B.5.

C.4 Security mechanisms

ISO/IEC 18013-5 specifies the following security mechanisms for the device retrieval method:

- **Session encryption**, i.e. encryption of the mdoc request and response messages
- **Issuer data authentication** which proves that the data is authentic and has not been changed
- **mdoc authentication**: authentication of the mdoc to the mdoc reader
- **mdoc reader authentication**: authentication of the mdoc reader to the mdoc (optional)

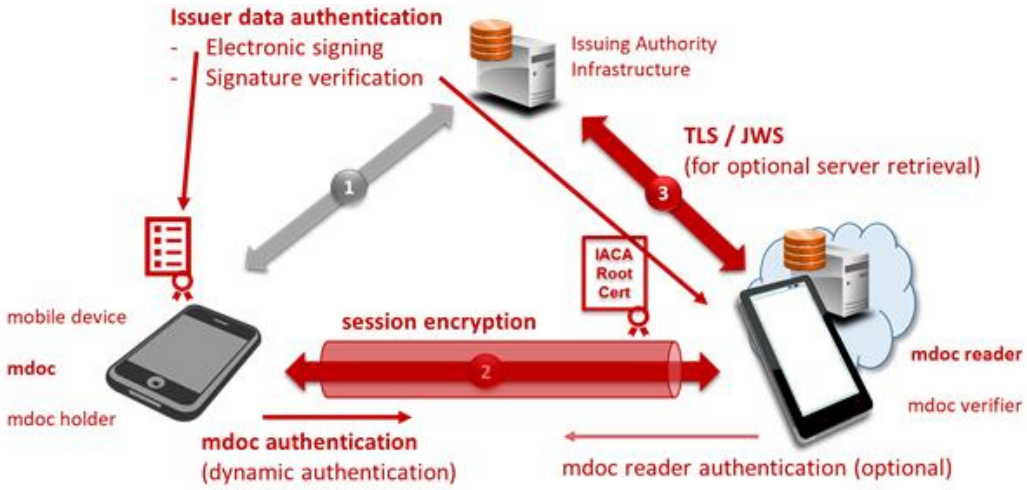

Figure C.3 - ISO/IEC 18013-5 mdoc security protocols

ISO/IEC 18013-5 specifies a set of cryptographic algorithms (called **cipher suite 1**) for these security mechanisms. In principle other cryptographic algorithms, i.e. another cipher suite, could be chosen.

In cipher suite 1 the following keys are used for these security mechanisms (without issuer data authentication):

- **EDeviceKey.Priv, EDeviceKey.Pub**: mdoc ephemeral EC key pair used for the session encryption mechanisms
- **EReaderKey.Priv, EReaderKey.Pub**: mdoc reader ephemeral EC key pair used for the session encryption mechanisms and the mdoc authentication with a MAC
- **SKReader, SKDevice**: AES 256 session keys used by the mdoc and mdoc reader for session encryption
- **SDeviceKey.Priv, SDeviceKey.Pub**: mdoc static EC key pair used for mdoc authentication

- mdoc reader static EC key pair for the optional mdoc reader authentication

Table C. lists the elliptic curves supported for ECDH, ECDSA and EdDSA in cipher suite 1.

Table C.1 - Elliptic curves for cipher suite 1 (source ISO/IEC 18013-5)

Definition	Specification	Curve identifier	Purpose
Curve P-256	FIPS PUB 186-4	IANA COSE registry	ECDH/ECDSA
Curve P-384	FIPS PUB 186-4	IANA COSE registry	ECDH/ECDSA
Curve P-521	FIPS PUB 186-4	IANA COSE registry	ECDH/ECDSA
X25519	RFC 7748	IANA COSE registry	ECDH
X448	RFC 7748	IANA COSE registry	ECDH
Ed25519	RFC 8032	IANA COSE registry	EdDSA
Ed448	RFC 8032	IANA COSE registry	EdDSA
brainpoolP256r1	RFC 5639	IANA COSE registry	ECDH/ECDSA
brainpoolP320r1	RFC 5639	IANA COSE registry	ECDH/ECDSA
brainpoolP384r1	RFC 5639	IANA COSE registry	ECDH/ECDSA
brainpoolP512r1	RFC 5639	IANA COSE registry	ECDH/ECDSA

Please note that CBOR data structures are used for the encoding of signatures, MACs, keys etc.

Figure C.4 provides an overview of the exchanged messages and the corresponding security mechanisms.

C.4.1 Session encryption

For session encryption the mdoc and the mdoc reader perform an ECKA-DH (Elliptic Curve Key Agreement Algorithm – Diffie-Hellman) to derive two session keys SKReader and SKDevice for AES-256-GCM encryption:

- The mdoc generates an ephemeral key pair (EDeviceKey.Priv, EDeviceKey.Pub) and provides the public key, curve identifier and information about the supported cipher suite during device engagement to the mdoc reader.
- The mdoc reader generates an ephemeral key pair (EReaderKey.Priv, EReaderKey.Pub) using the identified elliptic curve, performs ECKA-DH and derives the two session keys. The mdoc reader encrypts its mdoc request message using SKReader and sends the encrypted message together with EReaderKey.Pub to the mdoc (session establishment message).
- The mdoc performs ECKA-DH, derives the two session keys, decrypts the encrypted mdoc request using SKReader and encrypts its mdoc response using SKDevice (session data message).
- The mdoc reader decrypts the encrypted mdoc response using SKDevice.
- Exchange of further encrypted messages.

For details see ISO/IEC 18013-5 Clause 9.1.1.

C.4.2 Issuer data authentication

For issuer data authentication the issuer generates a digital signature over the **mobile security object (MSO)**. The MSO is a CBOR encoded data structure which contains:

- for every data element of the document a digest value calculated over the data element itself and an unpredictable random or pseudorandom value (to ensure that the digest value by itself does not provide any information about its contents);
- the public key SDeviceKey.Pub and information related to the corresponding key pair used for the mdoc authentication;
- validity information related to the validity of the MSO and its signature (not the document itself):
  - date and time of signature creation,
  - validity period,
  - optional: a timestamp at which the issuer expects to re-sign the MSO (and potentially update data elements);
- version information, the doctype, information on the hash algorithm used.

Supported hash algorithms are SHA-256, SHA-384, and SHA-512; for the supported signature algorithms and curves see Table C.2.

Table *C.2* - Algorithms and curves for issuer data authentication, mdoc ECDSA/EdDSA authentication, and mdoc reader authentication

Signature algorithm	Curves
ECDSA with SHA-256	P-256, brainpoolP256r1
ECDSA with SHA-384	P-384, brainpoolP320r1, brainpoolP384r1
ECDSA with SHA-512	P-521, brainpoolP512r1
EdDSA	Ed25519, Ed448

Algorithms and curves for issuer data authentication, mdoc ECDSA/EdDSA authentication, and mdoc reader authentication

For details see ISO/IEC 18013-5 Clause 9.1.2.4.

C.4.3 mdoc authentication

For the authentication of the mdoc itself and the mdoc response message the mdoc uses the EC key pair (SDeviceKey.Priv, SDeviceKey.Pub). As the MSO contains the public key SDeviceKey.Pub, the public key is subject to issuer data authentication, see above.

For the mdoc authentication the mdoc calculates a MAC (see mdoc MAC authentication below) or an ECDSA / EdDSA signature (see mdoc ECDSA / EdDSA authentication below) using as input the

- device engagement including any handover messages,
- the reader public key EReaderKey.Pub used in session encryption,
- the doctype of the mdoc response,
- data elements returned in the mdoc response messages, which are not directly subject to issuer data authentication (device signed data elements; e.g. mdoc generated authorization tokens for certain services).

NOTE: The MSO encodes the authorization of the mdoc authentication key to sign / MAC certain data elements.

For details see ISO/IEC 18013-5 Clause 9.1.3.

C.4.3.1 mdoc MAC Authentication

To calculate the ephemeral MAC key, the mdoc and the mdoc reader perform ECKA-DH (Elliptic Curve Key Agreement Algorithm – Diffie-Hellman) using the SDeviceKey.Priv and EReaderKey.Pub for the mdoc and EReaderKey.Priv and SDeviceKey.Pub for the mdoc reader. The ephemeral MAC key is derived from the shared secret and the MAC is calculated using HMAC with SHA-256.

C.4.3.2 mdoc ECDSA / EdDSA Authentication

The mdoc signs the device authentication data with the mdoc authentication private key. See Table C.2 for the supported algorithms and curves.

C.4.4 mdoc reader authentication

A private key stored in the mdoc reader is used to authenticate the mdoc reader and the mdoc request. A certificate containing the mdoc reader public key is sent to the mdoc within the mdoc request message. The format of this certificate is not prescribed in ISO/IEC 18013-5, but the standard specifies a recommended X.509 certificate profile.

For this authentication the mdoc reader calculates an ECDSA / EdDSA signature, see Table C.2 for the specified cryptographic algorithms, using as input the device engagement including any handover messages and the ephemeral reader public key EReaderKey.Pub used in session encryption, see above.

For details see ISO/IEC 18013-5 Clause 9.1.4.

C.5 Server retrieval security mechanisms

For server retrieval standard security mechanisms are re-used, for details see ISO/IEC 18013-5 Clause 9.2:

- Transport Layer Security (TLS) for the authentication of the issuing authority infrastructure and optionally the mdoc reader as well as session encryption;
- JSON Web Signatures for the authentication of the data.

Communication between the mdoc reader and the issuing authority infrastructure will use TLS version 1.2 (support mandatory) or version 1.3 (support optional). While the TLS server authentication of the issuing authority infrastructure is mandatory, the TLS client authentication of the mdoc reader is optional. The usage of the following cipher suites is specified:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (support mandatory)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (support mandatory)
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (support recommended)

The issuing authority infrastructure will sign the response data using one1 of the following JSON Web Algorithms:

- ES256: ECDSA using Curve P-256 and SHA-256
- ES384: ECDSA using Curve P-384 and SHA-384
- ES512: ECDSA using Curve P-521 and SHA-512

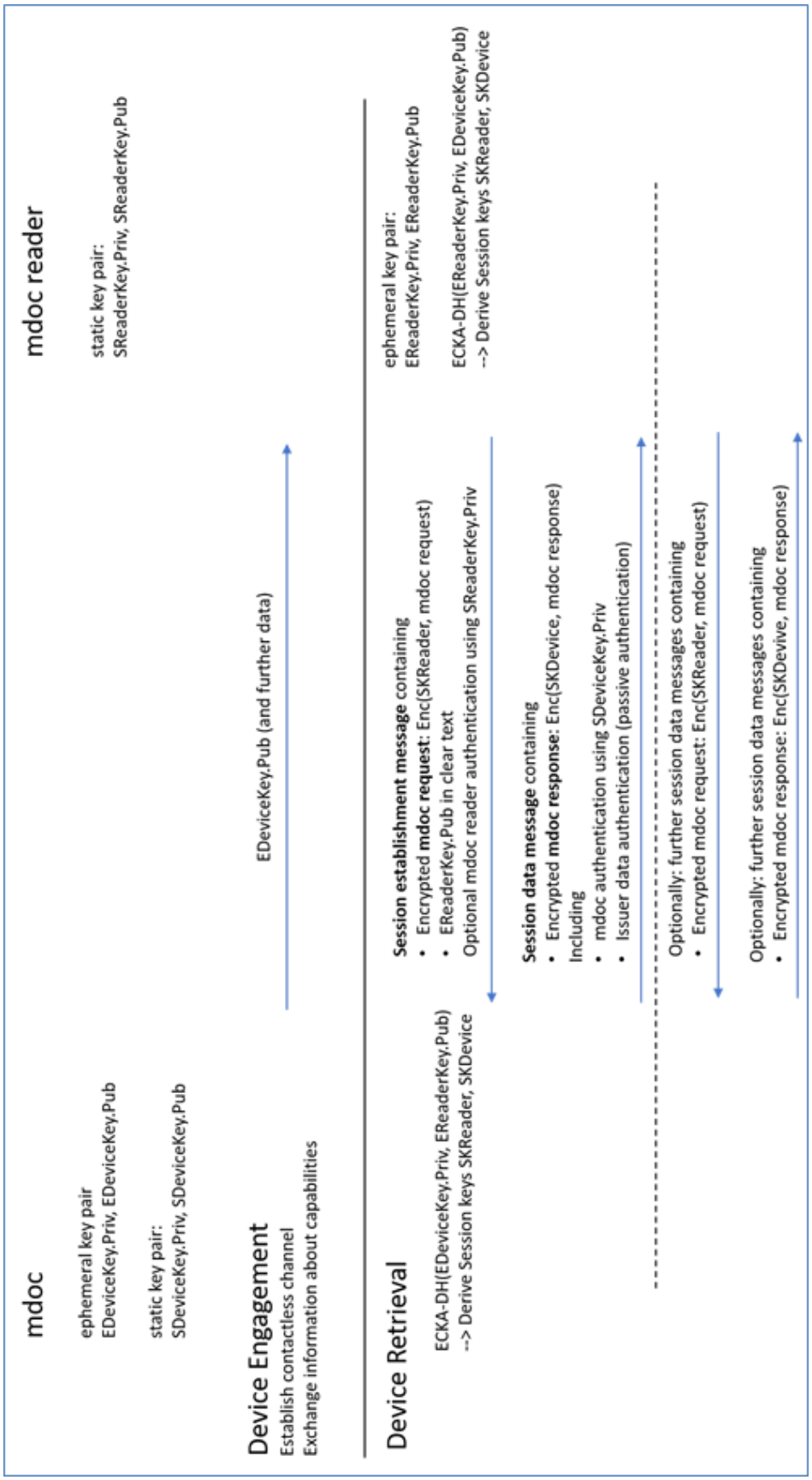

Figure C.4 - mdoc device retrieval overview

Annex D

ISO/IEC 18013-5 standardization

D.1 Contributors to ISO/IEC 18013-5

ISO/IEC 18013-5 has been developed in ISO/IEC JTC1/SC17 (cards and security devices for personal identification) work group 10/task force 14 (mobile driving licence). This task force includes a diverse group of people employed by driving licence issuers, such as government organizations from Australasia, Europe, Japan and the United States; relying parties, such as retail, financial services, government organizations and law enforcement; academia: security and privacy researchers; the identity technology industry; the mobile computing industry, such as operating system (OS) and handset providers. Experts actively participating in the development of the international standard represent their national standardisation bodies, which include:

- AFNOR, France
- ANSI, United States
- ASI, Austria
- BSI, United Kingdom
- DIN, Germany
- DSM, Malaysia
- IPQ, Portugal
- JISC, Japan
- KATS, Korea
- NBN, Belgium
- NEN, the Netherlands
- SA, Australia
- SABS, South Africa
- SAC, China
- SCC, Canada
- SFS, Finland
- SII, Israel
- SIS, Sweden
- SIST, Slovenia
- SNV, Switzerland
- UNMZ, Czech Republic

D.2 Vetting, testing and proving the standard

The ISO/IEC 18013-5 standard has been vetted through ISO's extensive balloting and review processes. In addition, members of the ISO task force have held a number of international interoperability test events in 2018 (Japan) and 2019 (USA and Australia).

Figure C.1 - 2019 interoperability test event,
featuring 30 implementations from all over the world

These events were coordinated by UL's Identity Management and Security division, and endorsed by the American Association of Motor Vehicle Administrators (AAMVA), Austroads, the European association of driver and vehicle registration authorities (EReg) and the UTMS Society of Japan.

Due to the pandemic, a planned interoperability test event in Europe (The Hague, 2020) was postponed. In the meantime, several implementations have passed conformity testing.

New interoperability test events are planned for October 2021 (EU), and November 2021 (USA).

D.3 Generalisation of ISO/IEC 18013-5 for mobile credentials

ISO/IEC 18013-5 has been adopted by ISO/IEC JTC1/SC17/WG4 (generic interfaces and protocols for security devices) as the basis for ISO/IEC 23220 (building blocks for identity management via mobile devices) - part 4 (protocols and services for the operational phase).

Bibliography

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

[2] ISO/IEC TS 23220-4, *Building blocks for identity management via mobile devices— Part 4: Protocols and services in the operational phase* (in preparation)

[3] WHO International Certificate of Vaccination or Prophylaxis, 2005;

[4] WHO, Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021;

[5] WHO, Digital Documentation of COVID-19 Certificates: Vaccination Status – Web Annex A. DDCC:VS core data dictionary, 27 August 2021;

[6] eHealth Network Guidelines on Technical Specifications for Digital COVID Certificates, Volume 1, V1.0.5, 2021-04-21;

[7] eHealth Network Guidelines on Value Sets for Digital COVID Certificates, Version 1.2, 2021-07-07;

[8] eHealth Network Guidelines on Technical Specifications for Digital COVID Certificates, JSON Schema Specification, Version 1.3.0, 2021-06-09.