ISO/IEC 18013-5 mdoc for eHealth

Internationally standardized protocols for vaccination certificates

Version 1.0, 16 March 2021

Contributors: 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, Bundesdrueckerei, DE; Gilles Roux, Google, US

Abstract: vaccination certificates are proposed as an instrument to recover society from the Coronavirus pandemic. Several technology propositions are 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 5 years, a task force under ISO/IEC JTC1/SC17 (security devices for personal identification) 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. Being originally initiated as a standard for mobile driving licence, it can be applied for vaccination credentials, addressing complex security and privacy issues, such as binding a holder to a credential, binding a credential to a mobile device, data minimisation (selective data release), and offline operation (non-traceability; availability, even if holder and verifier are without internet connectivity). The authors of this paper (a selection of the ISO/IEC task force members) believe that vaccination certificates can benefit from those technologies. This paper provides an introduction to the ISO/IEC 18013-5 mdoc concept, and provides an example how this concept can support vaccination and COVID-19 recovery certificates, based on the WHO *International Certificate of Vaccination or Prophylaxis*, eHealth Network *Guidelines on verifiable vaccination certificates - basic interoperability elements, Release 2, 2021-03-12* and *Guidelines on COVID-19 citizen recovery interoperable certificates - minimum dataset, Release 1, 2021-03-15*. In addition to the translation of this work into a mobile international certificate of vaccination (micov) doctype and namespace for medical purposes, an example namespace is provided for “vaccination attestation”, maximizing the privacy benefits that the ISO standard offers. The contributors to this paper prepare a companion paper, discussing potential adaptations, to support paper-based credentials and to integrate with other proposed technologies,

Why this paper?

Vaccination against Covid-19 is a key enabler for the world to get back on its feet in the midst of a devastating pandemic. Accurate vaccination information helps manage public health. And the pros and cons of “vaccination and test passports” are being debated: proof of vaccinations or negative tests to enable convening larger gatherings safely.

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

Whether for conveying medical details, or for attestation, during the actual use of vaccination certificates, there should be no doubt to whom the data pertains. Uncertainty about the holder could lead to incorrect medical or safety related decisions. As a result, technology enabling the operational use of vaccination certificates should facilitate verification of the **identity** of the holder of such 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 5 years, ISO/IEC has developed a standard that addresses a number of issues that, to our knowledge, are yet to be addressed by, and complementary to, existing approaches for vaccination certificates: ISO/IEC 18013-5. Although developed for "mobile Driving Licence", the protocols in this standard have been explicitly designed to be usable for other types of documents (health cards, vehicle registration cards, etc.). The standard is nearing publication, 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 allows data models for identity credentials/ attributes/ authorizations 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*, and 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, practicing **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 wireless communication** channel, and subsequent data exchange, including structured request and response messages;
- **identification** of the mdoc holder (**user binding**);
- selective release of *mdoc data elements* by the *mdoc holder* (**data minimisation**);
- a protocol to retrieve mdoc data from the mobile device of the mdoc holder (*device retrieval*, **purely offline**, facilitating **availability** and **non-traceability**);
- a protocol to optionally retrieve mdoc data from the issuing authority (*server retrieval*, in case the mdoc data does not reside on the mobile device);
- a mechanism by which an mdoc reader establishes that the mdoc was truly issued by a valid issuing authority, and unchanged (**issuer data authentication**);
- a mechanism by which an mdoc reader establishes that the mdoc is bound to the device on which it is resident (*mdoc authentication***, device binding**)

Scope

In this paper, we introduce the ISO/IEC 18013-5 mdoc concept, and demonstrate how the standard is ready to be used for vaccination certificates, without any adaptation.

We are preparing a companion paper, in which we will present potential adaptations to the standard. In that paper, we may address

- use-cases such as an end-user presenting a paper-based credential;
- integration with technologies selected by various vaccination certificate initiatives;

We invite our audience to provide feedback to this paper, and input for the companion paper.[1]

[1] Please provide feedback at https://github.com/18013-5/micov or by email to arjan.geluk@ul.com

Introduction to the ISO/IEC 18013-5 mdoc concept

Security, privacy, and interoperability for mobile credentials

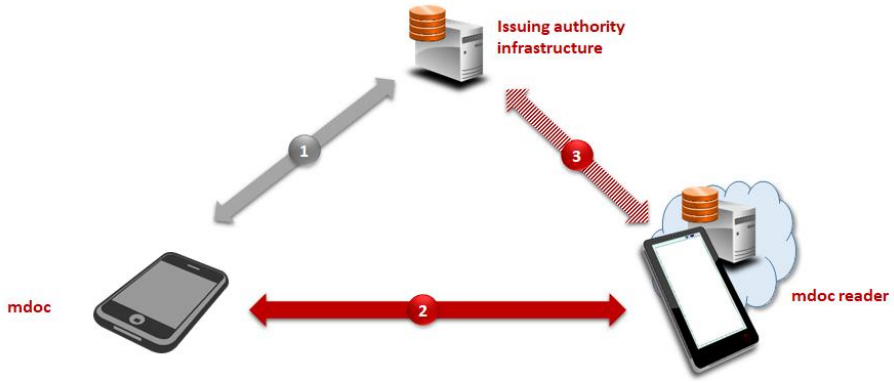
Following the trend toward contactless and mobile interactions set by the payment sector, driving licence issuers around the world are preparing for the introduction of a mobile driving licence and similar types of mobile documents.

To facilitate **secure**, **privacy-preserving** and **globally interoperable** mobile credentials, stakeholders from around the world (See Annex C for details) have collaborated to develop an international standard with protocols for mobile documents (mdocs). The result: 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, yet more privacy preserving (as it supports selective disclosure), and **available offline** (i.e. even if neither the holder nor the verifier of the credential has internet connectivity, facilitating non-traceability).

A critical difference between a physical document and an mdoc is that the latter is verified electronically and cryptographically. A verifier uses an mdoc reader (app) to obtain mdoc data from the mdoc through secure wireless communication.

mdoc interfaces

Figure 1 shows the interfaces in scope of the standard:



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

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

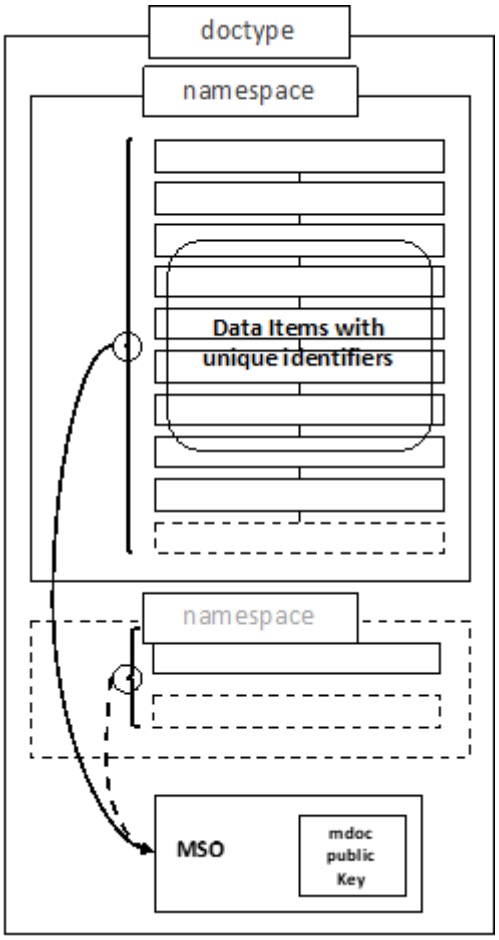
Interface 3: mdoc reader ↔ issuing authority infrastructure. This optional interface can be used to retrieve mdoc data, in case the mdoc data does not reside on the mobile device.

mdoc functional requirements

Key stakeholders (issuers, verifiers) provided the ISO/IEC work group the following minimum functional requirements, to be enabled in a standard for mdocs:

- an mdoc verifier with an mdoc reader shall 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** shall be able to verify the integrity and authenticity of the mdoc
- the mdoc verifier shall be able to **confirm the binding** between the person presenting the mdoc and the person identified in the mdoc (mdoc holder)
- the interface between the mdoc and the mdoc reader shall support the **selective release** of mdoc data to an mdoc reader

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.

mdoc data is organized as individual **data elements** which 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) hash values for at least 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.

Trust model

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

At transaction time, the mdoc shares (1) at least one data element together with a digestID, which identifies the applicable hash value in the MSO, and (2) the MSO, which includes the document signer public key certificate (or an X.509 certificate chain in case the mdoc is trusted under a multi-level PKI).

The mdoc reader obtains the Issuing authority CA public key (or highest CA in case of a multi-level PKI) 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.

ISO/IEC 18013-5 facilitates situations in which the ecosystem is not subject to a “super-CA” for the whole ecosystem or applicative domain. 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 organizations.

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) introduce driving licence and vehicle registration mdocs. Since Android 11, Google made the Android IdentityCredentialAPI available, which implements ISO/IEC 18013-5, facilitating uniform **hardware security** for mdoc.

ISO/IEC 18013-5 mdoc for vaccination certificates

Existing harmonization: international certificate of vaccination

The International Certificate of Vaccination or Prophylaxis, 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.

Applying ISO/IEC 18013-5 in support of WHO, eHealth Network

As described above, ISO/IEC 18013-5 allows existing data models for identity credentials/ attributes 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 rather 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 vaccination certificate as a basis for a doctype and namespace: **mobile international certificate of vaccination (micov)**.

To demonstrate the extensibility of this approach, we added the basic interoperability elements defined in the ***eHealth Network Guidelines*** *on proof of vaccination for medical purposes* to the "*micov.medical*" namespace.

Privacy-preserving attestation of vaccination/ test/ recovery

To provide strong, yet privacy-preserving proof that an mdoc holder has been vaccinated, or has obtained a negative test result, ISO/IEC 18013-5 provides an attestation mechanism which can be used.

To support attestation that, for any specified 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,

a "*micov.attestation*" namespace has been added, supplementing the medical namespace.

The namespace definitions are presented in Annex A.

Annex A - certificate of vaccination mdoc

A.1 Basis for this namespace proposal

Namespace proposal for a mobile international certificate of vaccination (micov), based on

- International Certificate of Vaccination or Prophylaxis, International Health Regulations (2005), World Health Organization (WHO), (online), https://www.who.int/ihr/IVC200_06_26.pdf?ua=1
- Guidelines on verifiable vaccination certificates - basic interoperability elements, Release 2 (2021-03-12), eHealth Network (eHN VVC), (online), https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

While this namespace proposal is suited to represent vaccination information regarding any disease, the namespace proposal is expanded to support specific proof of immunisation after recovery from COVID-19, according to:

- Guidelines on COVID-19 citizen recovery interoperable certificates - minimum dataset, Release 1 (2021-03-15), eHealth Network (eHN RIC), (online), https://ec.europa.eu/health/sites/health/files/ehealth/docs/citizen_recovery-interoperable-certificates_en.pdf

The WHO published a harmonized international certificate of vaccination or prophylaxis, based on international health regulation in 2005. 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 dataset defined in the eHN VVC publication largely overlaps with the data contained in the internationally regulated WHO Certificate of Vaccination or Prophylaxis. In addition to the Vaccination/Prophylaxis information and Person identification, it provides more options for binding the certificate to the identity of the vaccinated person, and it provides certificate metadata.

More binding options to the identity of the vaccinated person

While the WHO provides linking the vaccination information to a passport/travel document and optionally a national identification document, the eHN enables linking the vaccination information to more identifiers pertaining to the vaccinated person.

Certificate metadata

On top of the information pertaining to individual vaccinations, the eHN publication provides for metadata pertaining to the overall certificate, such as certificate issuer, and validity period of the certificate (rather than validity of the individual vaccinations only).

A.2 Doctype and namespace

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

mobile international certificate of vaccination (micov) - doctype

```
doctype: org.micov.1
```

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

mobile international certificate of vaccination (micov) - namespaces

```
namespace: org.micov.medical.1
namespace: org.micov.attestation.1
```

A.2.1 namespace: org.micov.medical.1

Verifiable vaccination certificate data elements

```
IDENTIFIER : FORMAT                 ; DESCRIPTION

Person Identification (minimum dataset)

"last_name" : tstr,                 ; the legal last name(s) of the vaccinated person.
"given_name" : tstr,                ; the legal given name(s) of the vaccinated person.
"birth_date" : full-date            ; full-date string as specified in RFC 3339.
*"PersonId_[x]" : PersonId_[x]      ; idenfitier of the vaccinated person, according to the
                                    ; policies applicable in each country. It should be
                                    ; captured what type of identifier is used. Examples:
                                    ; citizen ID card or identifier within the health
                                    ; system/IIC/e-registry.
?"sex" : uint,                      ; Administrative gender. Values as defined in ISO/IEC 5218.

PersonId_[x] =                      ; [x] to encode the type of PersonId (e.g. "PersonId_pp"
                                    ; for passport, "PersonId_nic" for national ID card,
                                    ; "PersonId_dl" for driving licence, PersonId_csn for
                                    ; citizen service number, PersonId_nhs for national health
                                    ; service, etc.
{
  "PersonIdNumber" : tstr,          ; unique number for the PersonIdType/PersonIdIS/PersonIdIA
                                    ; combination
  "PersonIdType" : tstr,            ; type of person identifier (may be further harmonised,
                                    ; e.g. "pp"for passport, "nic" for national ID card, "dl"
                                    ; for driving licence, "csn" for citizen service number, …)
  "PersonIdIS" : tstr,              ; Issuing State of the PersonIdType.
 ?"PersonIdIA" : tstr               ; Issuing Authority of the PersonIdType (conditional;
                                    ; mandatory if the PersonIdNumber is not guaranteed unique
                                    ; for the combination of the PersonIdType and PersonIdIS)
}

Vaccination / prophylaxis information (minimum dataset)

"VPInfo_[ICD-10_PN]_[n]" = VPInfo   ; data element identifier includes [ICD-10 Preferred Name]
                                    ; and the [number] of the dose, e.g. "VPInfo_COVID-19_1",
                                    ; "VPInfo_COVID-19_2", "VPInfo_YellowFever_1"

VPInfo =
{
```

```
 ?"VaccDiseaseAgent" : tstr,       ; disease or agent that the vaccination provides protection
                                   ; against. (format: ICD-10 preferred name)
  "VaccineProphylaxis": tstr,      ; Generic description of the vaccine/prophylaxis or its
                                   ; component(s)
  "VaccMedicinalProd" : tstr,      ; medicinal product name, as registered in the country
  "VaccMktAuthHolder" : tstr,      ; vaccine marketing authorisation holder or vaccine
                                   ; manufacturer, e.g. Pfizer BioNTech
  "VaccDoseNumber: tstr,           ; Number in a series of vaccinations/doses; order in
                                   ; vaccination course, e.g. "2/2" for "VPInfo_COVID-19_2"
                                   ; or "1/1" for "VPInfo_YellowFever_1"
 ?"VaccBatchLotNumber" : tstr,     ; A distinctive combination of numbers and/or letters
                                   ; which specifically identifies a batch
  "VaccAdmDate" : full-date,       ; Date of vaccination
 ?"VaccAdmCentre" : tstr,          ; Name/code of administering centre or a health authority
                                   ; responsible for the vaccination event
 ?"VaccHealthProfId" : tstr,       ; Name or health professional code responsible for
                                   ; administering the vaccine or prophylaxis
  "VaccCountry" : tstr,            ; ISO 3166 country code; The country in which the
                                   ; individual has been vaccinated
 ?"VaccNextDate" : full-date,      ; Date on(by?) which the next vaccination should be
                                   ; administered

                                   ; the following elements have been added to enable
                                   ; reflecting a validity period on individual vaccination
                                   ; level, conform the WHO International Certificate of
                                   ; Vaccination or Prophylaxis
 ?"VaccProtDuration" : tstr,       ; duration of protection (e.g. "10 years" for DTP vaccin)
 ?"VaccValidFrom" : full-date,     ; start of validity of the vaccination (e.g. 10 days after
                                   ; administering a Yellow Fever vaccine)
 ?"VaccValidUntil" : full-date     ; end of validity of the vaccination
}
```

Certificate meta-data

```
"CertIssuer" : tstr                ; Entity that has issued the certificate
"CertId" : tstr                    ; Unique identifier of the certificate (UVCI), the unique
                                   ; identifier can be included in the IIS
?"CertValidFrom" : full-date       ; start of validity of the certificate
?"CertValidUntil" : full-date      ; end of validity of the certificate
?"CertSchemaVersion" : tstr        ; Version of the dataset definition - currently set at
                                   ; 1.0.0
```

Citizen recovery certificate data elements

Note: this section contains additional data elements for information about past infection. Citizen recovery certificates reuse Person Identification and Certificate Metadata elements from the Verifiable Vaccination Certificate

Information about past infection

```
"RecovDiseaseAgent" : tstr,         ; Disease or agent the citizen has recovered from
"FirstPosTest" : PosTest            ; Date when the sample for the test was collected that
                                    ; led to positive test obtained through a procedure
                                    ; established by a public health authority in the country

"PosTest" =
{
  "posResult" : bool                ; (true/false)
 ?"TypeOfTest" : tstr               ; e.g. PCR test
  "TestDate" : full-date            ; Complete date, without time
  "TestCountry" : tstr,             ; ISO 3166 country code; The country in which the first
                                    ; positive test was performed
}
```

A.2.2 Namespace: org.micov.attestation.1

This namespace supports attestation that, for any specified disease (as identified by the ICD-10 preferred name), the mdoc holder:

- has been vaccinated;
- has recovered (and is considered immune);
- has obtained a negative test result;
- fulfils set requirements for safe entry.

For binding the attestation/claim to the holder, optional identity attributes are provided for selective release, incl. face image, initials, and elements of the holder's date of birth.

```
IDENTIFIER : FORMAT                  ; DESCRIPTION

Attestation/Claims

?"[ICD-10_PN]_vaccinated" : bool     ; (true/false) The ISO/IEC 18013-5 mechanism for age
                                     ; attestation (Age_over_N) can be used to
                                     ; attest that the holder of the mdoc has been vaccinated

?"[ICD-10_PN]_recovered" : Recovered; attest that the holder has recovered (considered immune)

"Recovered" =
{
  "RecovDiseaseAgent" : tstr,        ; Disease or agent the citizen has recovered from
  "FirstPosTest" : PosTest           ; Date when the sample for the test was collected that
                                     ; led to positive test obtained through a procedure
                                     ; established by a public health authority in the country
}

"PosTest" =
{
  "posResult" : bool                 ; (true/false)
 ?"TypeOfTest" : tstr                ; e.g. PCR test
  "TestDate" : full-date             ; Complete date, without time
 ?"TestCountry" : tstr,              ; ISO 3166 country code; The country in which the first
                                     ; positive test was performed
}

?"[ICD-10_PN]_negTest" : NegTest     ; attest that the holder obtained a negative test result

"NegTest" =
{
  "negResult" : bool                 ; (true/false)
 ?"TypeOfTest" : tstr                ; e.g. PCR test
  "TimeOfTest" : tdate               ; consider rounding to the hour in the interest of privacy
                                     ; preservation
}

?"[ICD-10_PN]_safeEntry" : SafeEntry; attest that the holder fulfils set requirements for
                                     ; safe entry (without disclosing whether that is based on
                                     ; vaccination, recovery or negative test)
"SafeEntry" =
{
  "SeCondFulfilled" : bool           ; (true/false)
 ?"SeCondType" : tstr                ; placeholder to determine different sets of conditions,
                                     ; e.g. safe to fly, safe to party, etc.
  "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)
}

Attributes for identity binding
```

```
?"face_image" : bstr                ; encoding: JPEG or JPEG2000 - enabling attestation in
                                    ; combination with a [ICD-10_PN]_vaccinated/recovered/
                                    ; negTest/safeEntry attestation element to confirm binding
                                    ; of that attestation to the holder.
                                    ; Alternatively,an mdoc reader could request a
                                    ; PersonId_[x] element to subsequently confirm the
binding
                                    ; of the holder to that person identifier.

?"last_name_initial" : tstr         ; supports attestation using partial ID information
?"given_name_initial" : tstr        ; supports attestation using partial ID information
?"birth_year" : uint                ; yyyy - supports attestation using partial ID information
?"birth_month" : uint               ; supports attestation using partial ID information
?"birth_day" : uint                 ; supports attestation using partial ID information
```

A.2.3 Coding provisions

Within these namespaces, only data elements defined in the following namespace definitions may be used. Source for a number of data element definitions and coding examples is the eHealth Network interoperability guidelines document.

- The "IDENTIFIER" column 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).
- The presence of the element is mandatory, except when preceded by a “?” (optional) or “*” (zero or more instances).
  NOTE: Mandatory presence does not mean that granting access for these elements to an mdoc reader is mandatory.
- The “FORMAT” column 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 7049 Section 2.4.1, 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 shall 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 7049, Section 4.1.

Annex B - Technical overview of ISO/IEC 18013-5

B.1 Introduction

B.1.1 General

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

B.1.2 Abbreviations

BLE	Bluetooth Low Energy
CBOR	Concise Binary Object Representation
EC	Elliptic Curve
MSO	Mobile Security Object

B.2 Overview

This ISO/IEC 18013-5 secure device retrieval mechanism allows in principle to request and read any number of data elements from different documents stored on a mobile device using just 1 request-response pair including the security mechanisms as e.g. establishing session encryption keys. Minimizing the number of necessary request-response messages has a major performance impact especially if using BLE. 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 (or Wi-Fi Aware or…) connection.

Similarly the ISO/IEC 18013-5 secure server retrieval mechanism allows to request and read any number of data elements from different documents stored in the issuing authority infrastructure using just 1 request-response pair..

B.3 Reading an mdoc

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

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

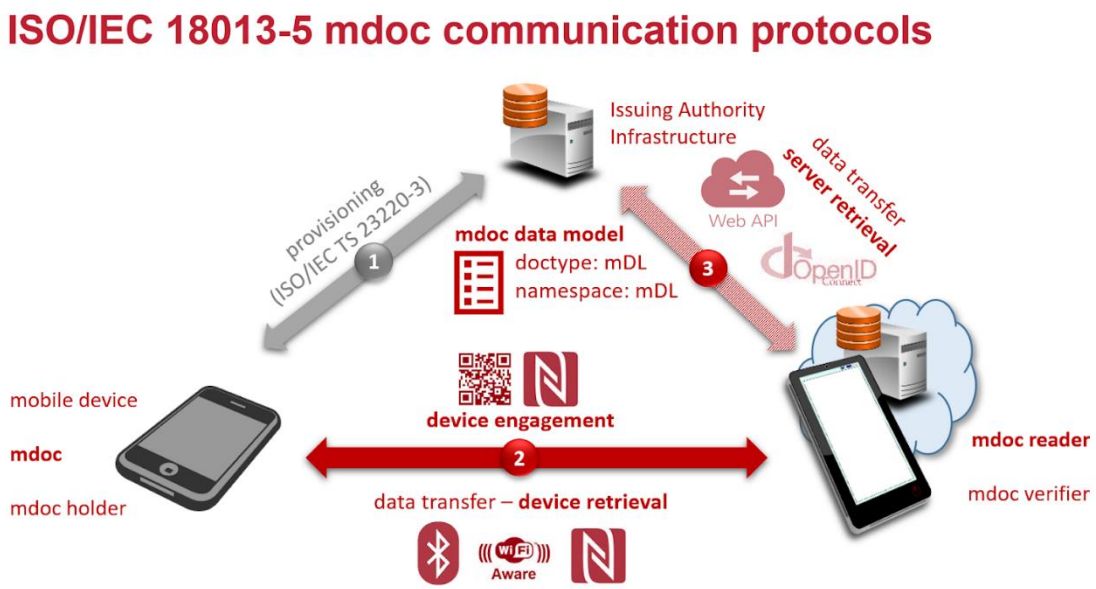
During **device engagement**, information required to setup and secure data retrieval is exchanged between the mDL and the mDL reader. Transmission technologies available to transfer the device engagement data are NFC or QR code.

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.



B.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 1 or more namespaces, see Figure B.1. 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.).

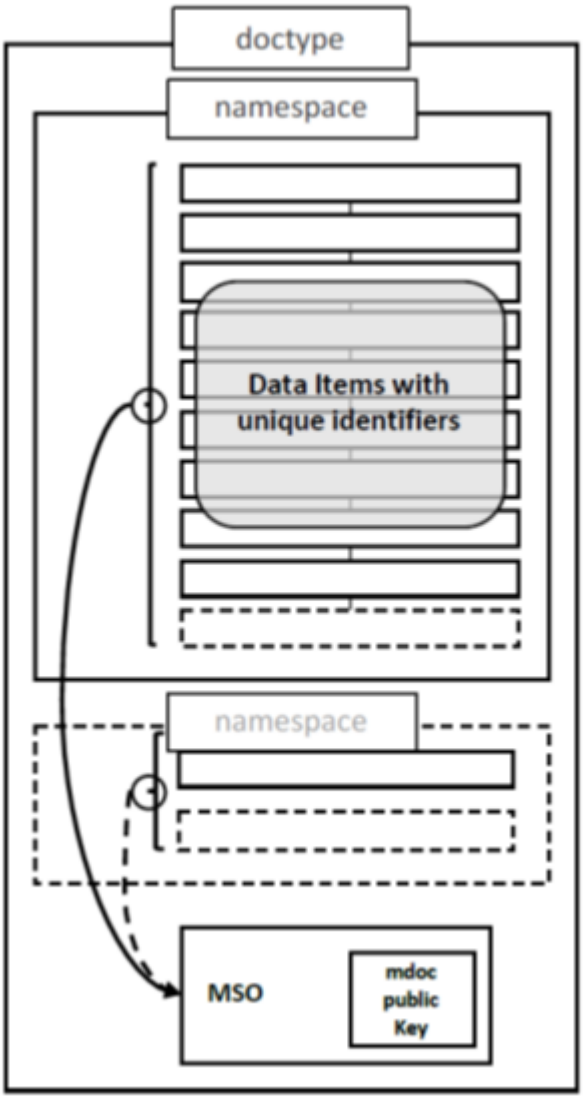


Figure B.1: mdoc data model (source: ISO/IEC 18013-5 draft)

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.

B.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.

B.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 shall 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.

B.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.

B.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.

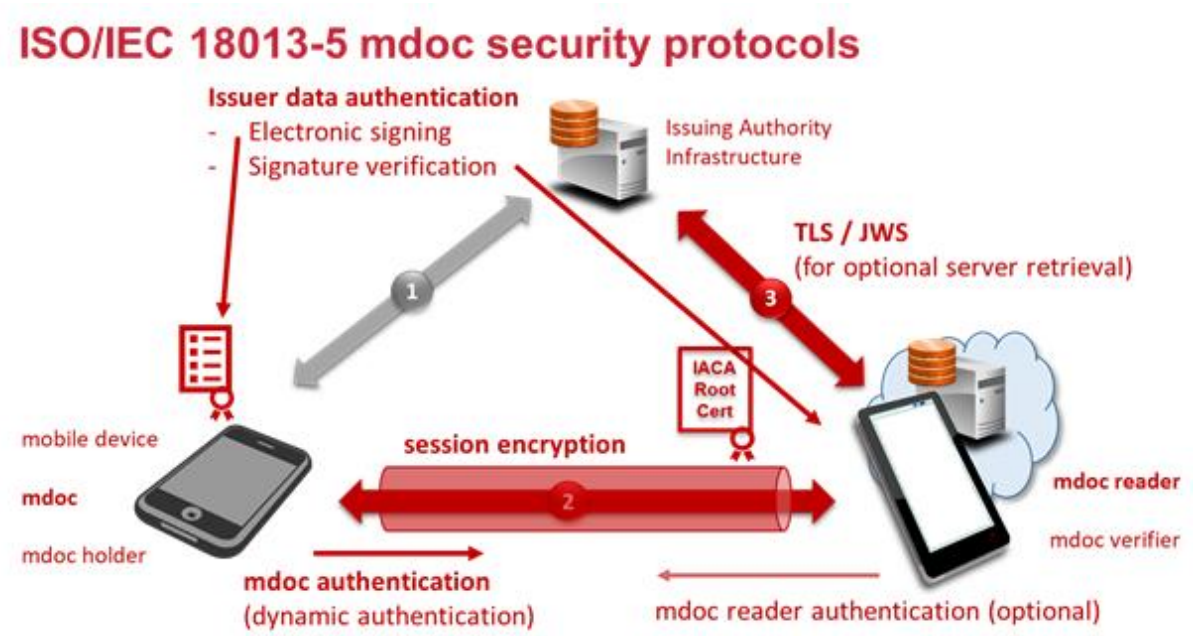
For the server retrieval the mdoc reader needs to retrieve the issuing authority address as well as an authorization token from the mdoc first. This server retrieval token identifies the mdoc holder and the mdoc to the issuing authority infrastructure and should be a one-time token with a short validity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

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

B.4 mdoc 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)



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

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 pending	ECDH/ECDSA
brainpoolP320r1	RFC 5639	IANA COSE pending	ECDH/ECDSA
brainpoolP384r1	RFC 5639	IANA COSE pending	ECDH/ECDSA
brainpoolP512r1	RFC 5639	IANA COSE pending	ECDH/ECDSA

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

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

Figure B.2 provides an overview of the exchanged messages and the corresponding security mechanisms.

B.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.

B.4.2 Issuer data authentication

For issuer data authentication the issuer generates a digital signature over the so called **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 2.

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

Table 2: 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.

B.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 (so called 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.

B.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.

B.4.3.2 mdoc ECDSA / EdDSA Authentication

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

B.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 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.

B.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 shall 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 shall 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

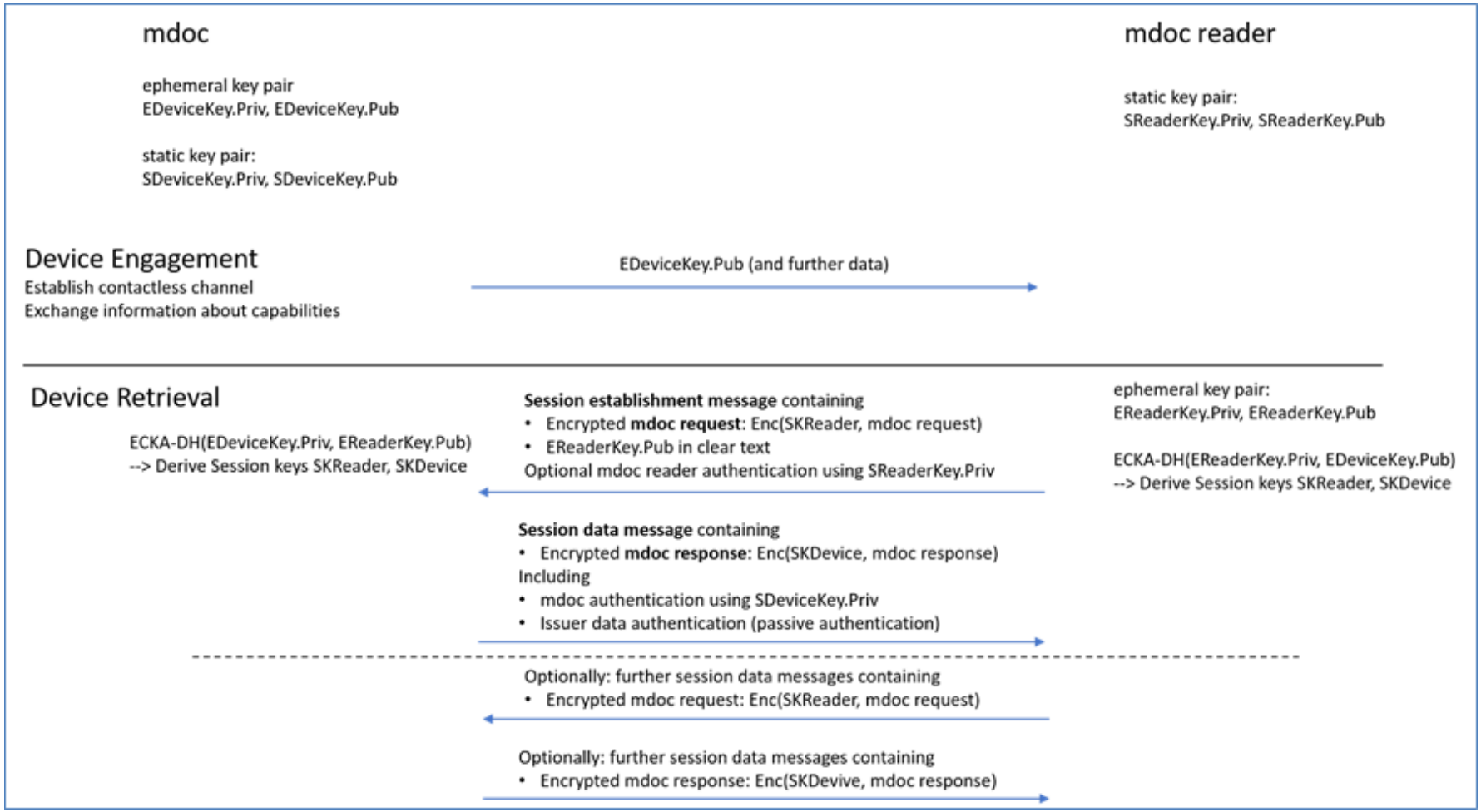


Figure B.2: Device retrieval overview

Annex C - ISO/IEC 18013-5 standardization

C.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

C.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).

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) has been postponed. In the meantime, several implementations have passed conformity testing.

C.3 generalization 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).