Technical Specification

ISO/IEC TS 23220-4

First edition
2026-04

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

Part 4: Protocols and services for operational phase

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

Partie 4: Protocoles et services pour la phase opérationnelle

Reference number
ISO/IEC TS 23220-4:2026(en)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document covers the operational phase introduced by ISO/IEC 23220-1. This document also expands on ISO/IEC 18013-5, especially regarding reader engagement, over the internet device retrieval operation and connections to other International Standards. It also expands operational data elements, such as for credential holder authentication, operations involving data elements from identical or different types of documents, and more.

Implementation conformant to ISO/IEC 18013-5 meets all requirements on selected building blocks specified in this document.

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

Part 4: Protocols and services for operational phase

1 Scope

This document specifies building blocks for the implementation of the operational phase of mobile eID systems and any other mdoc for national bodies or document-specific standards to create profiles according to their needs.

This document specifies the interface between the mdoc app and mdoc reader and the interface between the mdoc reader and the issuing authority infrastructure.

More specifically, this document defines transport protocols for various RF solutions and for over the internet. It defines the application layers, such as the request-response protocols between an mdoc app and mdoc reader and between an mdoc reader and issuing authority.

It further defines the security mechanism for issuer authentication, mdoc authentication and credential holder verification.

This document also specifies mechanisms enabling parties other than the issuing authority to:

— use a machine to obtain the mdoc data;

— bind the mdoc to the mdoc holder;

— authenticate the origin of the mdoc data;

— verify the integrity of the mdoc data.

The following items are out of scope for this document:

— provisioning of the mdoc data (this is covered by ISO/IEC TS 23220-3);

— how holder's consent to share data is obtained;

— requirements on storage of mdoc data and mdoc private keys.

Finally, it provides information to create a conformant profile.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 7816-4:2020, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

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

ISO/IEC 23220-1:2023, *Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems*

ISO/IEC TS 23220-2, *Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 2: Data objects and encoding rules for generic eID systems*

BSI TR-03111, *Elliptic Curve Cryptography (ECC)*

NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

RFC 4122:2005, *A Universally Unique IDentifier (UUID) URN Namespace*

RFC 4395, *Guidelines and Registration Procedures for New URI Schemes*

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

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

RFC 6066:2011, *Transport Layer Security (TLS) Extensions: Extension Definitions*

RFC 7515:2015, *JSON Web Signature (JWS)*

RFC 7518, *JSON Web Algorithms (JWA)*

RFC 7519:2015, *JSON Web Token (JWT)*

RFC 8152, *CBOR Object Signing and Encryption (COSE)*

RFC 8259, *JavaScript Object Notation (JSON)*

RFC 8422:2018, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*

RFC 8446:2018, *The Transport Layer Security (TLS) Protocol Version 1.3*

RFC 8610:2019, *Concise Data Definition Language (CDDL)*

RFC 8949:2020, *Concise Binary Object Representation (CBOR)*

RFC 9052, *CBOR Object Signing and Encryption (COSE): Structures and Process*

RFC 9053:2022, *CBOR Object Signing and Encryption (COSE): Initial Algorithms*

RFC 9112:2022, *HTTP/1.1*

RFC 9360, *CBOR Object Signing and Encryption (COSE)*

Bluetooth SIG, Bluetooth Core Specification, Version 5.2, December 2019

NFC Forum, CH 1.5, Connection handover technical specification

Wi-Fi Alliance, Neighbour awareness networking specification, Version 3.1

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 23220-1 and the following apply.

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

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

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

3.1
credential
set of data presented as evidence of a claimed or asserted identity and/or entitlements

Note 1 to entry: A user attribute signed by the issuer as proof of authenticity is a credential that can be verified by the verifier by validating the electronic signature.

Note 2 to entry: According to ISO/IEC 29115, an assertion is considered a stronger statement than a claim.

Note 3 to entry: Where identity is a set of attributes characteristic or property of an entity (see ISO/IEC 24760-1)

[SOURCE: ISO/IEC 29115:2013, 3.8, modified — Example added, Note 1 to entry replaced, Note 2 to entry added.]

3.2
device retrieval
process to retrieve user attribute(s) and credentials from the mdoc app

3.3
mdoc
mobile document (digital credential) issued by an issuing authority

3.4
PCD mode
mode in which a mobile device with NFC operates as a PCD

[SOURCE: ISO/IEC 14443-3:2018, 3.7, modified — The word “PXD” has been replaced with “mobile device with NFC”.]

3.5
PICC mode
mode in which a mobile device with NFC operates as a PICC

[SOURCE: ISO/IEC 14443-3:2018, 3.8, modified — The word “PXD” has been replaced with “mobile device with NFC”.]

3.6
server retrieval token
token identifying the mdoc holder and the mdoc app to the identity or attribute provider service

[SOURCE: ISO/IEC 18013-5:2021, 3.17, modified — App added after mdoc, "issuing authority" changed to the identity or attribute provider service.]

4 Symbols and abbreviations

CBOR	concise binary object representation
CDDL	concise data definition language
CHV	credential holder verification
DEM	device engagement message
DH-OVR	holder device handover
E2EE	end to end encryption between the mdoc app and a verification application
IA	issuing authority
GATT	generic attribute profile
JARM	JWT secure authorization response mode
JSON	java script object notation
JWE	JSON web encryption
JWT	JSON web token
NDEF	NFC data exchange format
NH-OVR	negotiated handover
NFC	near field communication
LoA	level of assurance
OID4VP	OpenID for verifiable presentation
RF	radio frequency
RH-OVR	reader handover

5 Overview

5.1 General

This document specifies building blocks for the implementation of the operational phase of mobile eID systems and any other mdoc for national bodies or document specific standards to create profiles according to their needs.

Annex B shall be used by national bodies or document specific standards for the specific rules to create a profile according to their needs that conforms to this document.

An example of photo ID profile is provided in Annex C.

5.2 Operational sub-phases

For the operational phase, ISO/IEC 23220-1 defines three sub-phases: initialization, engagement and communication.

Initialization is out of scope of this document. During this phase, the mdoc app and mdoc reader are activated by the holder (e.g. using the mobile UI to access the app), triggered by some events such as NFC, BLE or an

API call facilitated by the mobile OS (e.g. deep linking), or scheduled and can require holder and verifier authentication, respectively.

Engagement (see Clause 6): during this phase, the necessary information to proceed with the communication phase is exchanged between the mdoc app and mdoc reader (see 6.5) or the mobile browser invokes the mdoc app (see 6.6).

Communication: this phase starts when establishing a connection for device retrieval (see Clause 7) or server retrieval (see Clause 8) and during which the transmission channel is used for user attribute requests and user attribute retrievals.

The sub-phases are sequential and can take place over periods of time and in different locations.

A profile can define a maximum duration between sub-phases.

Figure 1 illustrates the transaction flows defined in this document for the operational phase.

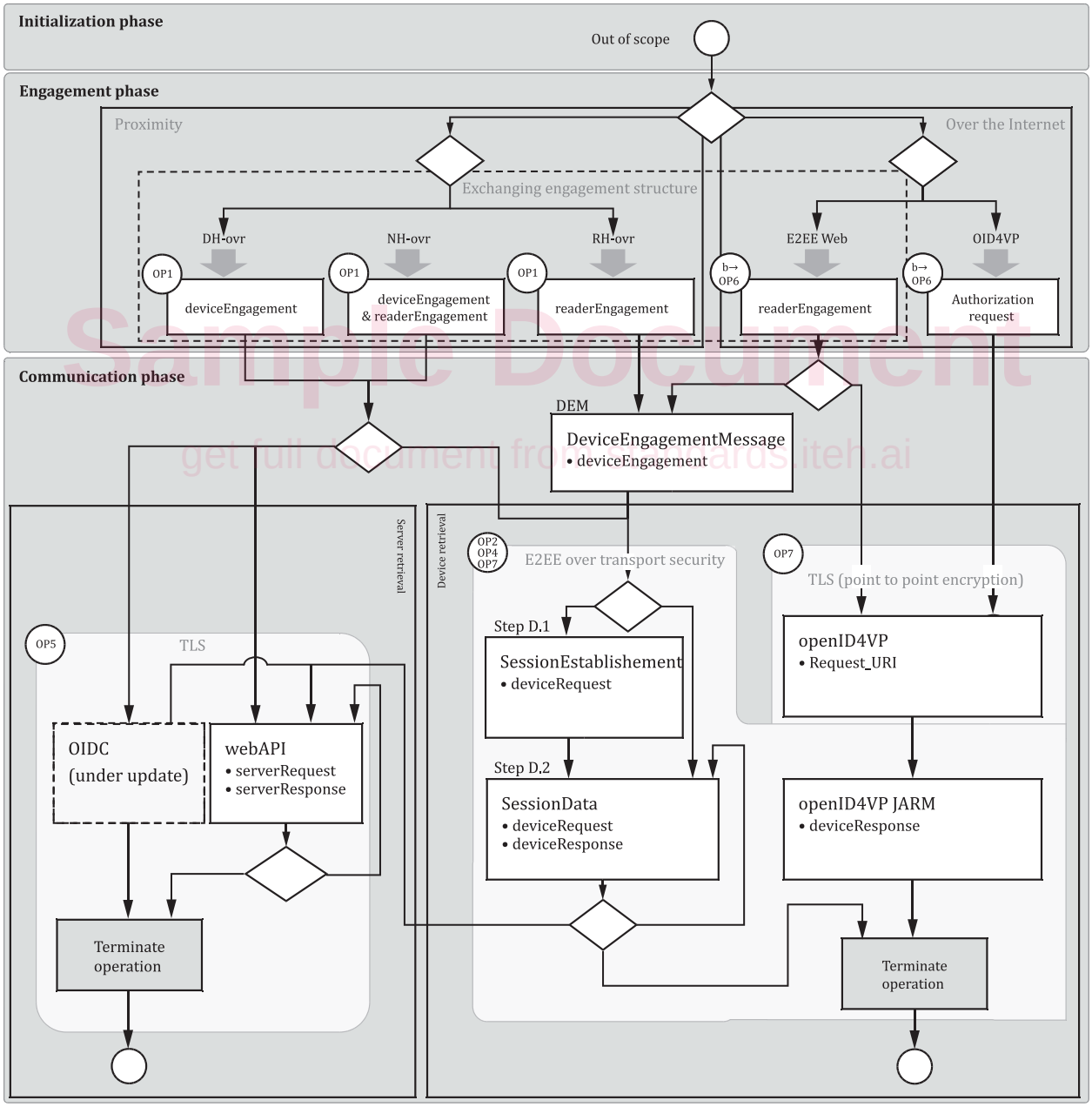

Figure 1 — Operational transaction flow

5.3 Interfaces

5.3.1 Interface and protocols for the engagement sub-phase

The following proximity interfaces, illustrated as OP-1 by ISO/IEC 23220-1:2023, Figure 11, are specified in this document in subclauses:

— 6.5.3 specifies the requirements when mdoc app uses a QR code to present the device engagement structure;

— 6.5.3 specifies the requirements when mdoc reader uses a QR code to present the reader engagement structure;

— 6.5.4 specifies the requirements when mdoc app uses Type 4 NDEF tag specified by NFC forum for static handover mode to perform handover;

— 6.5.4 specifies the requirements when mdoc app uses Type 4 NDEF tag specified by NFC forum for negotiated handover mode, and where mdoc reader further shares the reader engagement structure.

The following interfaces from Internet Browser to mdoc app, illustrated as interface 'b' by ISO/IEC 23220-1:2023, Figure 13, are specified in this document in subclauses:

— 6.6.3 specifies how mdoc reader shall use W3C URISchemes specified by RFC 4395 to present the reader engagement structure or OID4VP engagement data through the mobile Internet browser to the mdoc app, both on the same device;

— 6.6.4 specifies how mdoc reader shall use deep links URL to present the reader engagement structure or OID4VP engagement data through the mobile Internet browser to the mdoc app, both on the same device.

5.3.2 Interface and protocols for the communication sub-phase

The following interfaces for device retrieval are specified in Clause 7 of this document:

— Transmission of attribute(s) part of (a) credential(s) from or through an mdoc app to an mdoc reader (illustrated respectively as OP-2 in Figure 11 from ISO/IEC 23220-1:2023 and as OP-4 in Figure 12 from ISO/IEC 23220-1:2023);

— Transmission of attribute(s) part of (a) credential(s) from an mdoc app to an mdoc reader over the Internet (illustrated as 'OP-7' or 'b' in Figure 13 from ISO/IEC 23220-1:2023).

The following interfaces for server retrieval are specified in Clause 8 of this document:

— Transmission of user attribute(s) part of (a) credential(s) between an mdoc reader and an identity or attribute provider service (illustrated as OP-5 in Figure 12 from ISO/IEC 23220-1:2023).

5.4 Additional methods and operations

Additional methods and operations can be performed during device retrieval:

— 7.2.5 specifies: Framework for credential holder verification where the mdoc reader can request for CHV and the mdoc app can respond accordingly with CHV status

NOTE This document defines only one additional operation.

5.5 Trust model

This document relies on the IA to be source of trust for verification of the mdoc:

— The IA digitally signs the mobile security object (A.1.2) of the mdoc for Authenticity. The authenticity of the signature can be verified using PKI. The IA is the root of trust for signed information and device binding.

— The mdoc is provisioned to an mdoc app that meets the Issuer privacy and security policies.

NOTE ISO/IEC TS 23220-3 can be used to determine the capabilities of the solution and the kind of secure area.

The authenticity of the mobile security object provides a means to the mdoc reader to verify if the returned information is authorized (user attribute(s), authentication factors, validity information and more) and can even permit to check the integrity of such data elements, and using the device key a mean to check if the response is delivered by the expected device (anti cloning) and when such device key is on the holder device to use such device as an authentication factor of something you have.

The issuer signature is verified using a public key infrastructure (PKI).

The issuing authority can define additional authentication factors that can be used for additional confirmation to confirm that the mdoc is presented by the credential holder.

Once communication is established between an mdoc app and an mdoc reader, a signed request provides a means to check for trust for the mdoc app to evaluate the risk prior to returning any information.

The mdoc app must acquire certificates from trusted sources to verify the authenticity of the signed request.

The mdoc reader must acquire certificates from trusted sources to verify the authenticity of the mdoc.

6 Data encoding and parsing of data structures and data elements

6.1 General

All structures in this document are either CBOR or JSON.

This document uses CDDL (Concise Data Definition Language) as specified in RFC 8610 to express CBOR encoded data including in JSON structures.

6.2 CBOR encoding

CBOR structures shall be encoded according to RFC 8949.

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

Note that RFC 8949 does not allow a map with multiple entries with the same key.

Because deterministic map ordering is not required, all CBOR maps that are used in a cryptographic operation are communicated in a tagged CBOR `bytestring`. For any cryptographic operation, an mdoc, mdoc reader or issuing authority infrastructure shall use these `bytestrings` as they were sent or received, without attempting to re-create them from the underlying maps.

EXAMPLE A data structure `DataItem` that is to be used in a cryptographic operation is communicated in a structure `DataItemBytes`, specified as follows:

```
DataItemBytes = #6.24(bstr .cbor DataItem)
```

The CDDL in this example is defined in RFC 8610:2019, section 3.6 and expresses a tagged data item (major type 6). As specified in RFC 8949:2020, section 3.4.5.1, tag value 24 indicates that the content of the CBOR bstr following the tag is itself a CBOR data item. The `.cbor` control operator indicates that this data item is in fact a `DataItem`.

When processing a data structure, an mdoc app, mdoc reader or issuing authority infrastructure shall ignore any value that is specified as RFU in this document.

Whenever data structures in this document use a version element that is encoded as a string, their contents follow the format of ‘major version number’.’minor version number’. A major version number

shall be incremented by 1 when any backwards incompatible changes are introduced in a future version of this document. A minor version number shall be incremented by 1 when new, but backwards compatible functionality is introduced. A minor version number shall be reset to 0 if the major version number is incremented. An mdoc app, mdoc reader or issuing authority infrastructure shall not give an error and continue a transaction if it receives a data structure having a known major version number but with an unknown minor version number.

6.3 JSON encoding

JSON structures shall be encoded according to RFC 8259.

6.4 Parsing encoding information

RFC 761:1980, Section 2.10, states Postel's robustness principle: be conservative in what they send, liberal in what they accept. An mdoc app and mdoc reader should follow this principle for all non-security related structures.

For any structure defined in this standard, unless explicitly stated otherwise, an mdoc app or mdoc reader shall not give an error if a map (major type 5) contains an element that is not defined in the CDDL for that structure.

EXAMPLE It applies when the CDDL definition of the data structure does not explicitly define that additional key-value pairs can be present in the map, next to the specified ones.

6.5 Engagement for proximity transmission

6.5.1 General

All proximity transmissions share the same engagement structures and the same operation messages for device request (7.2.1) and device response (7.2.2) and the same E2EE transport messages (session establishment and session data, respectively 7.3.1 and 7.3.2).

6.5.2 Engagement structures

6.5.2.1 Engagement structures

The `DeviceEngagement` and `ReaderEngagement` structures shall be CBOR encoded. The full CDDL structure can be found in D.1.1.

The `DeviceEngagement` and `ReaderEngagement` structures share identical items. Refer to Table 1 to see which items are needed for each.

The detailed information for each item in the structure is provided in 6.5.2.2.

Testing examples are provided in D.1.2.

Table 1 — Engagement structures

Engagement structure CDDL	DeviceEngagement		ReaderEngagement		Purpose	Details
	DH-ovr	DEM	RH-ovr, E2EE Web	NH-ovr		
Engagement = { 0: tstr	M	M	M	M	Version of structure	6.5.2.2.1
? 1: Security	M	M	M	O	Needed data to establish E2EE	6.5.2.2.2
? 2: DeviceRetrievalMethods	C	N/A	C	N/A	Data to connect mdoc app and mdoc reader	6.5.2.2.3
? 3: ServerRetrievalMethods	O	O	N/A	N/A	Token for server retrieval	6.5.2.2.4
? 4: ProtocolInfo	RFU	RFU	RFU	RFU	Reserved for additional protocol information	6.5.2.2.5
? 5: OriginInfos	O	M	C	O	Info about the source of engagement structure	6.5.2.2.6
? 6: Capabilities	C	C	N/A	N/A	Capabilities such as MacKeys	6.5.2.2.7
? *int => any	Positive values are RFU	Positive values are RFU	Positive values are RFU	Positive values are RFU	Positive values are reserved for future extensions. Negative values can be used.	
}						

Key
M: Mandatory
C: Conditional – see details about condition criteria in related section in 6.5.2.2
O: Optional
N/A: Not applicable
RFU: reserved for future use

An application-specific extension shall use a negative integer for the key. An mdoc app or mdoc reader shall ignore any key-value pairs with a negative key value that it is not able to interpret

6.5.2.2 Details

6.5.2.2.1 version

The *tstr* value for key 0 characterizes the content of the structure as follows:

— The value shall be 1.0 when both Key 5 (*OriginInfos*) and key 6 (*Capabilities*) are not present.

— The value shall be 1.1 when at least one of Key 5 (*OriginInfos*) and key 6 (*Capabilities*) is present.

The value of key 0 defines the version.

6.5.2.2.2 security

The security item specifies the cipher suite and the ephemeral public key to use to establish E2EE. See A.1.1 for session encryption.

The mdoc app shall use that structure to specify the cipher suite to use for the E2EE for the communication phase and to deliver its ephemeral public key for the mdoc reader to use to derive E2EE keys.