Technical Specification

ISO/IEC TS 23220-3

First edition
2026-06

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

Part 3: Protocols and services for installation and issuing phase

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

Partie 3: Protocoles et services pour la phase d'installation et d'émission

Reference number
ISO/IEC TS 23220-3:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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

The ISO/IEC 23220 series consists of the following parts, under the general title Cards and security devices for personal identification — Building blocks for identity management via mobile devices:

— Part 1: Generic system architectures of mobile eID systems

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

— Part 3: Protocols and services for the installation and issuing phase

— Part 4: Protocols and services for the operational phase

— Part 5: Trust models and confidence level assessment

— Part 6: Mechanisms for use of certification on trustworthiness of secure area

— Part 7: Registration Authority Procedures for Mobile Documents

The objective of ISO/IEC TS 23220-3 is to:

— minimize the burden on issuers to engage in device discovery, device attestation, device binding;

— ease the process of categorizing a mdoc app implementation according to the issuer's policy;

— ease the process of provisioning mobile documents;

— rely on a third party for integral Mobile eID function characterization.

This document introduces data structures and APIs applicable for discoverability mechanisms and for mdoc provisioning purposes. Future versions of this document can specify normative protocols based on the data structures and APIs defined in this document that can be referenced by a profile identifier.

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

Part 3: Protocols and services for installation and issuing phase

1 Scope

This document provides building blocks for mobile eID-System infrastructures and normalizes protocols, interfaces and services for mdoc apps by:

— specifying interfaces for data interchange for installing of software in installation phase as well as issuing and deriving of attributes and credentials in issuing phase;

— specifying security and data protection mechanisms;

— applying privacy-enhancing mechanisms;

— specifying discoverability mechanisms.

Mechanisms for updating or revoking of attributes and credentials or mdocs are out of scope of this document and are provided by SA specific protocols.

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

2 Normative references

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

ISO/IEC 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*

ISO/IEC TS 23220-4, *Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 4: Protocols and services for operational phase*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

RFC 9360, *J. Schaad, CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates, February 2023*

IETF RFC draft 06, *OAuth 2.0 Attestation-Based Client Authentication, July 2025*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
attestation statement
proof of authenticity and integrity of data created by a certain entity

Note 1 to entry: Proof of authenticity and integrity is usually achieved by the creation of a digital signature over a particular attestation

3.2
key attestation
attestation statement (3.1) about capabilities of one or more cryptographic keys managed by a SA-application of a secure area

3.3
mdoc app attestation
attestation statement (3.1) about capabilities of an mdoc app instance issued by the mdoc app provider service

3.4
mdoc app capability descriptor
set of data describing capabilities of mdoc app including one or more *secure area attestation objects* (3.7)

Note 1 to entry: See ISO/IEC 23220-1.

3.5
proof of association
statement by an entity providing evidence that two sets of data are managed by the same secure area

EXAMPLE An attestation statement that digitally signs to public keys can serve as Proof of Association that the corresponding private keys are managed by the same SA-Application of a secure area.

Note 1 to entry: Data structures and protocols addressing proof of associations are not yet part of this document but can be specified in future editions. Implementations of proof of associations can require updates on existing secure area solutions in particular hardware-based solutions.

3.6
proof of possession
statement by an entity providing evidence that the entity has access to specific data

EXAMPLE Proof of possession of a cryptographic private key can be achieved by creation of a digital signature over a nonce provided by a verifying entity by applying the cryptographic private key.

3.7
secure area attestation object
SAAO
set of data describing capabilities of SA-Application

Note 1 to entry: See ISO/IEC 23220-1.

4 Symbols and abbreviations

For the purposes of this document, the following abbreviations apply.

CBOR	concise binary object representation
CDDL	concise data definition language
IA	issuing authority
IIN	issuer identification number
MCD	mobile eID capability descriptor
MSO	mobile security object
PoA	proof of association
PoP	proof of possession
SAAO	secure area attestation object
SED	service engagement data

5 General principles

5.1 Security principles

The process of issuing a mobile document into an mdoc app is divided into three sub-phases (see ISO/IEC 23220-1) whereas the respective services can be operated by or under supervision of the Issuing Authority: user identification service, mdoc app discovery service and issuing service. As the mobile device and the mdoc app are considered not under the control of the Issuing Authority three issues are of concern:

— Mechanism and strength of binding of respective installation of mdoc app or mobile document or both to the mobile device to prevent from cloning;

— Mechanism and strength of secure storage of document data to preserve data privacy;

— Mechanism and strength of binding of holder to the mdoc app or mdoc or both to preserve holder-binding and sharing protection.

This document introduces amongst others the concept of mdoc app capability descriptor (MCD) including Secure Area Attestation Object (SAAO) and its retrieval and verification. The concept includes specifications of mechanisms for implementation of interfaces IS-1, IS-2, IS-3 and IS-4 in ISO/IEC 23220-1. In addition, mechanisms for issuing service including the generation of mobile document specific keys and storage of data is specified in this document, see Interface IS-5 in ISO/IEC 23220-1. Mechanisms of the user identification service are out of scope of this document.

5.2 Design principles

The specifications in this document are based on the following principles:

1. The Issuing Authority trusts at least the mdoc app and mdoc app provider or the secure area provider and, if involved in the framework, the ID-Provisioning Entity.
2. The arrangement and negotiation between the Issuing Authority, the device manufacturer or OEM-Vendor and the secure area provider covering the choice of secure area form-factor, its capabilities, its drivers, its hardware interface customization, etc. is out of scope of this document.
3. An mdoc app can support more than one SA-Application and hence, can manage different attestation statements related to each SA-Application.
4. A SA-Application can be of various kinds such as a System-On-Chip acc. to Trusted Connectivity Alliance, part of the operating system, Trustlet of TEE or Java Card Applet of an embedded secure element.

5. An attestation of the SA-Application can be provided by a secure area provider, such as DLOA by Global Platform or FIDO attestation. An attestation is SA-Application specific.

6. The MCD can be optionally signed by the mdoc app provider in addition to the SA-Application statements provided by SA-Application providers.

This document describes the issuing procedure as given in general in ISO/IEC 23220-1 by specifying basic data structures (see Clauses 7 and 8). These basic data structures can be combined to construct data structures and specific messages according to an issuing protocol. An ordered sequence of messages is considered an issuing protocol. General requirements and general action flows of issuing protocols are given in 5.4 and 5.5. Examples of issuing protocols are given in Annex A, Annex B, Annex C and Annex D.

Basic data structures are specified for the purpose of encoding:

1. service engagement data;
2. session encryption data;
3. user attributes (see ISO/IEC 23220-1:2023, 3.1);
4. one or more credentials linked to user attributes (see ISO/IEC 23220-1:2023, 3.5);
5. user binding data;
6. control or access rules to be applied by mdoc app;
7. error codes to be returned by mdoc app or issuing service;
8. attestation information about issuing process to be used at presentation time;
9. attestation information about mdoc app or secure area;
10. lifecycle management information about the issued mobile document to be applied by mdoc app.

5.3 Trust model

The trust model follows a 3-Level approach according to the generic architecture given in Figure 3 (see ISO/IEC 23220-1).

Level 3 describes the mdoc level. Attestation of Level 3 is created by the respective Issuing Authority by means of mobile document specific mechanisms (e.g. Mobile Security Object in ISO/IEC 18013-5 and ISO/IEC TS 23220-4). The mdocs are managed by the mdoc app and SA-Application. A relying party operating a verification application trusts the Issuing Authority.

Level 2 describes the mdoc app level. Attestation of the Level 2 is created by the mdoc app provider service typically operated by the mdoc app provider by means of issuing an mdoc app attestation. An Issuing Authority operating an issuing service trusts the mdoc app provider service. A relying party operating a verification service can also trust the mdoc app provider service.

Level 1 describes the SA-Application level. Attestation of Level 1 is created by the SA-Application provisioning service. Either an mdoc provider operating a mdoc app provider service or the Issuing Authority operating an Issuing Service or both trust the SA-Application service.

5.4 General requirements of protocols for mdoc issuing

Protocols for mdoc issuing shall meet the requirements of issuing authorities listed in this clause. A respective protocol or set of protocols may fulfil all or parts of the requirements. Issuing authorities can choose protocols according to their intended workflows and issuing policies.

An issuing authority is able to:

1. Perform out-of-band user identification either in-person or electronically and to perform in-session user authentication.

2. Perform in-session user data capturing to enable user identification and user authentication.
3. Invoke validation processes to determine suitability of the mdoc app, secure areas, mobile device or all.

   EXAMPLE 1 Requesting and receiving attestation statements from the mdoc app by the IA allows for determination of confidence levels.

4. Establish a secure end-to-end data transmission between remote services of the issuing authority and either the mdoc app or secure area.
5. Uniquely identify and authenticate an mdoc (i.e. different identifiers to different IAs).
6. Select a respective secure area out of a choice.
7. Provision user attributes, i.e. the mdoc, and the MSO simultaneously or at different times.
8. Update user attributes, i.e. the mdoc, and the MSO simultaneously or at different times.
9. Provision of one or more MSOs for the same user attributes, i.e. the mdoc.

   EXAMPLE 2 An IA can update MSOs without updating the user attributes and without performing user identification.

   EXAMPLE 3 Multiple MSOs allow for the single use of a respective MSO to prevent from tracking by the verifier.

10. Provision one mdoc at a time.

    NOTE 1 An IA can process the respective workflow multiple times in order to provision multiple mdocs.

    NOTE 2 Conveying information about already provisioned mdocs in one mdoc app instance to an IA is out of scope of the protocol.

    EXAMPLE 4 A wallet mdoc app manages more than one mdocs.

    EXAMPLE 5 Holders can get issued two mdocs with same user attributes but different MSOs from the same IA.

    EXAMPLE 6 Parents can provision mdocs of their kids in the mdoc app instance of the parents.

11. Perform a provisioning workflow, an update workflow, a deletion workflow and a revocation workflow.
12. Provision an mdoc into an mdoc app and mobile device with limited input/output capacities by leveraging a companion device with suitable input/output capacities.

    NOTE 3 A companion device to a mobile device is a device that has been securely paired with the mobile device.

    EXAMPLE 7 A smart watch can not feature a camera and the camera of the coupled smart phone can be used for capturing QR codes or face images or taking a photo of the plastic card.

    EXAMPLE 8 An mdoc already provisioned onto an mdoc app of one mobile device is available on a companion mobile device.

13. Use different authentication form factors of authentication as part of user identification.
14. Provision a new factor of authentication as part of the mdoc provisioning that is uniquely associated to the holder and stored by the mdoc app.

    NOTE 4 The new factor of authentication is stored by the mdoc app and can be part of the backup system of the mdoc app.

    EXAMPLE 9 IA can request the image of the plastic card as factor of possession as well as a portrait image to provision a first mdoc to the holder. The IA can return a new factor of authentication to the holder as part of the provisioning of the first mdoc (e.g. a digital secret number stored by the mdoc app). The new digital factor and additional user authentication means can in turn be used by the IA to provision a second mdoc onto a further mobile device assigned to the holder.

EXAMPLE 10 Holder has been provisioned an mdoc on one mobile device together with a QR code stored by the mdoc app, which is still operational and wants to migrate onto another device without going through the same user identification procedure but by presenting QR code provisioned by the IA. The former mdoc might be revoked by the IA according to IA policy.

EXAMPLE 11 Holder is no longer in possession of an mdoc and wants to restore an mdoc from a backend onto new mobile device without going through the same user identification procedure. The holder restores the mdoc app from a backend onto the new mobile device and holder uses the restored factor of authentication to authenticate towards the IA and in turn to get mdoc provisioned to the new mdoc app.

15. Interact with the applicant as part of the protocol.

    EXAMPLE 12 IA can request the applicant to approve the deletion of a previously provisioned mdoc to the holder.

16. Provision mdoc through the mdoc app provider service.

5.5 General action flow diagram of issuing protocols

Figure 1 specifies general action flows that are supported by the protocols. An issuing protocol can include all or parts of the steps in the general action flow in any order. Examples of workflows of provisioning mdocs into an mdoc app according to the action flows are given in Annex G.

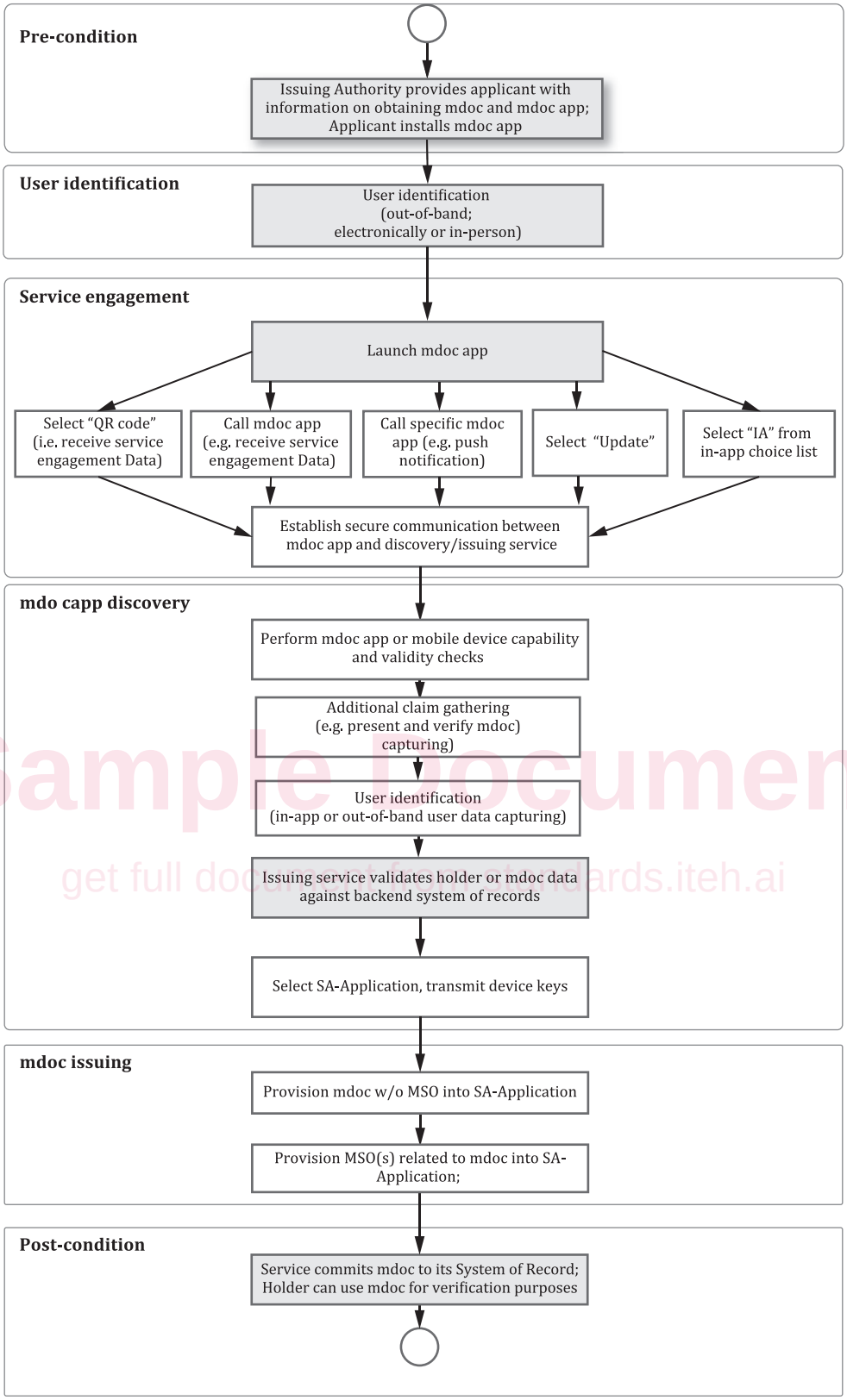
The specific action flow is determined by the issuing policy of the IA and controlled by the entity operating the respective remote services. The protocols require the holder to have the mdoc app installed and to be informed by the IA about the general procedure.

User identification should be performed out-of-band prior to the issuing protocol or in-session as part of the issuing protocol and mdoc app. The former option allows for the integration of any kind of user identification and proofing either electronically or in-person. The latter depends on the capabilities of the mdoc app and mobile device.

In a next step, the holder selects the method to initiate the issuing process. This can be done by launch of the mdoc app followed by selection of "QR code", "Update" or "select IA" from a list. Alternatively, this step can also be initiated by another application, e.g. a browser app or mobile app, installed on the mobile device. The mdoc app connects to the respective remote service and both establish a secure communication. Furthermore, the mdoc app provider service can connect to a specific mdoc app instance, e.g. by means of push notification, in order to receive status information or to start a provisioning or update flow.

Through the secure communication the remote service requests and receives information about mdoc app capabilities and supported secure area applications. This information can include the public parts of the device keys that will be part of the MSOs. The remote service may perform user authentication that links to the out-of-band user identification or may perform in-session user identification and user authentication. Based on these information the remote service checks for a record in the backend system and, if present, may proceed with the selection of a secure area according to the issuing authority policy. If no record is present, the remote service should abort the session and inform the holder about possible next actions not part of the protocol.

In a last step, the service prepares mdoc data and MSOs and sends these data to the mdoc app or secure area application. This step may include the establishment of a further secure communication between remote service and secure area application. Eventually the holder can use the mdoc for verification purposes.



Key

steps in scope

steps out of scope

Figure 1 — General action flow diagram of issuing protocols

6 mdoc app descriptor and attestations

6.1 General description of MCD

The MCD capability descriptor object encodes the minimal required information needed for issuing a mobile document into the mdoc app. An Issuing Authority should examine the MCD to decide whether a mdoc app fulfils its policy of a mobile document or the issuing into the mdoc app is to be denied. If the mdoc app fulfils the Issuing Authority's policy, the Issuing Authority should select the mdoc app's options based on the MCD information.

The MCD is structured into three main objects:

— mdoc app application descriptor listing the main features of the mdoc app,

— SA-Attestation Object (SAAO) listing the main features of the supported SA-Applications,

— Signature over the MCD (optionally) created by the MCD Attestation Service.

The MCD shall be created and shall be made available in the installation phase of the mdoc app by the mdoc app provider. Updates of the mdoc app that change the feature set of the app requires an update of the MCD. The SA-Application and SA-Attestation information encoded in the SAAO may be provided by an entity different to the mdoc app provider. As an mdoc app may support more than one SA-Application, an MCD may hold multiple SAAOs. The MCD may be signed by the MCD Attestation Service. The signature provides authenticity and integrity of the MCD but does not provide a strong link to the mdoc app. Such a link can be provided by an SA-Application Statement created as part of the SA-Application specific protocol.

6.2 Data objects of mdoc app application descriptor

The mdoc app application descriptor shall encode the information given in Table 1. In the tables below, identifiers serve as map keys and denote simple digit or number for the sake of compact encoding; they shall be of type UTF-8 string. When identifiers indicate map values, they shall be of type integer (see 6.4 for CDDL definition). The existence of an identifier in the array of identifiers indicates support of the respective feature by the mdoc app. Any negative values of the identifier, i.e. –n in the tables below, indicate support of further proprietary features.

Table 1 — Data objects of mdoc app application descriptor

Name of object	Occurrences	Description/ Specified values	Identifier	Encoding
`App supported device features`	o	list of supported features of mdoc app and mobile device	0	see Table 2
`App engagement interfaces`	o	List of supported device engagement interfaces provided by mdoc app and mobile device	1	see Table 3
`App data transmission IF`	o	List of supported data transmission interfaces provided by mobile device	2	see Table 4
`Certifications`	o	List of certifications assigned to mdoc app	4	see Table 5
m – mandatory object, o – optional object any other values are RFU				

The data object "App supported device features" encodes supported features of the mdoc app and the mobile device that are required by protocols and services described in the ISO/IEC 23220 series (see Table 2). The value `other` encodes proprietary information about further app features and may be interpreted by the discovery service.

Table 2 — Values and identifiers of "App supported device features"

Specified values	Identifier	Encoding
Webview feature	0	uint
Simple view feature	1	uint
other	-n	uint
Any other values are RFU		

The data object "App engagement interfaces" encodes supported device engagement transmission technologies (see Table 3). The value `other` encodes proprietary information about further transmission technologies and may be interpreted by the discovery service.

Table 3 — Values and identifiers of "App engagement interfaces"

Specified values	Identifier	Encoding
QR	0	uint
NFC	1	uint
other	-n	uint
Any other values are RFU		

The data object "App data transmission IF" encodes supported data retrieval transmission technologies (see Table 4). The value `other` encodes proprietary information about further transmission technologies and may be interpreted by the discovery service.

Table 4 — Values and identifiers of "App data transmission IF"

Specified values	Identifier	Encoding
NFC in accordance with ISO/IEC TS 23220-3 and ISO/IEC TS 23220-4	0	uint
BLE	1	uint
WiFi aware	2	uint
Internet	3	uint
other	-n	uint
Any other values are RFU		

The data object "Certifications" encodes information about approvals or certifications assigned to the mdoc app or SA-Application (see Table 5). The mdoc app may be subject to a security certification that is bound to a certification of the SA-Application (see 6.3). If the mdoc app does not provide any certification but the SA-Application is certified, it is in the responsibility of the issuing service to trust the security functions applied by the mdoc app. The issuing service may alternatively establish a trusted communication with the certified SA-Application.

The value `other` encodes proprietary information about further app certifications and may be interpreted by the discovery service.

Table 5 — Values and identifiers of "Certification"

Specified values	Identifier	Encoding
Common Criteria Protection Profile number	0	bstr
Common Criteria certification number	1	bstr
Certification number according to ISO/IEC 19790	2	bstr
Reference to Digital Letter Of Approval of the secure area platform according to [1]	3	tstr
Reference to Digital Letter Of Approval of the SA-Application according to [1]	4	tstr