INTERNATIONAL STANDARD

**ISO/IEC 23220-1**

First edition
2023-02

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

## Part 1: Generic system architectures of mobile eID systems

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

*Partie 1: Architectures génériques des systèmes d'identification électronique mobiles*



Reference number
ISO/IEC 23220-1:2023(E)



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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

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

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

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

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

# Introduction

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

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

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

The technical preconditions for the deployment of mdoc apps exist and they are partly standardized to support security and privacy on a mobile device. Examples for containers of eID-App solutions are the software-based Trusted Execution Environment (TEE), hardware-based secure elements such as universal integrated circuit card (UICC), embedded or integrated UICC (eUICC or iUICC), embedded secure elements, secure memory cards with cryptographic module [17] or other dedicated internal security devices residing on the mobile device, as well as solutions with server-based security means.

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

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

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

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

a) secure channel establishment;

b) API call serialization method;

c) data element naming convention;

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

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

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

Other parts in the ISO/IEC 23220 series specify the following:

— generic data formats (see ISO/IEC TS 23220-2);[1)]

— protocols and services for issuing phase (see ISO/IEC TS 23220-3);[2)]

— protocols and services for operational phase (see ISO/IEC TS 23220-4)[3)];

— trust models and confidence levels (see ISO/IEC TS 23220-5)[4)];

— mechanism for use of certification on trustworthiness of secure area (see ISO/IEC TS 23220-6).[5)]



1) Under preparation. Stage at time of publication: ISO/IEC AWI TS 23220-2.

2) Under preparation. Stage at time of publication: ISO/IEC AWI TS 23220-3.

3) Under preparation. Stage at time of publication: ISO/IEC AWI TS 23220-4.

4) Under preparation. Stage at time of publication: ISO/IEC AWI TS 23220-5.

5) Under preparation. Stage at time of publication: ISO/IEC AWI TS 23220-6.

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

# Part 1: Generic system architectures of mobile eID systems



## 1 Scope

This document specifies generic system architectures and generic life-cycle phases of mobile eID systems in terms of building blocks for mobile eID system infrastructures. It standardizes interfaces and services for mdoc apps and mobile verification applications.

It 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

There are no normative references in this document.

## 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**
**attribute**
**user attribute**
characteristic or property of an *entity* (3.6)

EXAMPLE An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes

[SOURCE: ISO/IEC 24760-1:2019, 3.1.3]

**3.2**
**attribute statement**
attribute describing a statement or assertion about *user attributes* (3.1) comprising predicates over attributes

[SOURCE: ISO/IEC 19286:2018, 3.6, modified — Added "attribute describing a" at the beginning of the definition and removed EXAMPLE.]

**3.3**
**authentication**
provision of assurance in the *identity* (3.10) of an *entity* (3.6)

[SOURCE: ISO/IEC 29115:2013, 3.2]

**3.4**
**authentication protocol**
defined sequence of messages between an *entity* (3.6) and a *verifier* (3.40) that enables the verifier to perform *authentication* (3.3) of an entity

[SOURCE: ISO/IEC 29115:2013, 3.4]

**3.5**
**credential**
set of data presented as evidence of a claimed or asserted *identity* (3.10) and/or entitlements

Note 1 to entry: According to ISO/IEC 29115 an assertion is considered a stronger statement than a claim.

EXAMPLE 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.

[SOURCE: ISO/IEC 29115:20133.8, modified — Replaced Note 1 to entry with new Note 1 to entry. EXAMPLE was added.]

**3.6**
**entity**
item relevant for the purpose of operation of a domain that has recognizably distinct existence

Note 1 to entry: An entity can have a physical or a logical embodiment.

EXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.1]

**3.7**
**holder**
*entity* (3.6), i.e. natural person, who holds the *mdoc app* (3.19) and uses it to perform *user identification* (3.8) towards a *verification application* (3.39)

**3.8**
**identification**
**user identification**
process of distinguishing an *entity* (3.6) within a given context by the unique association of a set of descriptive parameters

EXAMPLE User attributes are descriptive parameters of the entity 'holder'.

[SOURCE: ISO/IEC 19286:2018, 3.15, modified — Added "of the entity 'holder'" to the EXAMPLE.]

**3.9**
**identifier**
data which identifies an *entity* (3.6) in a given context towards another entity

[SOURCE: ISO/IEC 19286:2018, 3.16]

**3.10**
**identity**
set of *attributes* (3.1) related to an *entity* (3.6)

Note 1 to entry: An entity can have more than one identity.

Note 2 to entry: Several entities can have the same identity.

Note 3 to entry: ITU-T X1252 specifies the distinguishing use of an identity. In this document, the term identifier implies this aspect.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.2]

**3.11**
**identity or attribute provider service**
service that receives *attributes* (3.1) authorized by the *issuer* (3.14) and makes these attributes available to *verification applications* (3.39) in the *operational phase* (3.26)

Note 1 to entry: An identity or attribute provider can be deployed as central service or as decentral service by using a distributed ledger technology managed by the holder.

Note 2 to entry: An attribute provider services provides any kind of *attributes* (3.1).

Note 3 to entry: An identity provider services makes attributes available that convey identity information.

**3.12**
**ID-provisioning entity**
entity that operates all or parts of services of *installation phase*, (3.13), *issuing phase* (3.15) and *operational phase* (3.26) on behalf of the *issuer* (3.14)

**3.13**
**installation phase**
phase of *mobile document system* (3.23) that includes the loading of the *mdoc app* (3.19) and related software onto the *mobile device* (3.17)

EXAMPLE Loading an app onto a smartphone or loading an SA-Application (e.g. a Java Card applet) into the secure area, e.g. an embedded secure element,[19] is part of the installation phase.

**3.14**
**issuer**
*entity* (3.6) that makes available *user attributes* (3.1) and *credentials* (3.5) in the *issuing phase* (3.15) and authorizes the instantiation of the *mdoc app* (3.19)

Note 1 to entry: An issuing authority acts as an issuer.

**3.15**
**issuing phase**
phase of *mobile document system* (3.23) that includes the initial issuing of either *user attributes* (3.1) or *credentials* (3.5) or both into the *mdoc app* (3.19) and can include the re-issuing of credentials

Note 1 to entry: In literature, issuing of user attributes and credentials is also referred to as provisioning of user attributes and credentials.

**3.16**
**issuing service**
service operated in *issuing phase* (3.15) that provides all data of a *mobile document* (3.22) stored either locally in the *mdoc app* (3.19) or remotely at an *identity or attribute provider service* (3.11)

**3.17**
**mobile device**
portable computing device that at least: a) has a small form factor such that it can easily be carried by a single individual; b) is designed to operate, transmit and receive information without a wired connection; c) possesses local, non-removable or removable data storage; d) includes a self-contained power source and e) includes means for the *holder* (3.7) of the portable computing device and the device to interact with each other

Note 1 to entry: Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or extended computer functionality and connectivity.

Note 2 to entry: Adapted from ISO/IEC 18013-5.

EXAMPLE Smartphones, tablets, and e-readers are mobile devices.

**3.18**
**discovery service**
service operated in *issuing phase* (3.15) that verifies *mdoc app* (3.19) characteristics by means of mdoc app capability descriptor

**3.19**
**mdoc app**
application on a *mobile device* (3.17) that manages *user attributes* (3.1) and *credentials* (3.5) for electronic identification purposes and controls access to the user attributes and credentials whether the user attributes and credentials are stored on the mobile device, on a server or on an external device

Note 1 to entry: In ISO/IEC 18013-5, mdoc represents mdoc app or *mobile document* (3.22).

**3.20**
**MCD attestation service**
service signing the mdoc capability descriptor

Note 1 to entry: The *mdoc app* (3.19) capability descriptor is specified in ISO/IEC TS 23220-3[6].

**3.21**
**mdoc app provider service**
webservice operated by the *mdoc app* (3.19) provider in *issuing phase* (3.15) that controls the issuing of *mobile documents* (3.22) into the mdoc app

**3.22**
**mobile document**
set of *attributes* (3.1) and *credentials* (3.5) issued by one or more issuers into an *mdoc app* (3.19) and managed by an mdoc app

Note 1 to entry: A mobile document is considered a digital document. An mdoc app managing more than one mobile document is also considered an eID-Wallet.

Note 2 to entry: In ISO/IEC 18013-5, mdoc represents mdoc app or mobile document.

EXAMPLE Mobile documents include eID documents and licenses or certificates that give the holder permissions.

**3.23**
**mobile document system**
**mobile eID-System**
set of components interacting to manage *mobile documents* (3.22)

EXAMPLE Components of a mobile document system are *mdoc app* (3.19), mobile verification application, issuing service or validation service.

**3.24**
**monitoring service**
service operated in *issuing phase* (3.15) that controls all or parts of a *user identification service* (3.37), *discovery service* (3.18), *issuing service* (3.16) or *MCD attestation service* (3.20)

**3.25**
**on-site identification**
use case of *mobile document system* (3.23) that requires a local device-to-device communication for *user identification* (3.8) between a *mobile device* (3.17) providing the *mdoc app* (3.19) and *verifier device* (3.41)

Note 1 to entry: Device-to-device authentication includes the mobile device with mdoc app and the verifier device with verification application.

**3.26**
**operational phase**
phase of *mobile document system* (3.23) that includes the usage of the *mdoc app* (3.19) for the purpose of *user identification* (3.8) and *authentication* (3.3)

**3.27**
**remote identification**
use case of *mobile document system* (3.23) that requires a remote device-to-service communication over the internet for *user identification* (3.8) between a *mobile device* (3.17) and *verification application* (3.39)

Note 1 to entry: Device-to-service authentication includes the mobile device with *mdoc app* (3.19) and the verification application without verifier device.

**3.28**
**remote user storage service**
service that manages data storage and that controls access to it

Note 1 to entry: Authorization by the holder is required.

**3.29**
**removal phase**
phase of *mobile document system* (3.23) that includes the removal of the *mdoc app* (3.19) and related software as well as *user attributes* (3.1) and *credentials* (3.5) from the *mobile device* (3.17)

**3.30**
**SA-Application**
application of the *secure area* (3.33) that manages *credentials* (3.5) and that may manage *user attributes* (3.1) for *user identification* (3.8) purposes and can control access to the user attributes

**3.31**
**SA-Application provider service**
service that installs *SA-Applications* (3.30) into secure areas by means of an SA-Client

**3.32**
**secure memory card**
non-volatile memory card format, i.e. a Secure Digital (SD) Card, for use in portable devices with physical sizes “original”, “mini” or “micro” together with a cryptographic module

[SOURCE: NIST SP 800-157 [17]]

**3.33**
**secure area**
isolated internal or attached area of a *mobile device* (3.17) that ensures secure processing and storing of data even when the primary operating system (OS) is compromised

Note 1 to entry: The primary OS is also referred to as rich OS or high-level OS.

EXAMPLE A secure element [19] or a Trusted Execution Environment (TEE) [19] serve as an internal secure area. A universal integrated circuit card (UICC) is considered as an attached secure area of a mobile device.

**3.34**
**server retrieval token**
token identifying the *holder* (3.7) and the *mobile document* (3.22) to the *identity or attribute provider service* (3.11)

**3.35**
**Trusted Execution Environment**
**TEE**
*secure area* (3.33) of the main processor of a mobile device

**3.36**
**TSM-Service**
SA-Application provisioning service that allows for loading and installing of *SA-Applications* (3.30) according to GlobalPlatform

EXAMPLE JavaCard Applets and Trustlets are SA-Applications.

**3.37**
**user identification service**
service operated in *issuing phase* (3.15) that identifies the *holder* (3.7) by electronic or non-electronic means with or without a *mobile document* (3.22)

**3.38**
**validation service**
service or mechanism in *operational phase* (3.26) that allows for determination of validity of *mobile documents* (3.22)

Note 1 to entry: Determination of validity can include revocation status of mobile documents.

EXAMPLE Certificate revocation lists or public key directories can be part of validation services.

**3.39**
**verification application**
**mdoc reader**
application on a *verifier device* (3.41) or on a remote server validating *user attributes* (3.1) and *credentials* (3.5) retrieved from an *mdoc app* (3.19) or an *identity or attribute provider service* (3.11)

Note 1 to entry: mdoc app and a verification application are typically part of a mobile document system.

Note 2 to entry: In ISO/IEC 18013-5 an mdoc reader is defined as a device that can retrieve mdoc data for verification purposes.

**3.40**
**verifier**
*entity* (3.6) that controls the *verification application* (3.39) and uses it to perform *user identification* (3.8)

**3.41**
**verifier device**
device that connects locally with the *mobile device* (3.17) providing the *mdoc app* (3.19) and that optionally provides the *verification application* (3.39)

EXAMPLE An ISO/IEC 14443 terminal that connects with a mobile device is a verifier device without a verification application. A mobile device providing a verification application that connects via ISO/IEC 14443 with the mobile device is a verifier device.

## 4 Abbreviated terms

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

| | |
|---|---|
| BLE | Bluetooth Low Energy |
| eID | Electronic identity |
| eSE | embedded secure element |
| eMRTD | electronic Machine-Readable Travel Document |
| eUICC | embedded universal integrated circuit card |
| IDS | Image Delivery Server |

| | |
|---|---|
| MCD | mdoc app capability descriptor |
| mdoc | mobile document |
| OFL | Open Firmware Loader |
| SA | Secure Area |
| SAAO | Secure Area Attestation Object |
| TEE | Trusted Execution Environment |

# 5 Design and privacy principles of mobile document systems

## 5.1 Design principles

This document specifies building blocks in terms of services. Protocols and interfaces implementing the data exchange for these services are specified in ISO/IEC TS 23220-2, ISO/IEC TS 23220-3, ISO/IEC TS 23220-4. Services can be operated by various entities such as an issuer or an entity acting on behalf of the issuer. The document distinguishes services directly communicating with the mdoc app and services communicating with other (backend)-services. For example, an issuer can operate all or some of those services. Deployment examples are given in Annex A.

A mobile document system in conformance to this document implements one or more of the specified system architectures involving an mdoc app running on a mobile device and used for identification and authentication purposes of a holder. The verifier is an entity providing a verification application either through a verifier device placed at a certain distance to the mobile device or through an online service. The verifier uses issuer information and a related confidence level to determine the quality of the identification or authentication process.

The user attributes and credentials are managed by the mdoc app or the SA-Application or by a remote identity and attribute provider or a combination of these options. The management of these data includes storage and access control. The use of an SA-Application with hardware backed secure area (see 6.2), e.g. a secure element,[19] provides higher confidence in the user identification and authentication process due to the involvement of tamper-resistant hardware components.

A mobile document system is an identity management system in accordance with ISO/IEC 24760 and manages identities in a certain domain. Different domains which have agreements about identity federation according to ISO/IEC 24760 are allowed for establishing trust in the cross-domain identification process and in the derivation of user attributes from a primary domain into a secondary domain. Hence, re-issuing or renewal as well as revoking and deleting processes of user attributes and credentials are part of a mobile document system together with the required infrastructures.

The specification of generic architectures of mobile document systems including services and interfaces use the following key in the figures if not stated otherwise.

**Key**

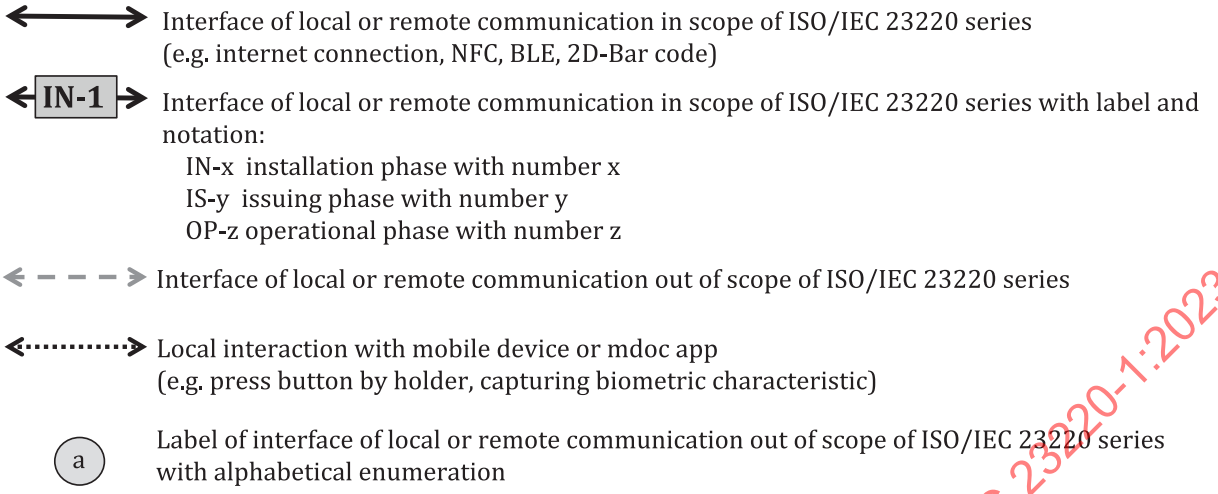



**Figure 1 — General notation of system architecture specifications**

## 5.2 Privacy and security principles

### 5.2.1 General

In the specification of the mobile document system, the following privacy and security principles according to ISO/IEC 29100 and ISO/IEC 19286 are considered:

### 5.2.2 Data minimization

a) Partial attribute release: Partial release of user attributes and attribute statements contributes to realizing data minimization. This requires the use of technology, which does not inherently lead to the release of all or large parts of the PII in each transaction.

b) Unlinkability: Unlinkability of transactions at the cryptographic or protocol level contributes to data minimization. Only identifiers that are required to establish necessary linkability with other transactions are disclosed. Establishing linkability of a transaction with other transactions by default through an improperly designed cryptographic protocol layer counters the ideas of data minimization.

c) Domain-specific identifier (Pseudonym): Domain-specific identifiers, or pseudonyms, are another concept towards data minimization. They are a form of identifiers, which avoid the use of the same unique identifier for a holder in all its interactions. Particularly, when a mobile document system is used for both governmental applications and private-sector applications, some countries mandate different identifiers to be used for public- and private-sector. This is to prevent the exposure of substantial personal information from one entity's data to other entities.

### 5.2.3 Consent and choice:

a) User-centric system: In a user-centric system the holders have control over the use of their attributes and can exert informed consent, whether the user attributes are managed by a SA-Application and/or by a remote identity or attribute provider.

### 5.2.4 Accuracy and quality

a) User binding: The user attributes and credentials are be bound to the holder, i.e. the legitimate holder to whom it is issued. This is crucial for the basic function of any government-issued document of associating attributes with people to whom they should apply.

b) Eavesdropping protection: Protocols executed between the components of the mobile document system can protect against eavesdropping of personal identifiable information of communications.

c) Attribute authenticity and integrity: This refers to the authenticity and integrity of attributes being protected and released to the relying entities being consistent with the attributes the issuer has issued. Thus, attribute integrity and authenticity are the basic security properties assuring security of user attribute information not being tampered with. Achieving authenticity and integrity of the contained attributes is a foundational function of any government-issued security document.

d) Attribute revocation: Revocation of attributes refers to preventing the revoked attributes from being used in future transactions or ensuring that such use would be recognized as illegitimate by verifiers.

e) Attribute update: The update of attributes refers to the change of attribute values or addition of attributes regardless of whether the attributes are stored within the mdoc app or at a remote Identity or Attribute Provider. The attribute update can be performed in the field or remotely with or without the holder being required to be in-person.

f) Cloning protection: Cloning protection prevents from cloning. Cloning refers to the illegitimate reproduction of the credentials and user attributes. Cloning can illegitimately give parties using cloned credentials privileges they would not hold otherwise.

#### 5.2.5 Information security

a) Secure data storage: The user attributes and credentials are securely stored ensuring the confidentiality, authenticity, integrity and availability of the data. This protects the data against risks such as unauthorized access, destruction, use, modification, disclosure or loss.

In technical aspects, the privacy and security principles can be fulfilled by protocols and mechanisms specified in the ISO/IEC 23220 series.

## 6 General life-cycle phases and components of mobile document systems

### 6.1 Life-cycle phases of mobile document systems

The deployment and operation of a mobile document system is divided into different generic phases with different components involved. Requirements for implementations of such components and services are given in ISO/IEC TS 23220-2, ISO/IEC TS 23220-3, ISO/IEC TS 23220-4, ISO/IEC TS 23220-5, ISO/IEC TS 23220-6. Deployment examples of components are given in Annex A. A mobile document system consists of the following five life-cycle phases and transitions (see Figure 2):

— the initialization phase is the starting phase that includes the setup of one or more infrastructures required for installation, issuing, operational and removal phases; specification of this phase is out of scope of the ISO/IEC 23220 series;

NOTE For information on how to securely inject a root of trust in a secure area see [18].

— the installation phase (see system architectures in Clause 7) that can be entered

  — by transition `start deployment` from initialization phase just by starting the deployment of required software, e.g. the mdoc app or firmware for tamper resistant elements (TRE), or

  — by transition `update mdoc app` from operational phase in case new software components are available, or

  - by transition `load mdoc app` from removal phase in case software components (e.g. mdoc app) have been removed from one mobile device and is newly to be loaded onto another mobile device;

— the issuing phase (see system architectures in Clause 8) that can be entered

  - by transition `start issuance` from installation phase upon request by the holder (e.g. after transition `update mdoc app` user attributes and credential may be still issued), or

  - by transition `re-issue user attributes and/or credentials` from operational phase in case values of user attributes or credentials or both have been changed;

    EXAMPLE A change of name or living address requires a re-issuance of these attributes, whereas the expiration of the validity of the mobile document or electronic signature of the issuer require the re-issuance of these credentials.

— the operational phase (see system architectures in Clauses 9 and 10) that can be entered by transition `start usage` from issuing phase after issuance of user attributes and credentials has been completed;

— the removal phase that can be entered by transition `remove from device` in case all software and data have to be deleted on a particular mobile device and conditionally user attributes and credentials on a remote server; life-cycle can start with installation phase by transition `load mdoc app`; specification of this phase is out of scope of this document.

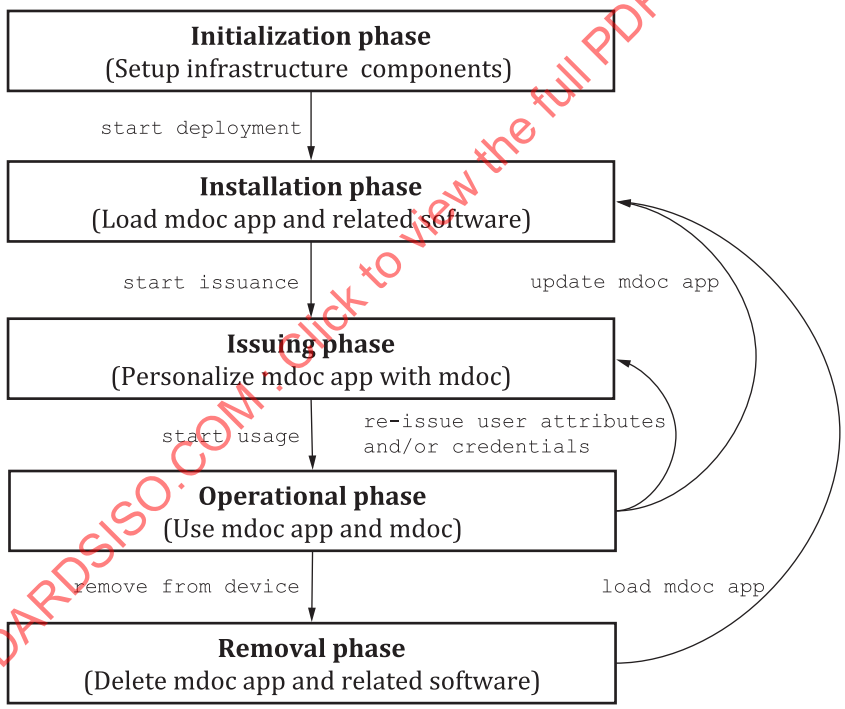



**Figure 2 — Life-cycle phases of mobile document system**

## 6.2 Components of a mobile document system

### 6.2.1 Operational modes of components

A mobile document system may be operated in different modes according to a policy by the issuer. The main distinguishing aspects of architectures are

— the kind of binding user attributes to the holder,

— the location and storage of the user attributes itself, and

— the mode of transmission of the user attributes and credentials.

User binding describes the method and strength of linking electronic data, i.e. the user attributes, to a natural person, i.e. the holder. The creation of the binding is the responsibility of the issuer; the verification of the binding is the responsibility of the verifier. A verifier that operates a verification application can verify this link (e.g. the verifier can compare an electronically received face image as part of the user attributes with the face of the holder). The issuer can establish a strong link between the electronic data and the natural person as part of the issuing process (e.g. the issuer can verify the identity of a holder through personal appearance in the issuing phase). If the confidence level matches the requirements of the verifier, the verifier shall have sufficient confidence in the binding established by the issuer and hence can accept the holder as a legitimate holder of the mdoc app and the respective mobile document.

Depending on the respective policy of an issuer, a subset of the specified interfaces and services given in Figure 3 (and specified in the ISO/IEC 23220 series) are to be implemented and are to be operated by certain entities. Annex A gives examples of typical deployment options of the services. Examples include an issuing authority that operates all services required for issuing and revoking of a mobile document by itself (see A.2 and A.3). Other examples include deployment options that allow for operating all or parts of the services by an entity different from issuer, i.e. by an ID-provisioning entity, but monitored by the issuer (see A.4 and A.6). An issuer can also choose to operate parts of the services by itself, whereas other parts are operated by the ID-provisioning entity (see A.5).

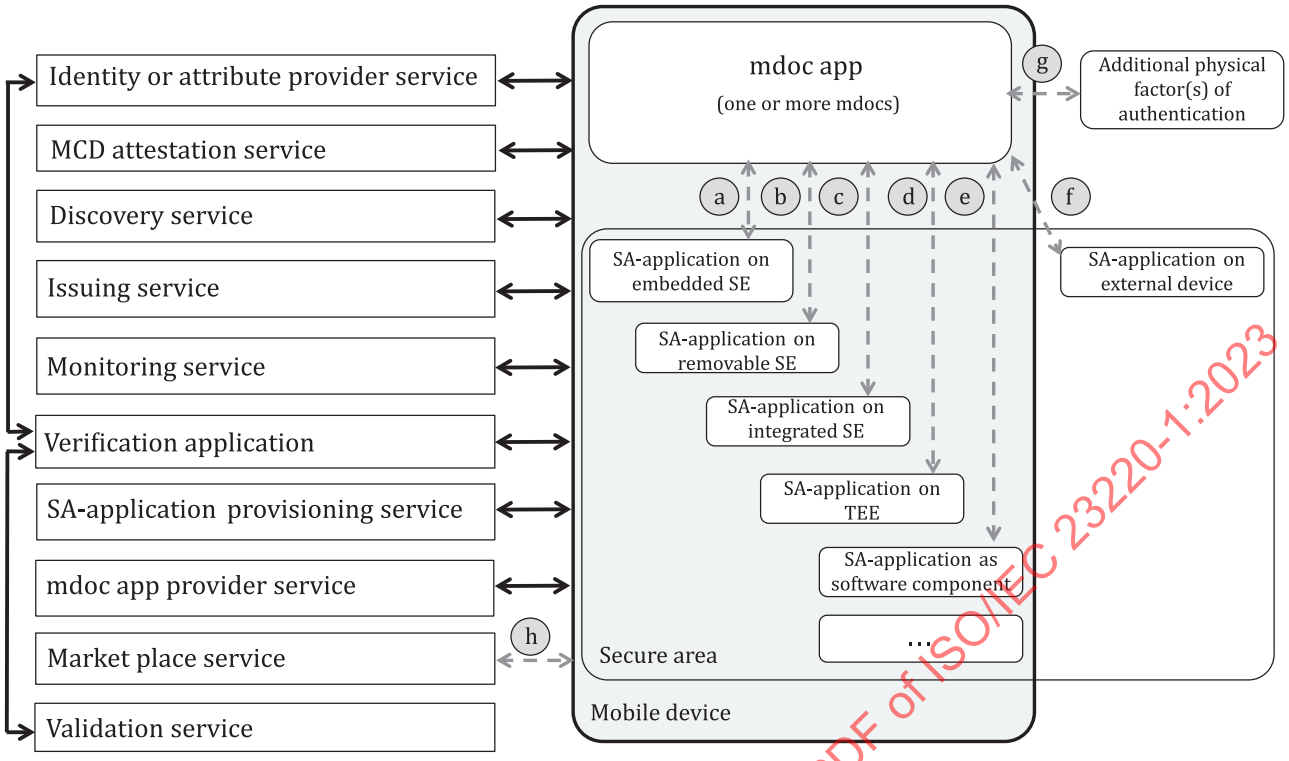
### 6.2.2 Components of mobile document systems

The main components of a mobile document system (see Figure 3) considered in this document are

— the mdoc app including one or more SA-Applications,

— all service related to the issuing of mobile documents, and

— all services related to the usage of mobile documents.




**Key**

see Figure 1

**Figure 3 — Components of mdoc app and related services**

A mobile document system may implement different architectures and functionalities (see system architectures in Clauses 7 and 8). Sensitive user attributes and credentials as well as authentication factors for the purpose of holder authentication (e.g. biometric factors or knowledge-based factors) can be managed in a secure area. The secure area can be hardware or software based or both. Mechanisms for verifying the trustworthiness of secure areas are specified in ISO/IEC TS 23220-6.

EXAMPLE 1 A SA-Application on a Secure Element[19] on a TEE[19] or any other software or firmware component or both as part of a TRE can serve as a secure area.

EXAMPLE 2 Certain OS extensions providing mechanisms to securely store and manage user attributes and credentials or an implementation of white box cryptography serve as a software-based secure area.

The mdoc app should at least use one option of the secure area given in Figure 3. Depending on the chosen SA-Application, an additional service for the provisioning of the SA-Application can be required (see SA-Application provider service in Figure 3 and in A.6, B.4 and B.5).

The mdoc app communicates with the secure area via mobile device internal communication channels [see relations (a), (b), (c), (d) and (e) in Figure 3] for the purpose of accessing and processing user attributes and credentials. The SA-Application can reside on an external device (e.g. contactless eID Cards or wearables) and communicates with the mdoc app via a local communication channel [see relation (f) in Figure 3]. Moreover, a physical token with or without electronic capabilities exhibiting physical security features that can be captured or interpreted by the mdoc app, can serve as additional authentication factor of the holder [see relation (g) in Figure 3 and examples in Annex D]. Additional physical factors of authentication can be used in the following life cycle phases:

— Issuing phase: In sub-phase user identification they can be used to enrol the holder or to confirm user attributes of the holder before sub-phase issuance;

— Operational phase: They are applicable in all architectures of operational phase to confirm the identity or the user attributes of the holder. They can be requested depending on the policy defined by the mdoc app, the issuer, or the verifier operating the verification application.

EXAMPLE 3 Additional physical factors are eMRTDs, electronic identity cards or secure identity documents with optical authentication features.

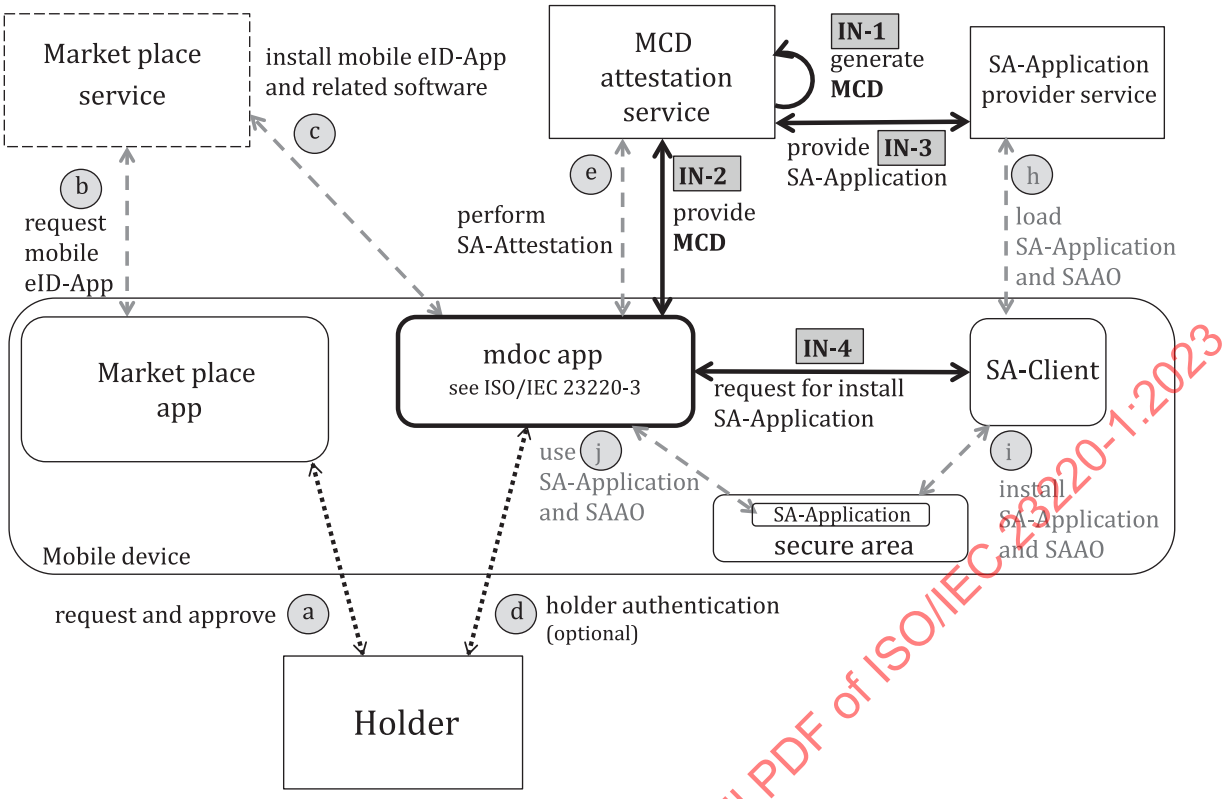
User attributes and credentials can be managed by one or more identity or attribute provider services (see Figure 3). Moreover, a mobile document system may include a market place service and SA-Application provisioning service to install, update or delete the mdoc app and SA-Application, respectively. Lastly, any combination of the above given options can be designed and deployed.

## 7 Generic system architectures of mobile document systems in installation phase

The installation phase includes all steps to make an mdoc app ready for issuing. These steps depend on the capabilities of the mdoc app. The capabilities and confidence levels are described in the mdoc app capability descriptor (MCD) that includes the Secure Area Attestation Object (SAAO) and are conveyed to the issuer in the issuing phase (see ISO/IEC TS 23220-3).

NOTE This document distinguishes attestations provided by the mobile device manufacturer, i.e. attestation of capabilities of secure area as part of the mobile device "SA-attestation", and attestation provided by the MCD attestation service, i.e. attestation of mdoc app capabilities. Both attestations can be conveyed to the issuing service in issuing phase as parts of the MCD.

In the installation phase the holder chooses to load and install the mdoc app via its market place app, e.g. see relation (a) and (b) in Figure 4. The holder can be made aware of such mdoc app and the market place via the issuing authority's portal website if such portal is available. Alternatively, the mdoc app can be pre-installed on the mobile device and the MCD is created during pre-installation or installation (see B.2).




**Key**

see Figure 1

**Figure 4 — Installation architecture with SA-Application provisioning**

In an alternative solution, the mdoc app communicates with an online MCD attestation service to start establishing a binding between the mdoc app and the mobile device after loading and launching the mdoc app the very first time [see relation (c) in Figure 4]. The binding is based on the SA-attestation as part of the SAAO (see ISO/IEC TS 23220-3) provided by the mobile device manufacturer. Information about further device capabilities are made available by means of device functionalities and mdoc app functionalities to the MCD attestation service [see relation (e) in Figure 4]. The service creates the MCD including the SAAOs and writes either the full MCD data into the mdoc app or the appropriate reference to the MCD (see interfaces IN-2 and IN-1 in Figure 4). In the latter case the MCD attestation service maintains the full MCD for online retrieval. A deployment example with an MCD attestation service without SA-Application Provider Service is given in B.3.

The SA-Application provider service allows for the provisioning of an mdoc app-specific SA-Application via a SA-Client application onto a secure area. Loading, installation as well as installation of the SAAO are specific to the chosen secure area and out of scope of this document [see relations (h) and (i) in Figure 5]. In an initial step, which is not necessarily part of the installation sequence, the SA-Application of the mdoc app provider should be made available to the SA-Application provider service (see interface IN-3 in Figure 4). During installation of the mdoc app, the app requests the installation of the respective SA-Application to the SA-Client already installed on the mobile device (see interface NA-2 in Figure 5). The SA-Client has administrative access rights to the secure area and controls the loading and installation of the SA-Applications. With the successful installation of the SA-Application and the corresponding SAAO, the mobile-eID-App can start using the SA-Application on application level and the mdoc app provider backend can create further attestations and provide the MCD (see interfaces IN-2 and IN-1 in Figure 4). Examples of SA-Application provider services and corresponding SA-Applications, i.e. JavaCard Applets, are given in B.4 and B.5.

# 8 Generic system architectures of mobile document systems in issuing phase

## 8.1 Source of user attributes

A mobile document system is an identity management system according to ISO/IEC 24760-1 that includes the collection of user attributes from various sources (see Annex C). It is in the responsibility of the issuing service to

— retrieve user attributes from one or more sources,

— validate the user attributes,

— optionally determine a confidence level, and

— issue user attributes and credentials into the mdoc app.

The generic system architectures for issuing specified in this document are independent of the source of user attributes. Mechanisms for identity proofing are out of scope of this document. Requirements for identity proofing are given in ISO/IEC TS 29003 and specification of confidence levels are given in ISO/IEC TS 23220-5. Examples of enrolment procedures of holders are described in Annex C.

## 8.2 Generic sub-phases of issuing phase

The issuing procedure follows three generic sub-phases (see Figure 5):

— User identification sub-phase;

— mdoc app discovery sub-phase;

— Data issuance sub-phase.

In dependency to the life-cycle state, i.e. transition `start issuance` or `re-issue user attributes and/or credentials`, it is possible that some of the phases will not apply. Protocols and interfaces as well as data formats applicable in theses sub-phase are specified in ISO/IEC TS 23220-3 and ISO/IEC TS 23220-2, respectively.

The sub-phase user identification includes the retrieval of the user attributes and verification of the binding of the holder to the attributes. This can be achieved by organizational non-electronic means (e.g. by physical inspection of physical document and verification of user binding by comparing face image) or by existing electronic identification means, even by a mobile document system. This sub-phase can alternatively be executed after sub-phase mdoc app discovery.

The source of user attributes together with an issuer policy determines the kind of issued mdoc. The retrieval and verification of user attributes from various sources (e.g. a breeder document or self-declared by the holder) is out of scope of this document [see relation (c) in Figure 6]. The source of attributes together with chosen mechanisms to create the credentials and the chosen security mechanisms of the mdoc app form one part to determine the confidence level. Mechanisms of this sub-phase and trust in the source of user attributes are out of scope of this document.

NOTE Guidelines for the identity proofing of a person including levels of such identity proofing are given in ISO/IEC 24760-1 and ISO/IEC 29100.

The mdoc app discovery sub-phase requires an electronic communication between mdoc app and discovery service and involves device detection. This communication can be either a local communication (e.g. via BLE) or a remote communication.

In this sub-phase, eligibility checks shall be performed to determine whether the mobile device and mdoc app with SA-Application match the confidence level of a certain policy or not. If the check passes, the binding between the holder and the mobile device and mdoc app can be verified. In addition, the match between the holder authenticated in user identification sub-phase and the holder authenticated

in mdoc app discovery sub-phase can be verified. Parts of this sub-phase can be omitted in the re-issuance procedure.

Once user identification and mdoc app discovery have been completed, the user attributes and credentials are issued to the target mobile device and mdoc app including SA-Application.

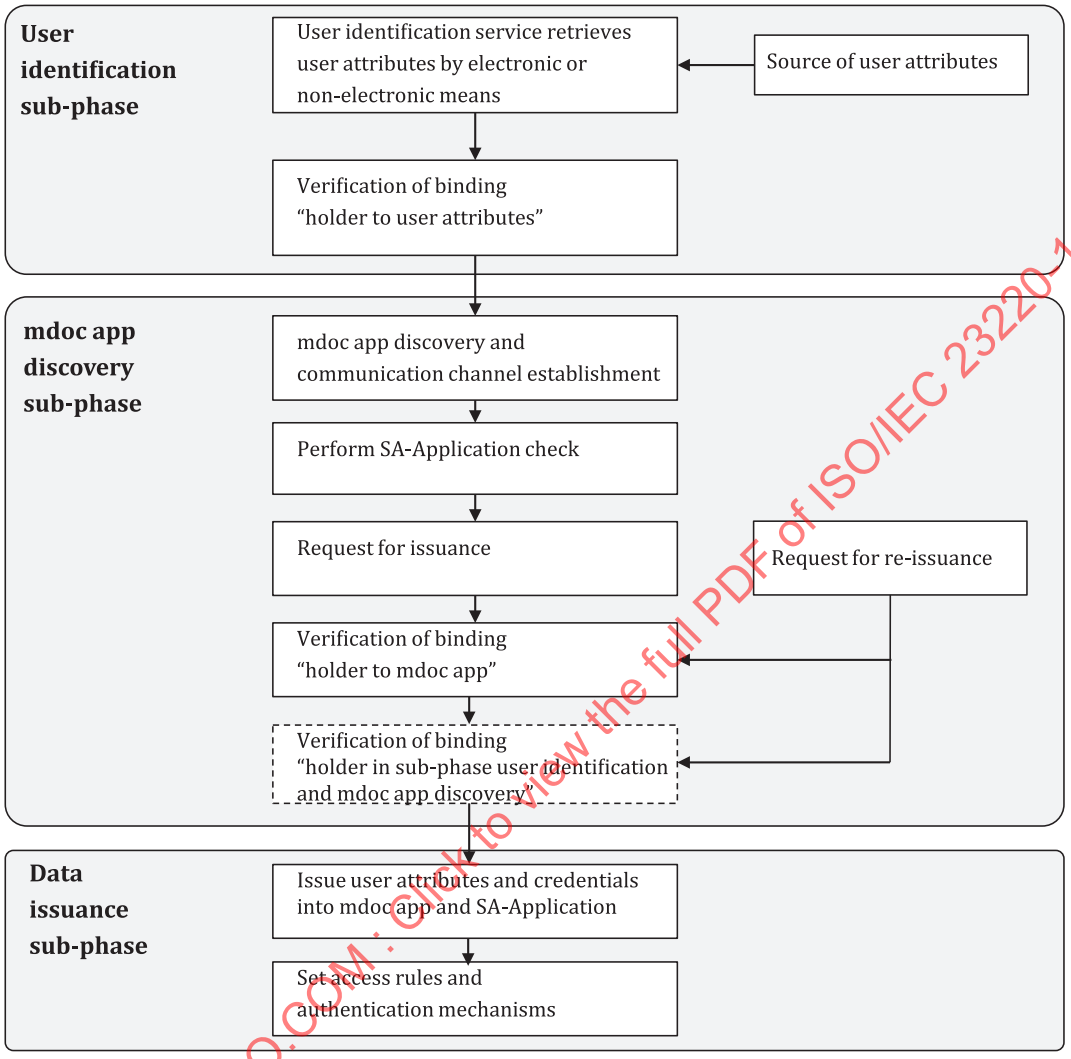



**Figure 5 — Generic sub-phases of issuing procedure in issuing phase**



## 8.3 System architectures in sub-phases user identification and mID-discovery

In the architecture given in Figure 7 the user identification service identifies the holder via an eID document already issued to the holder [see relations (a) and (b) in Figure 6]. The user identification service can retrieve additional attributes from further sources [see relations (c) in Figure 6]. Based on this identification and the established connection to the mdoc app and the mobile device of the holder, the discovery service retrieves the MCD (see interfaces IS-1 and IS-2 in Figure 6) either directly from the mdoc app or online from the MCD attestation service. The release of the MCD can require holder authentication [see relations (d) in Figure 6]. Holder authentication can alternatively be performed in sub-phase issuance. With successful verification of the MCD and with conformance to a respective policy, the discovery service is ready for next sub-phase issuance (see 8.4).

This document distinguishes three kinds of eID documents that determine the protocol required in interface IS-3 of Figure 6:

— The eID document is a mobile document and is available in the mdoc app;

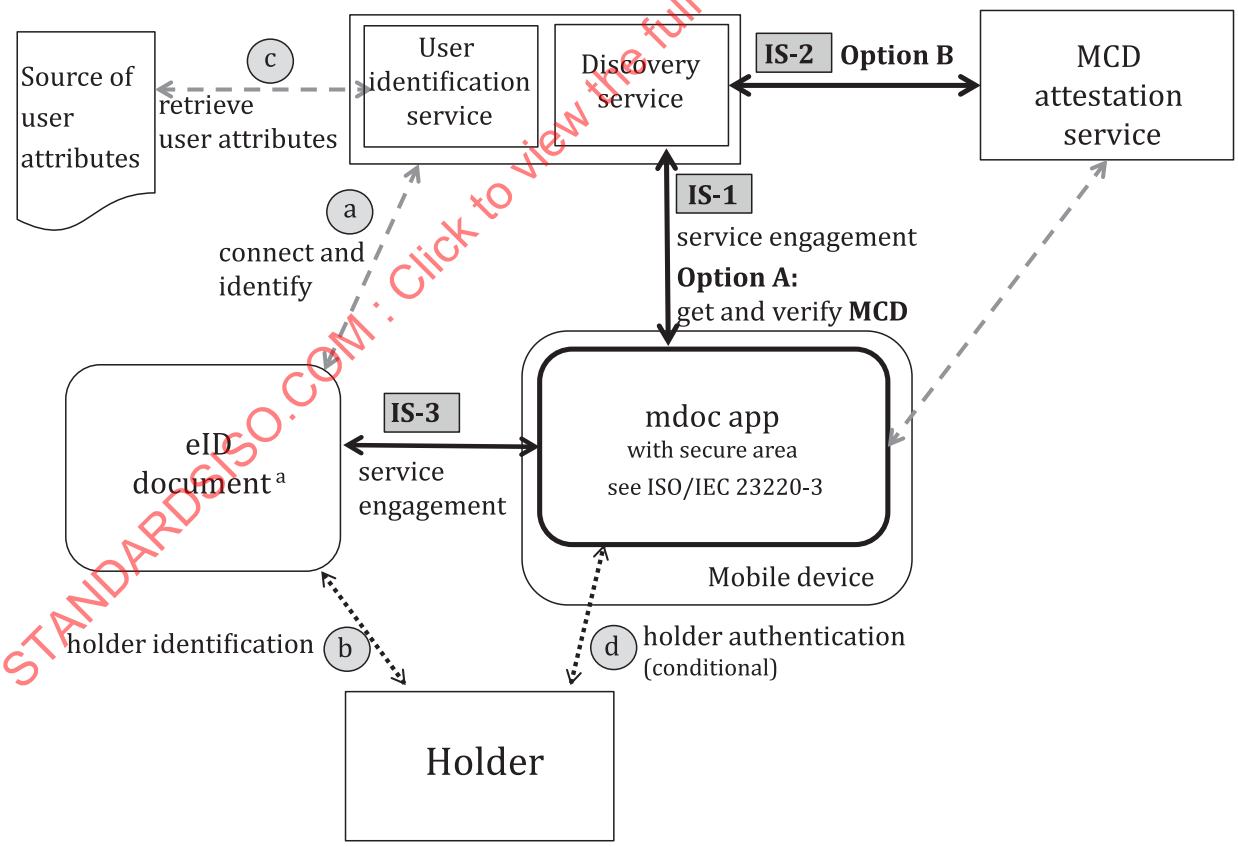
EXAMPLE 1 The holder has successfully installed the mdoc app and has, in addition, a mobile document issued to the mdoc app that is trusted by the issuer operating the user identification service. Such mobile document can be an ID1 sized card with electronic or even non-electronic capabilities. The mdoc app provides a list of supported issuers (e.g. different jurisdictions offering mDL issuance) that the holder can choose and start the issuing process.

— The eID document is a mobile document not controlled by the mdoc app but installed on the same mobile device;

EXAMPLE 2 The holder has successfully installed the mdoc app and has, in addition, a mobile document issued to and controlled by a separate app that is trusted by the issuer. Such mobile document can be an ID1 sized card with electronic or even non-electronic capabilities. The holder browses the website of the issuer and starts the issuing process. The issuer website can provide a list of supported mdoc apps that the holder can choose in accordance to the installed mdoc app.

— The eID document is not a mobile document and the user identification service identifies the holder by means of the eID document through a web-browser or application not residing on the mobile device.

EXAMPLE 3 The holder has successfully installed the mdoc app and browses the issuer's website with a browser of a desktop computer at home. The holder can use any already issued document (electronic or non-electronic) to identify towards the web-service of the issuer. Example of those remote identification means are "Video Identification" or "Video Legitimation" or "Remote in-person vetting". The holder can also select the issuing service via a self-service terminal that, for example, provides means to verify electronic passports physically and electronically (e.g. similar to eGates). Holder authentication can be performed with face image comparison. After user identification, the holder can open the mdoc app and scan a 2D-bar code from the issuer's webservice to do the device and app binding.






**Key**

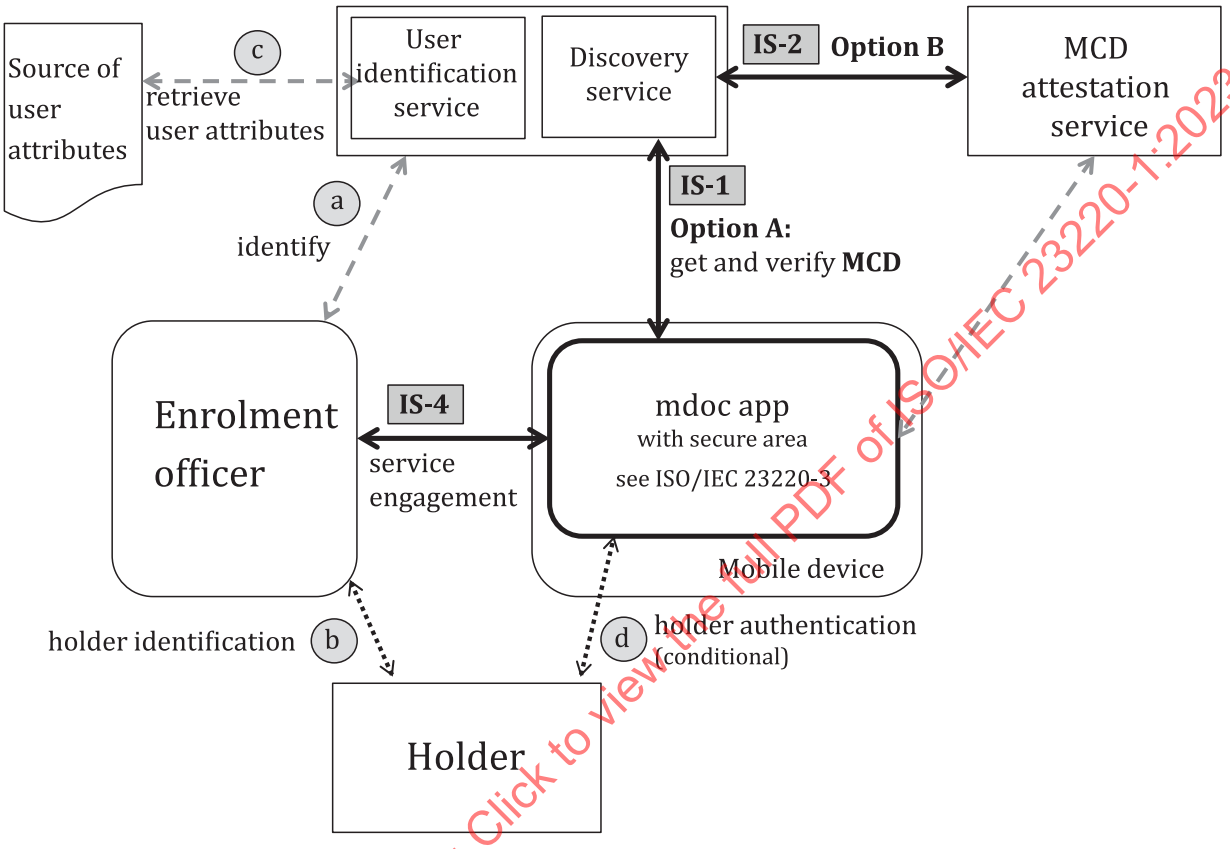
see Figure 1

[a] eID document may include external eID token with or without electronic capabilities.

**Figure 6 — Architecture in sub-phase user identification and mdoc app discovery with eID document**

The architecture in Figure 7 allows the user identification service to identify the holder through manual identification through an enrolment officer. Binding between identified holder and mobile device and mdoc app are achieved by organizational means (see also interface IS-4 in Figure 7).

EXAMPLE 4 The holder has successfully installed the mdoc app and applies for the mobile document at an enrolment office of the issuer. The enrolment officer can manually proof identity via a physical document and start the issuing process into the mobile device and mdoc app that the holder physically presents to the enrolment officer.




**Key**

see Figure 1

**Figure 7 — Architecture with manual identification**

## 8.4 Architectures in sub-phase issuance

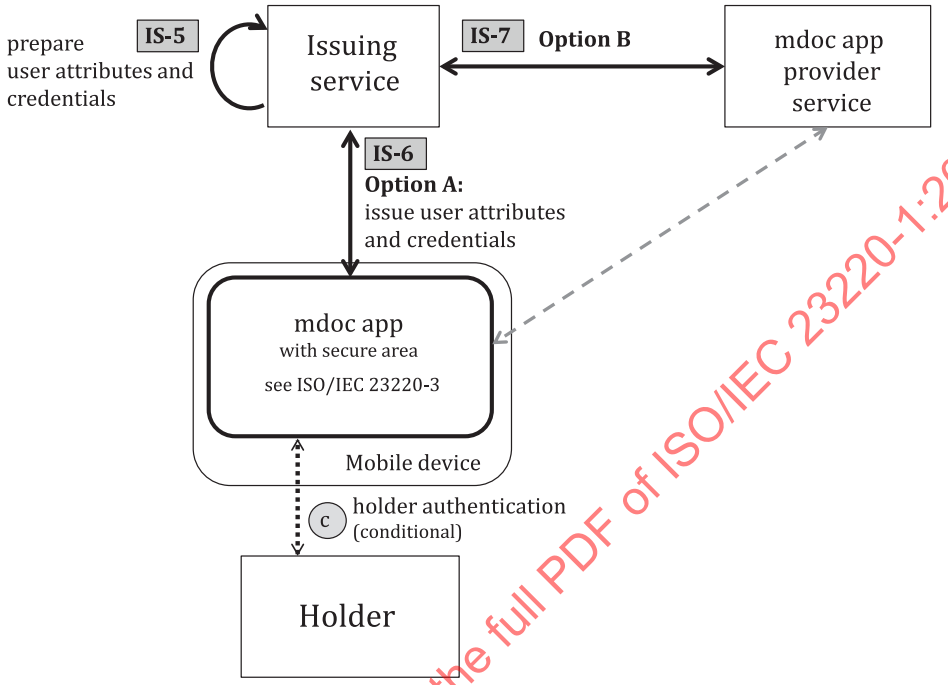
In sub-phases user-identification and mdoc app discovery the user identification service has identified the holder and has all required user attributes assembled. The discovery service has verified the capabilities of the mdoc app or SA-Application or both. Optionally, the discovery service has associated the identified holder to the mdoc app.

In sub-phase issuance the issuing service generates the credentials that are unique to the respective mdoc app and mobile device (see interface IS-5 in Figure 8). The issuing service can either send the user attributes and credentials directly to the mdoc app for installation or indirectly via the mdoc app provider service. The data are locally stored in the mdoc app and secure area (see interfaces IS-6 and IS-7 in Figure 8). A detailed description of issuing attributes and credentials into the SA-Application of the secure area are given in ISO/IEC TS 23320-3.

In case an issuing service chooses an identity or attribute provider service for remote attribute storage, the issuer sends the data together with mobile device and mdoc app information to the respective identity or attribute provider service (see interface IS-8 in Figure 9). That provider finally stores the user attributes and credentials remotely and does the binding of the mobile device and mdoc app to the

user attributes and credentials again either directly (see interface IS-9 in Figure 9) or indirectly via the mdoc app provider service (see interface IS-10 in Figure 9).

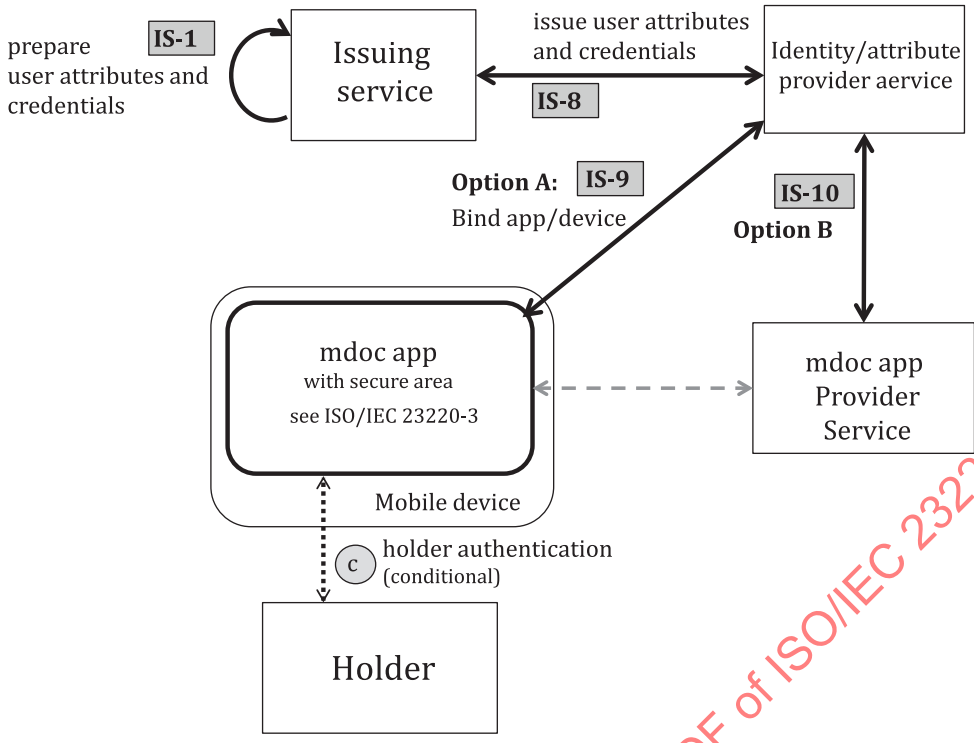
Holder authentication can be required if not given by sub-phases user identification or mdoc app discovery to ensure at a certain level of confidence that the mobile device holder is also the legitimate holder being involved in the attribute issuance process [see relation (c) in Figure 8 and Figure 9].




**Key**

see Figure 1

**Figure 8 — Issuing architecture with local attribute and credential provisioning**



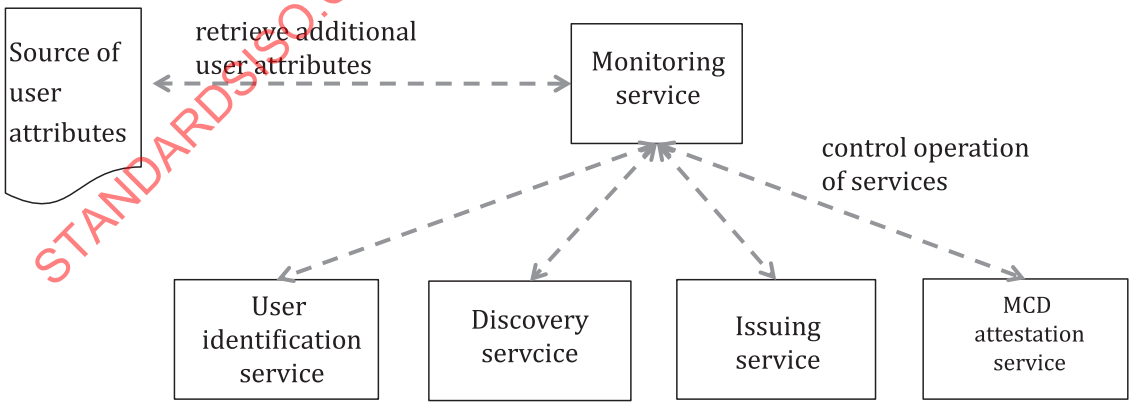

**Key**

see Figure 1

**Figure 9 — Issuing architecture with remote attribute and credential provisioning**

## 8.5 Monitoring service in issuing phase

In addition to the services specified for installation and issuing phase, a monitoring service can be used to control the operations of the services. The monitoring service does not interact with the mdoc app but with the user identification service, the discovery service, the issuing service and the MCD attestation service (see Figure 10). Examples of deployment options using the monitoring service are given in Annex A (see A.4, A.5 and A.6).




**Key**

see Figure 1

**Figure 10 — Issuing architecture with monitoring service**

# 9 On-site identification system architecture in operational phase

## 9.1 General sub-phases of on-site identification system architecture

The on-site identification system architecture is divided into three main sub-phases: initialization sub-phase, device engagement sub-phase and data transmission sub-phase. During initialization the mdoc app and verification application are activated and can require holder and verifier authentication, respectively. The initialization sub-phase is out of scope of this document. During device engagement sub-phase, information required to setup a secure connection between mdoc app and verification application are exchanged. With successful device engagement a transmission channel is established that is used for user attribute requests, user attribute retrievals and server retrieval token. Protocols and interfaces as well as data formats applicable in these sub-phases are specified in ISO/IEC TS 23220-4 and ISO/IEC TS 23220-2, respectively.

## 9.2 On-site identification system architecture with local attribute storage

The system architecture given in Figure 11 adapts the identification process known from physical identity cards, i.e. a holder presents or hands over its identity card to an official or another holder for identification purposes. In the electronic scenario, the electronic identity data are transmitted from the holder's mobile device to the verifier device of the verifying person (see interfaces OP-1 and OP-2 in Figure 11) that in turn proves electronically the integrity, authenticity and validity of the received user attributes and credentials (see interface PO-3 in Figure 12). Before transmission of the user attributes and credentials, the holder approves the operation and can perform an authentication towards the mdoc app [see relation (a) in Figure 11]. The mdoc app can check whether the verification application is authorized to retrieve data.

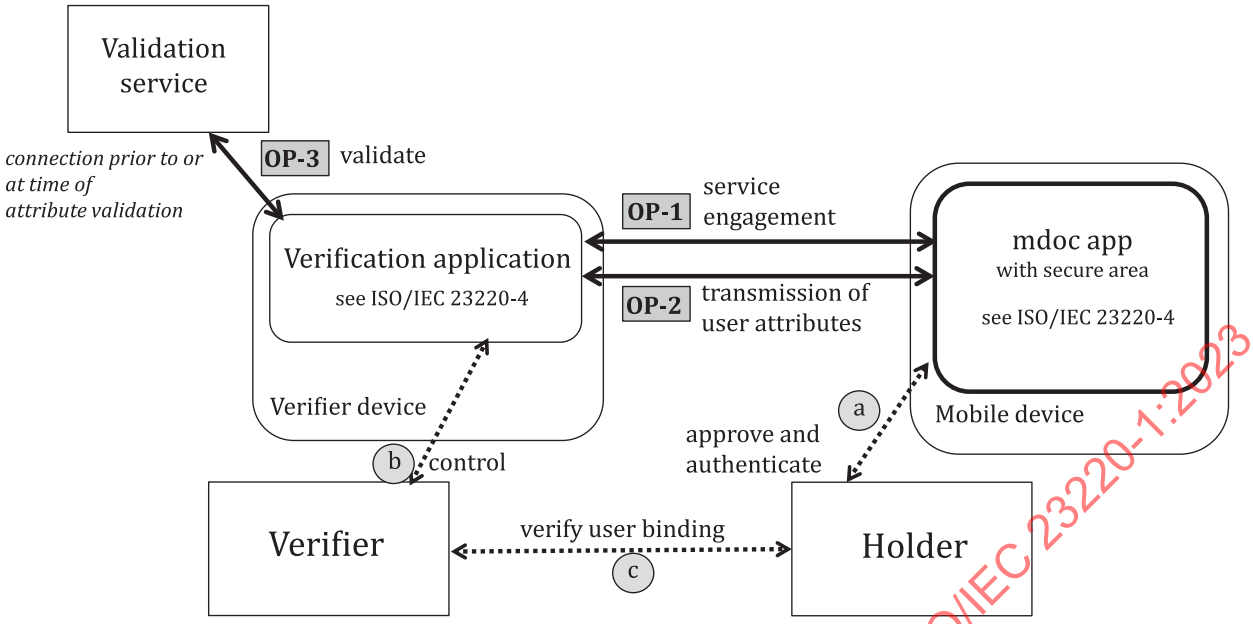
The verifier (e.g. a natural person or part of the verification application) can verify the binding between the holder and transmitted user attributes and credentials, e.g. by performing a visual inspection by a person for comparing the electronic and visualized image with the live image of the holder or by capturing a fingerprint with a fingerprint reading device as part of the verification application [see relations (b) and (c) in Figure 11].

NOTE The binary data of a visualized image of the holder can be considered a static identifier that allows linkability across all usages of the mdoc app and the identity when that data are exposed to a verifier.

As the user attributes and credentials are completely managed by the mdoc app, including the SA-Application, this system architecture allows for an offline operation of the mdoc app. If no real-time validity check is required by the verification application, the system architecture allows for offline operation of the verification application as well. Hence, in this offline scenario the validation service can also be part of the verification application or verifier device.

This system architecture includes the verification application, the validation service and mdoc app with interfaces OP-1, OP-2 and OP-3 in Figure 11.

The validation service of this system architecture provides means to verify the validity of a certain credential and can be operated in separate service or in one single service.




**Key**

see Figure 1

**Figure 11 — On-site identification system architecture with local attribute storage**

## 9.3 On-site identification system architecture with remote attribute storage

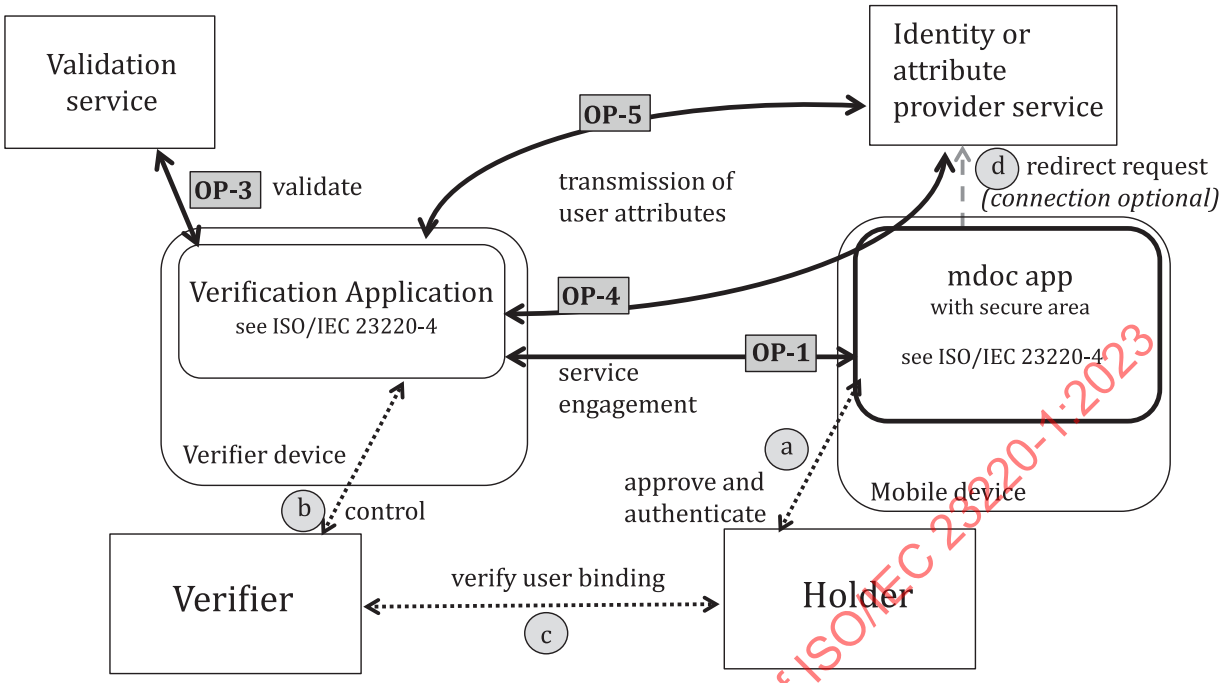
The system architecture given in Figure 12 specifies the same system architecture as described in 9.2, but the user attributes and credentials are partly managed by an identity or attribute provider service. The request of user attributes by the verification application (see interface OP-1 in Figure 12) is upon approval by, and authentication of, the holder redirected to the identity or attribute provider service that in turn releases the user attributes and credentials to the verification application. The communication can be either a direct (see interface OP-5 in Figure 12) or indirect communication via the mdoc app (see interface OP-4 in Figure 12). There are more options to implement the architecture in Figure 12 as given in this subclause.

If authentication of the verification application is required, the verification application can be authenticated by the identity or attribute provider service and the service can check whether the verification application is authorized to retrieve data prior to the release of data. The authentication and the check of authorization can alternatively be processed by the mdoc app prior to redirecting the request to the identity or attribute provider service.

This system architecture requires an online connection of the mdoc app or the verification application. In case of a direct communication between verification application and identity or attribute provider service an online connection of the verification application is required. If no real-time validity check is required by the verification application and an indirect communication to the identity or attribute provider service is chosen, the system architecture allows for offline operation of the verification application but requires an online connection of the mdoc app. In this offline scenario the validation service can also be part of the verification application or verifier device.

This system architecture includes the verification application, the identity or attribute provider service and mdoc app with relations (c), (d), (e) and (h) in Figure 12.

The validation service of this system architecture can be operated by separate services or by one single service. It includes relation OP-3 in Figure 12.




**Key**

see Figure 1

**Figure 12 — On-site identification system architecture with remote attribute storage**



## 10 Remote identification system architecture in operational phase

### 10.1 General

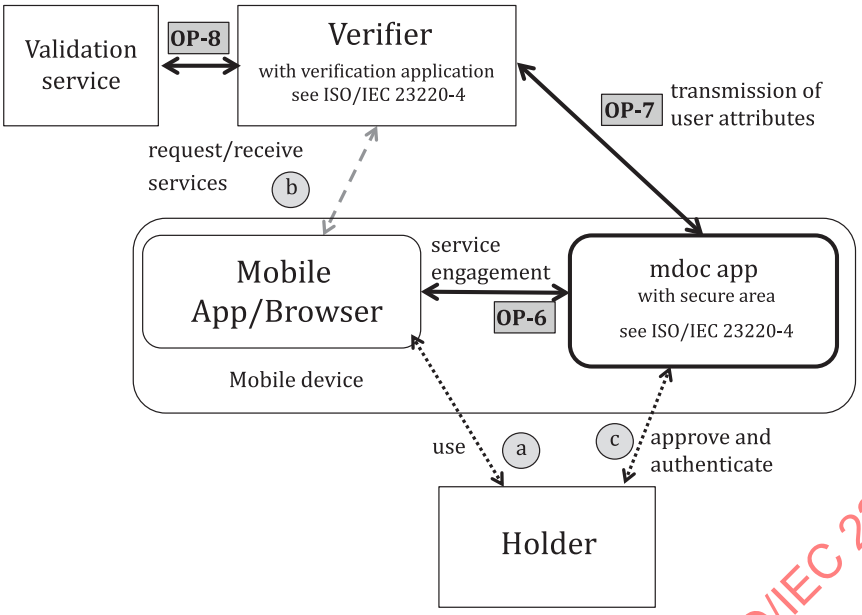
Protocols and interfaces as well as data formats applicable in the architectures of remote identification are specified in ISO/IEC TS 23220-4 and ISO/IEC TS 23220-2, respectively.

### 10.2 Remote identification system architecture with local attribute storage

In the system architectures given in Figure 13 and Figure 14 the verifying party is a remote server providing a service to the holder and operating a verification application. The holder accesses the service either by the mobile browser or a dedicated mobile app running on the mobile device [see relations (a) and (b) in Figure 13]. Upon request by and identification of the verification application of the verifier, the requested user attributes, verifier information as well as a purpose description are provided to the mdoc app (see interface OP-6 in Figure 13) and is presented to the holder for approval and for holder authentication [see relation (c) in Figure 13]. A purpose description can include a brief description for what purpose the user attributes are requested by the verifier.

Holder authentication, i.e. verification of the binding between holder and user attributes and credentials, is controlled by the mdoc app. The authentication mechanism can be processed by the mdoc app itself, by the SA-Application or by additional physical factors of authentication [see relation (c) in Figure 13].

The mdoc app releases the requested and approved user attributes and credentials to the verification application of the verifier (see interface OP-7 in Figure 13) that validates the received data by means of the verification/revocation infrastructure (see interface OP-8 in Figure 13). Optionally, the mdoc app can authenticate and check authorization of the verification application of the verifier prior to the release of data. A protocol providing this attribute release can ensure that attributes are released only to the requesting verification application.

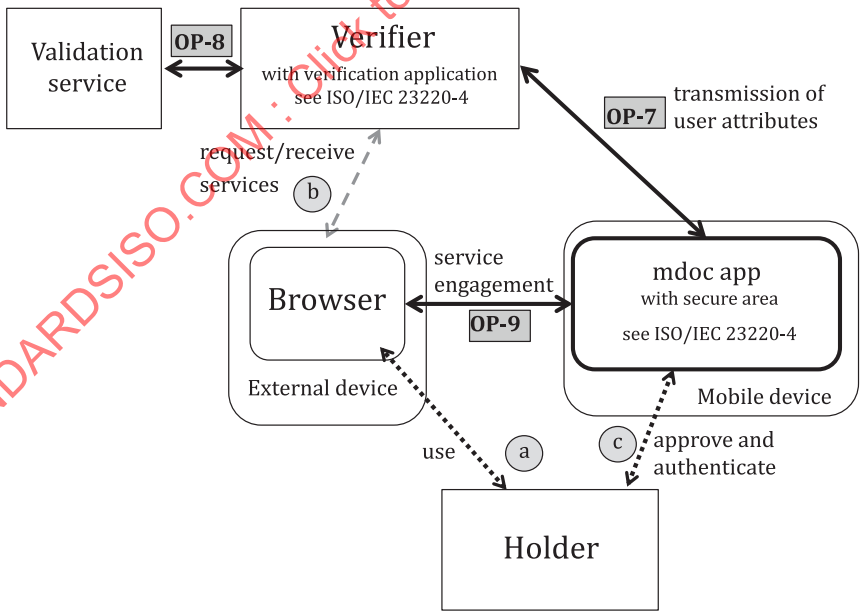



**Key**

see Figure 1

**Figure 13 — Remote identification system architecture with local attribute storage with mobile browser**

Alternatively to the system architecture in Figure 13, the holder can access the remote service by a browser running on an external device (e.g. a desktop computer or other mobile device). In this system architecture (see Figure 14) a binding between the external browser session and the mdoc app of the respective holder by a local communication is required (see interface OP-9 in Figure 14).




**Key**

see Figure 1

**Figure 14 — Remote identification system architecture with local attribute storage with external browser**

This system architectures include the verification application, browser or app and mdoc app with interfaces OP-6, OP-7, OP-8 and OP-9 in Figure 13 and Figure 14. The validation system of this system architecture can be operated by separate services or in one single service and includes interface OP-8 in Figure 13 and Figure 14.

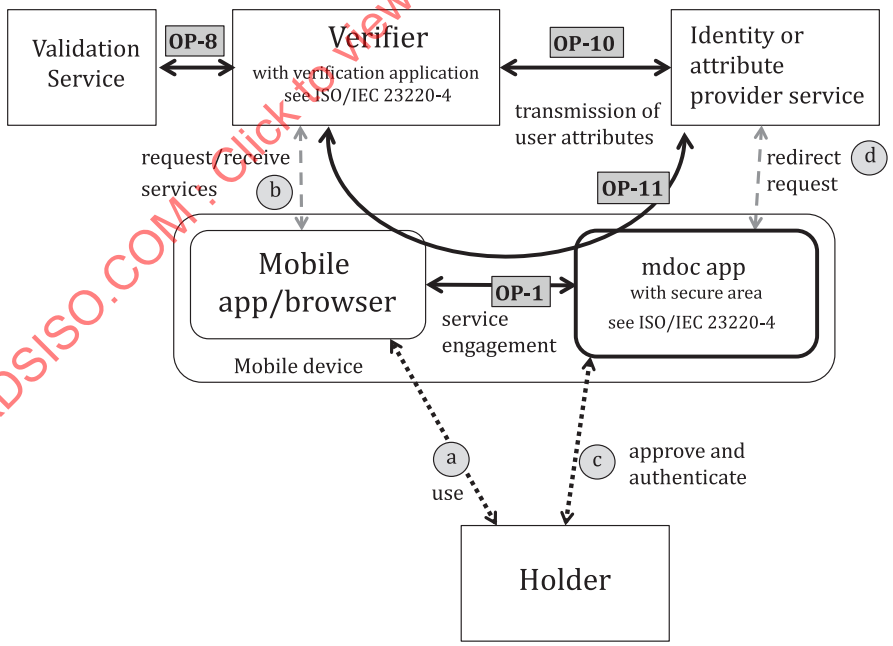
## 10.3 Remote identification system architecture with remote attribute storage

In the system architecture given in Figure 15, the verifying party is a remote server providing a service to the holder and operating a verification application. The holder accesses the service either by the mobile browser or a dedicated mobile app running on the mobile device [see relations (a) and (b) in Figure 15]. Upon request by and identification of the verification application of the verifier the requested user attributes, verifier information as well as a purpose description are provided to the mdoc app (see interface OP-6 in Figure 13) and is presented to the holder for approval and for holder authentication [see relation (c) in Figure 15].

Then the request is re-directed to the identity or attribute provider service [see relation (d) in Figure 15] that provides the requested attributes to the verifier either in a direct communication between verifier and identity or attribute provider service (see interface OP-10 in Figure 15) or in an indirect communication (see interface OP-11 in Figure 15).

NOTE In the remote identification system architecture with remote attribute storage the identity or attribute provider service is present in each transaction; therefore, the identity or attribute provider service knows when an mdoc app is used and what data are shared (i.e. data include transaction data, user attributes or credentials). If tracking is a concern, the identity or attribute provider service is advised to implement mitigating strategies to ensure the mdoc app and the holder are not tracked (e.g. architecture given in Figure 17).

If authentication of the verification application is required, the mdoc app or the identity or attribute provider service can authenticate and check the authorization of the verification application of the verifier prior to the release of data.



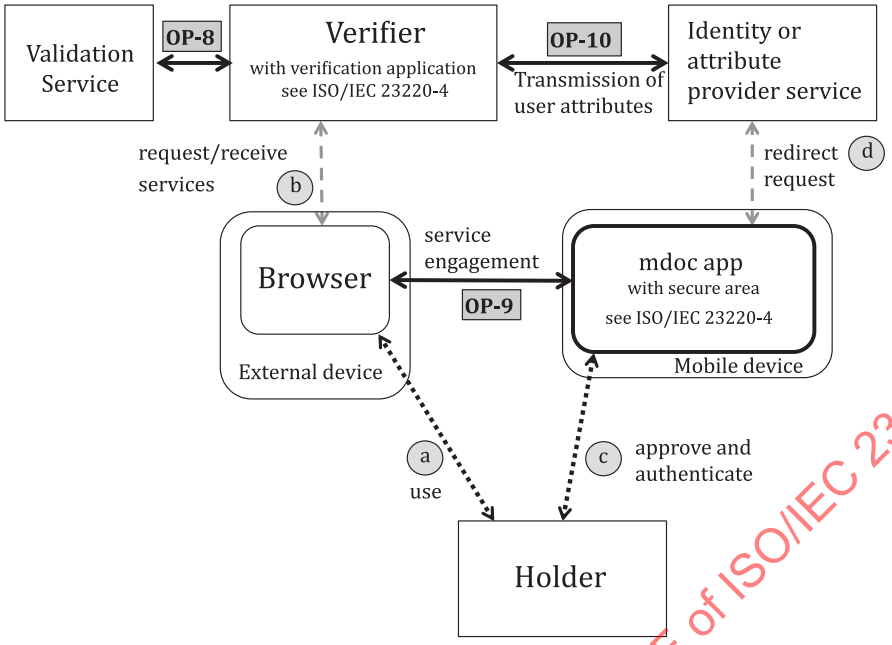

**Key**

see Figure 1

**Figure 15 — Remote identification system architecture with remote attribute storage and mobile browser**

In contrast to the system architecture described in Figure 15, the holder can access the service of the verifier by a browser running on an external device (e.g. a desktop computer). This system architecture

(see Figure 16) requires a binding between the browser session (see interface OP-9 in Figure 16) and the mdoc app of the respective holder by a local communication.

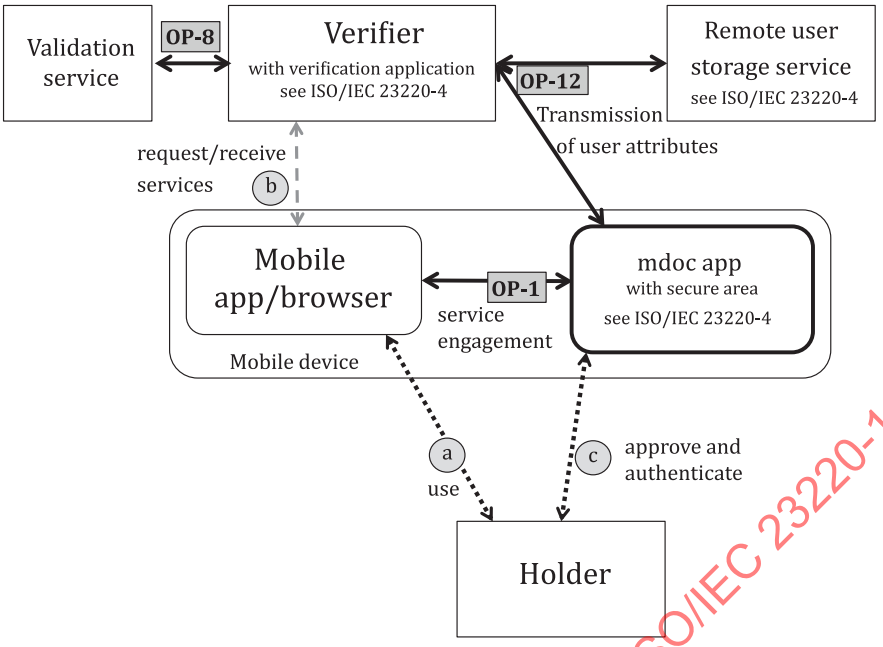



**Key**

see Figure 1

**Figure 16 — Remote identification system architecture with remote attribute storage and external browser**

A mobile document system can apply a remote user storage service instead of an identity or attribute provider service as described in Figure 17. In this case, a holder transmits user attributes via mdoc app and gives permit to a verifier to get access to the holder's remote user storage. Then, a verifier can get access to the holder's remote user storage and retrieve additional user attributes (see interface OP-12 in Figure 17). The interface OP-9 (see Figure 16) can also be supported in this architecture.




**Key**

see Figure 1

**Figure 17 — Remote identification system architecture with remote user storage**

The system architectures include the verification application, the identity or attribute provider service and mdoc app with interfaces OP-6, OP-8, OP-9, OP-10, OP-11 and OP-12 in Figure 15, Figure 16 and Figure 17.

The validation service of the system architectures can be operated by a separate service or by one single service and includes interfaces OP-8 in Figure 15 and Figure 16.

# Annex A
(informative)

# Examples of deployment options for issuers in issuing phase

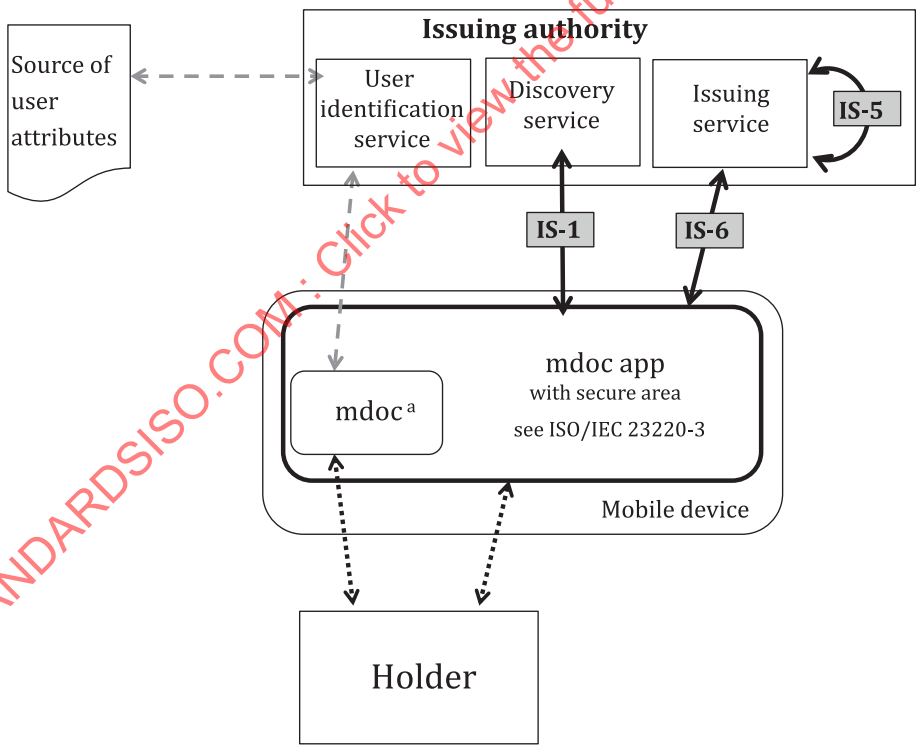
## A.1 General

This document specifies protocols and services as building blocks for issuing and operating mdocs as well as for installing an mdoc app. The building blocks allow for the deployment of such services in a number of ways. This annex describes typical deployment examples of services in the issuing phase.

## A.2 Deployment example for issuing with local user attribute storage

An issuing authority can operate the user identification service, the discovery service and the issuing service by itself. The policy of the issuing authority can also require the local storage of the user attributes, i.e. without using remote identity or attribute provider service.

User identification can be done by means of an already issued mobile document of the mdoc app or alternatively, the issuing authority can use an eID document not managed by the mdoc app (see examples in Figure A.1 and Figure A.2).

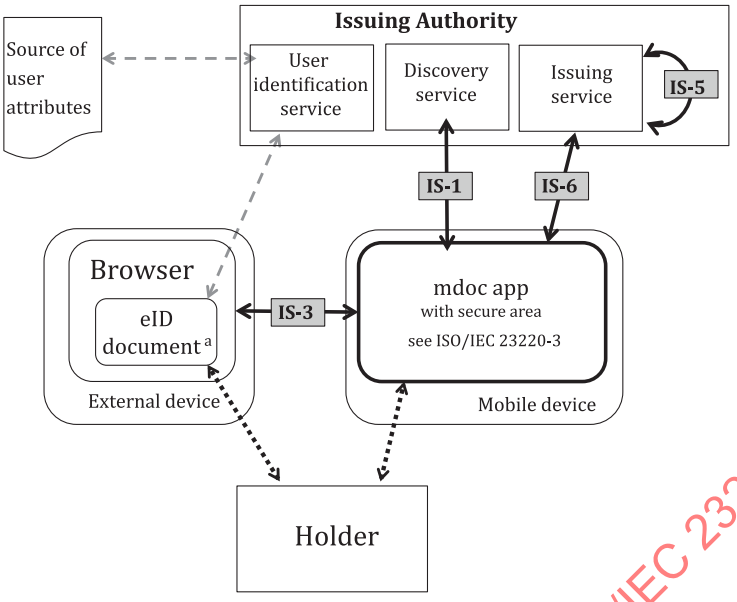



**Key**

see Figure 1

a Mobile document may include external eID token with or without electronic capabilities.

**Figure A.1 — Example of deployment for issuing with local user attribute storage and mobile document**




**Key**

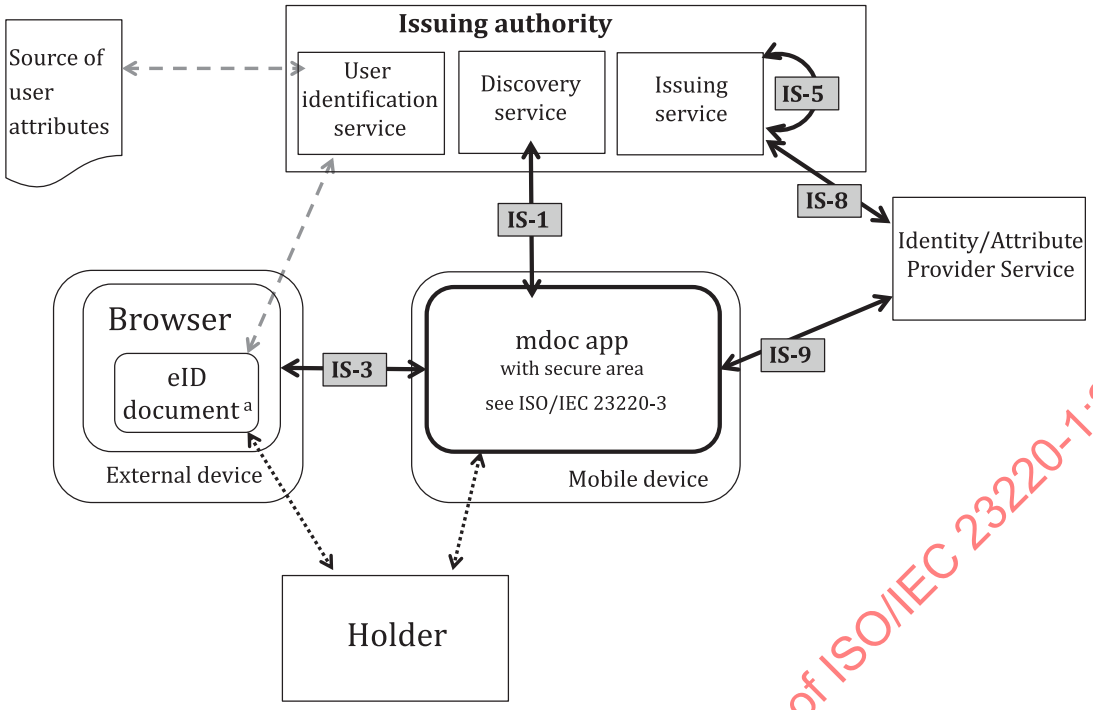
see Figure 1

[a] eID document may include external eID token with or without electronic capabilities.

**Figure A.2 — Example of deployment for issuing with local user attribute storage and eID Document**

## A.3 Deployment example for issuing with remote attribute storage

In this deployment example, the issuing authority operates the user identification service, the discovery service and the issuing service by itself. The policy of the issuing authority allows for the remote storage of user attributes at an identity or attribute provider service (see example in Figure A.3).




**Key**

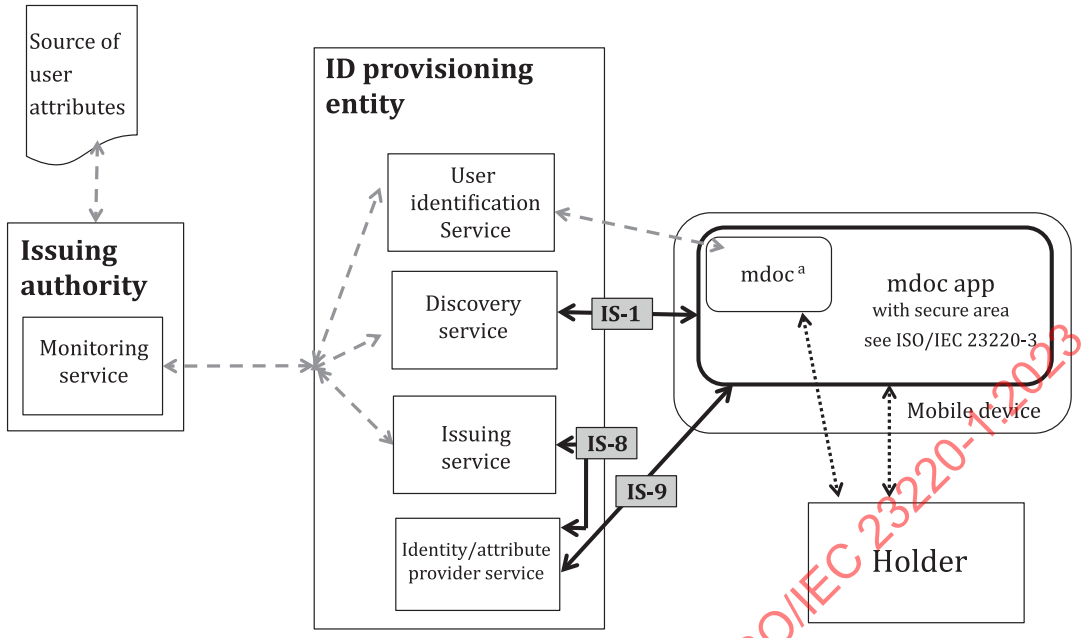
see Figure 1

[a] eID document may include external eID token with or without electronic capabilities.

**Figure A.3 — Example of deployment for issuing with remote user attribute storage and eID Document**

## A.4 Deployment example for issuing with ID-provisioning entity

An issuing authority can choose to contract with an ID-provisioning entity that operates all or parts of the required services on behalf of the issuing authority. In the example (see Figure A.4) the ID-provisioning entity operates user identification service, discovery service, issuing service and an identity provider service for remote user attribute storage. The issuer has established a trust or business relationship or both with the ID-provisioning entity and controls the issuing process by means of a monitoring service. The ID-provisioning entity can in addition provide services of installation phase, e.g. the MCD attestation service (see example in Figure A.5) or Open Firmware Loader (OFL) (see examples in Figure A.4 and Figure A.5).

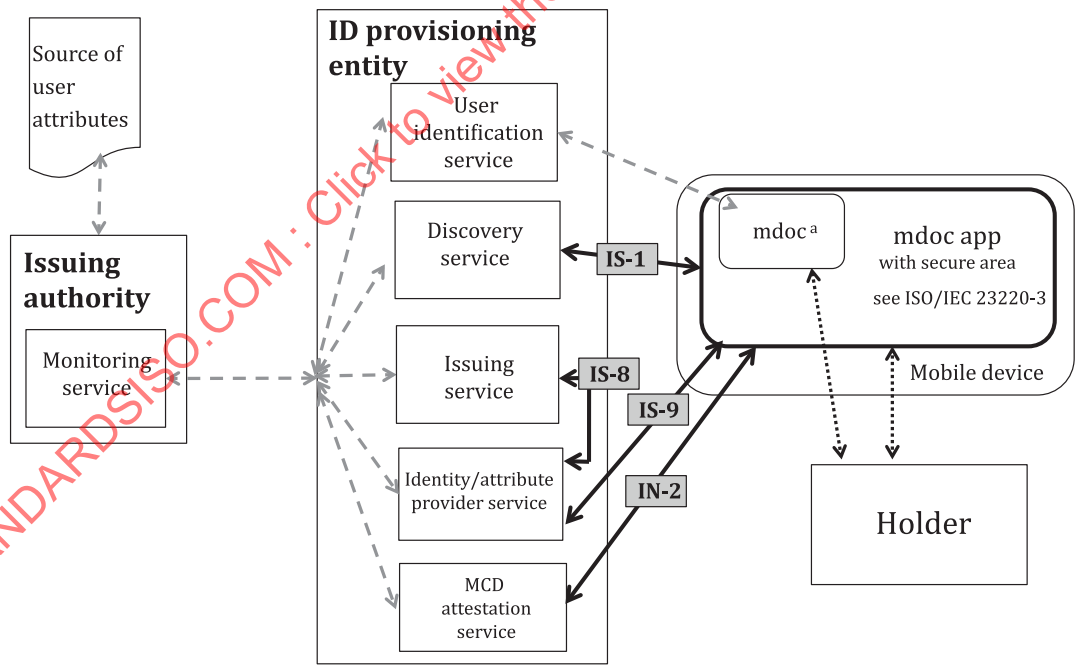



**Key**

see Figure 1

[a] Mobile document may include external eID token with or without electronic capabilities.

**Figure A.4 — Example of deployment for issuing with ID-provisioning entity**




**Key**

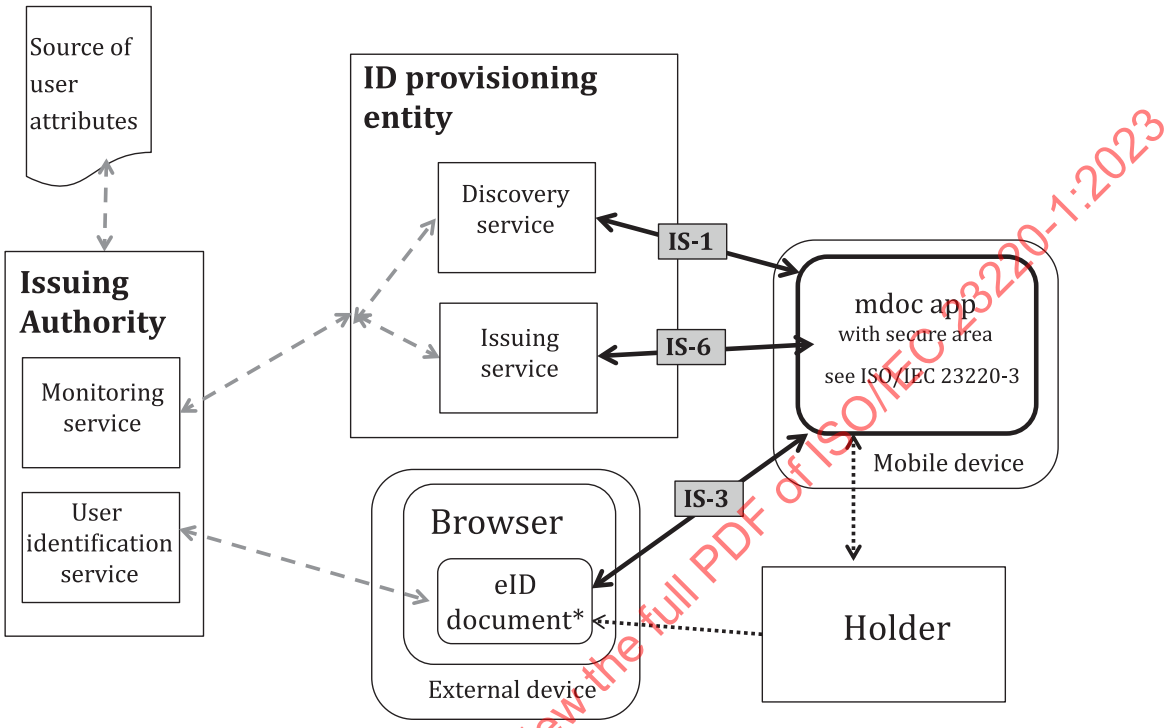
see Figure 1

[a] Mobile document may include external eID token with or without electronic capabilities.

**Figure A.5 — Example of deployment for issuing and installation with ID-provisioning entity**

## A.5 Deployment example for issuing with user identification service operated by issuer

As a further example the issuing authority can operate the user identification service by itself and can choose to let the remaining service to be operated by the ID-provisioning entity (see example in Figure A.6).




**Key**

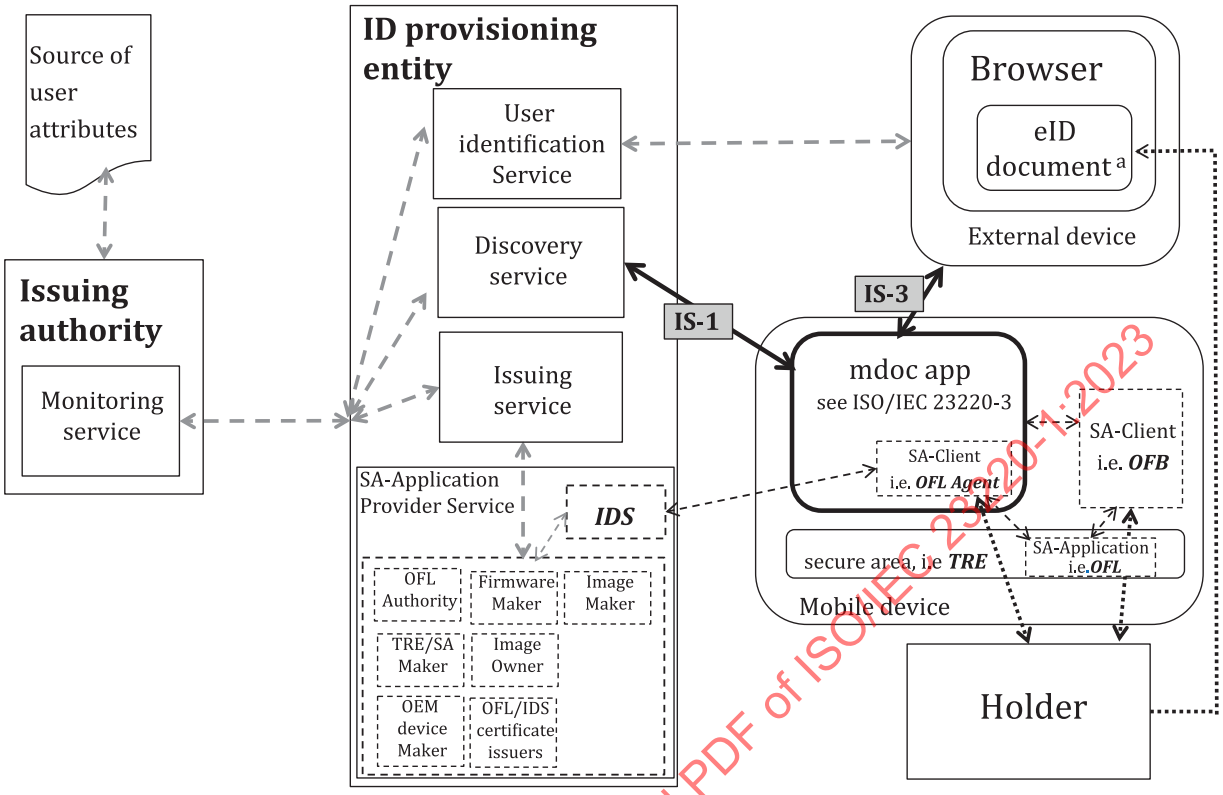
see Figure 1

[a] Mobile eID document may include external eID token with or without electronic capabilities.

**Figure A.6 — Example of deployment for issuing with user identification service operated by issuer**

## A.6 Deployment example for issuing with Open Firmware Loader (OFL)

The example given in Figure A.7 is based on a Trusted Connectivity Alliance publication[31] and describes general functions and actors involved during the process of loading firmware into a TRE. The OFL agent, i.e. software integrated in the mobile equipment, communicates with the Image Delivery Server (IDS) to load the images into the TRE that is the secure container encapsulating TRE firmware (including OS, SA-Application and user attributes and credentials).




**Key**

see Figure 1

[a] eID document may include external eID token with or without electronic capabilities.

**Figure A.7 — Example of deployment for issuing and installation with Open Firmware Loader (OFL)**

The overall OFL workflow as envisioned by GlobalPlatform and Trusted Connectivity Alliance [18][20][21][22][23][31] is as follows:

The IDS function can be assigned to different actors (i.e. TRE Maker, OEM Device Maker, Image Maker and Image Owner). The IDS is the function in charge to deliver Bound Images to the OFL agent or to the OEM Device Maker. The OFL Authority generates certificates granting access rights to a TRE.

The Image Owner defines requirements and directives for user services to the Image Maker. The Image Owner provides the user credentials to the Firmware Maker via the Image Maker or directly with an interface. These credentials are different from the user attributes and credentials managed by the mdoc app in the mobile document system. The Image Maker gets a Firmware from a Firmware Maker supporting the requirements and the input data from an Image Owner. The Image Maker encapsulates the Firmware within a secure container called the Unbound Image. The Unbound Image is provisioned to the IDS under control and agreement with the Image Owner.

The OFL Certificate Issuers (CIOFL) and IDS Certificate Issuers (CIIDS) can manage multiple Public Key Infrastructures (PKI) ensuring trusted exchanges between the Actors and the Functions. The OFL CIOFL issues all certificates to the OFL and the Certificates ensuring a trustable collaboration with other Functions depending to IDS Certificate Issuers. The IDS CIIDS issues all certificates to the IDS.

The TRE Maker manufactures the TRE according to specifications from Industry or Standardization Organization. The OEM Device Maker manufactures an OEM device embedding the OFL agent and the TRE provisioned from the TRE Maker. The OEM Device Maker implements the OFL Agent and the Open Firmware Block (OFB), which bridges the IDS and OFL running in the TRE.

The holder interacts with the OFB. The holder can be prompted for giving explicit consent validating some OFL operations or retrieving specific credentials that are required for initiating the OFL operations from the verifier.

The OFL agent is the Function in charge of supporting the procedure of a data flow from IDS to OFL agent Interface. This function manages a certificate used for authentication with the IDS and gets or forwards meta-data between the IDS and the OFB or between the OFL Agent and the OFB.

The OFL agent can be a function performed by e.g. MCD attestation service, SA-Application provider. The TRE is a secure environment able to run the instance of the Firmware. The TRE can be compliant with the Virtual Primary Platform (VPP) specifications.

The OFB implements the requirements from Industry or a Standardization Organization. The OFB is usually use case dependent and can interact with the holder through a man machine interface. The OFB collaborates with the OFL Agent.

# Annex B
(informative)

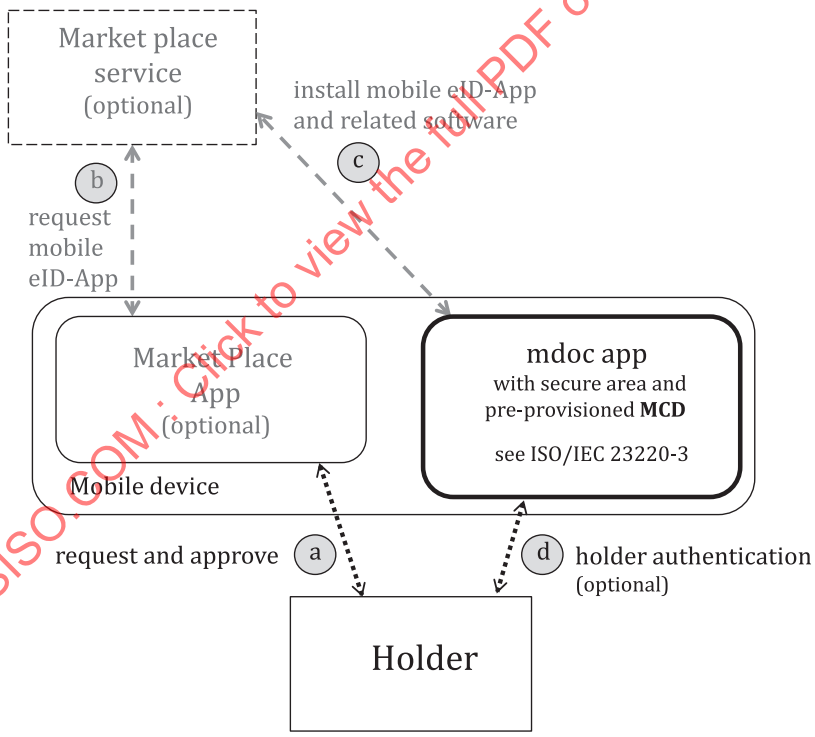
# Examples of deployment options in installation phase

## B.1 General

This document specifies protocols and services as building blocks for issuing and operating mdocs as well as for installing a mdoc app. The building blocks allow for the deployment of such service in a number of ways. This annex describes typical deployment examples of services in the issuing phase.

## B.2 Deployment example with pre-installed mdoc app and MCD

The mdoc app can be pre-installed on the mobile device and the MCD is created during pre-installation or installation (see Figure B.1). The MCD can contain the complete set of data or can contain a reference for online retrieval of the MCD from the MCDAttestation Service.



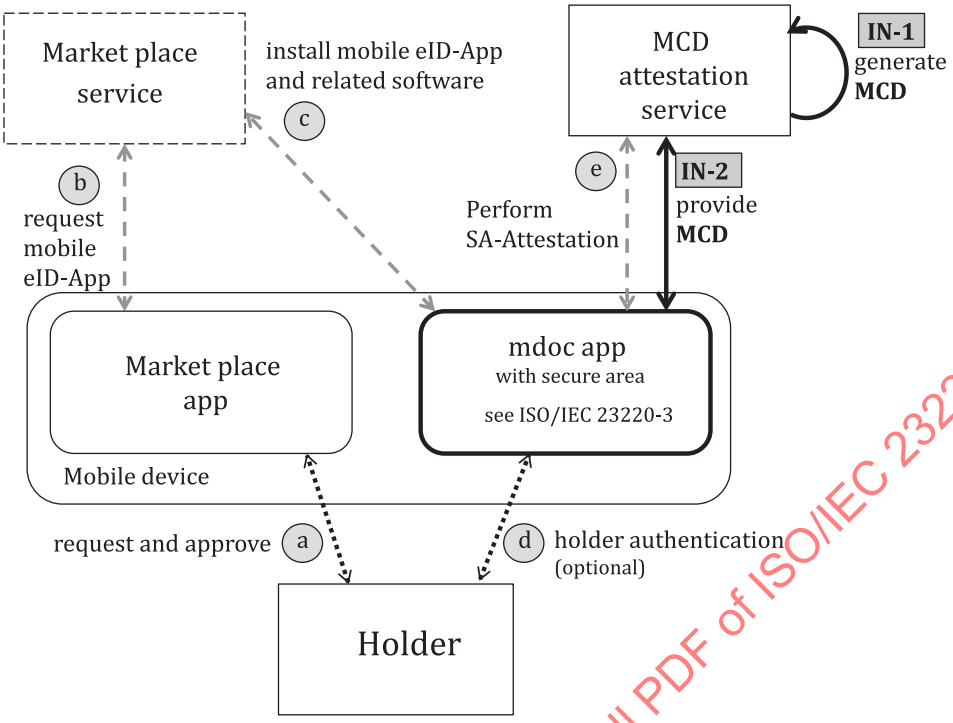

**Key**
see Figure 1

**Figure B.1 — Installation architecture with pre-installed mdoc app and MCD**

## B.3 Deployment example with MCD attestation service only

Information about device capabilities are made available by means of device functionalities and mdoc app functionalities to the MCD attestation service [see relation (e) in Figure B.2]. The service creates the MCD including the SAAOs and writes either the full MCD data into the mdoc app or the appropriate reference to the MCD (see interfaces IN-2 and IN-1 in Figure B.2). In the latter case the MCD attestation

service maintains the full MCD for online retrieval. The respective SA-Application and SAAOs are already installed and available to the mdoc app.




**Key**

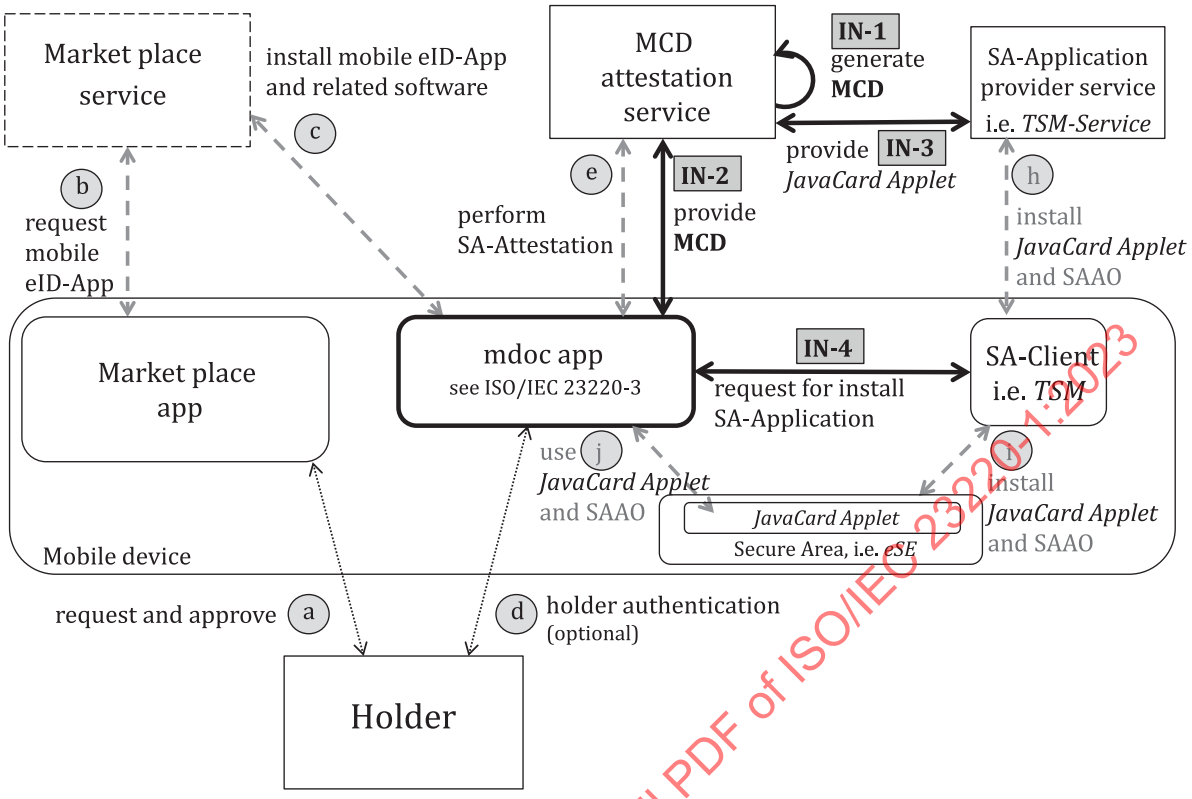
see Figure 1

**Figure B.2 — Installation architecture with MCD attestation service**



## B.4 Deployment example for installation phase with JavaCard Applets onto eSE

In this example, the secure area is realized as an embedded Secure Element. The SA-Application provider service allows for the provisioning of an mdoc app-specific Java Card applet (i.e. the SA-Application) via a TSM-Service and related TSM-App (i.e. the SA-Client) onto a Java Card and GlobalPlatform conformant secure area. Loading, installation and initial personalization of a Java Card applet are specified in accordance to GlobalPlatform Specification [see relations (h) and (i) in Figure B.3]. In an initial step, not necessarily part of the installation sequence, the Java Card applet of the mdoc app provider must be made available to the TSM-Service (see interface IN-3 in Figure B.3). During installation of mdoc app the app requests the installation of the respective Java Card applet to the TSM-App already installed on the mobile device (see interface IN-4 in Figure B.3). The TSM-App has administrative access rights to the secure area, i.e. Issuer Security Domain or Sub-Security Domain, and controls the loading, installation and personalization of the Java Card applet according to GlobalPlatform. With the successful installation of the Java Card applet the mdoc app can start using the Java Card applet on application level [see relation (j) in Figure B.3].




**Key**

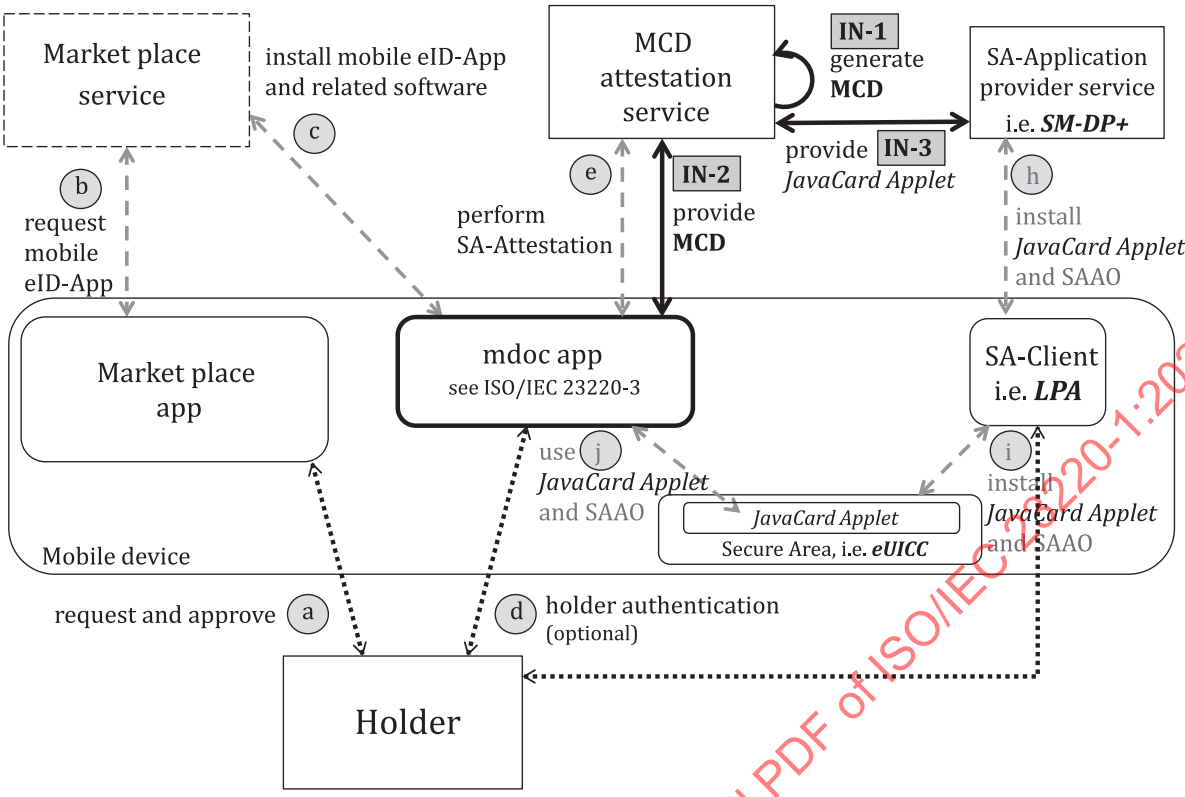
see Figure 1

**Figure B.3 — Example of deployment for installation of Java Card applets onto eSE**

## B.5 Deployment example for installation phase with Java Card applets onto eUICC

The eUICC market is strongly growing. Due to its highly standardized interface given in[29] it can provide a secure area for secure mobile identities as part of an eSIM profile. In future, the Common Security Domain is able to add services besides the usual MNO profiles and to run them in parallel.

In this example, the secure area is realized as part of an MNO eSIM Profile within an eUICC. The holder obtains an MNO contract and installs the corresponding eSIM profile including the SA-Application (e.g. Java Card Applet) on the eUICC by means of the SM-DP+ backend system. The mdoc app must be downloaded by the holder from a market place service. Once the mdoc app is installed, the mdoc app performs an eligibility check. For this deployment example, the eligibility will provide the information, that the SA-Application has been already installed as part of the eSIM-profile and is ready for use. Additionally, the eligibility check provides information concerning certification of the eUICC (see [27] [28][30]). Information concerning the device and the eUICC can be collected directly from the eUICC or indirectly via MCD attestation service (see interface IN-2 in Figure B.4).




**Key**

see Figure 1

**Figure B.4 — Example of deployment for installation of JavaCard Applets onto eUICC**