Deleted:

ISO/IEC TC JTC1/SC17 N

Deleted: 2022-06-30¶

Date 2022-10

Deleted: 2021-09-21

ISO/IEC FDIS 23220-1:2022(E)

Deleted: DIS

Deleted: 2021

ISO/IEC TC JTC1/SC 17/WG 4

Secretariat: BSI

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 personnelle — Briques techniques pour l'identification par dispositifs mobiles

Deleted:
Deleted: DIS
Deleted: 2021
Deleted: 2016

Deleted: ii © ISO/IEC 2021 – All rights reserved¶

Deleted: DIS

Deleted: 2021

Contents

Foreword v

Introduction vi

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Symbols and abbreviations 13

5 Design and privacy principles of mobile eID-Systems 13
5.1 Design principles 13
5.2 Privacy and security principles 14

6 General life-cycle phases and components of mobile eID-Systems 15
6.1 Life-cycle phases of mobile eID-Systems 15
6.2 Components of a mobile eID-System 16

7 Generic system architectures of mobile eID-Systems in installation phase 18

8 Generic system architectures of mobile eID-Systems in issuing phase 20
8.1 Source of user attributes 20
8.2 Generic sub-phases of issuing phase 21
8.3 System architectures in sub-phases user identification and mID-discovery 22
8.4 Architectures in sub-phase issuance 24
8.5 Monitoring service in issuing phase 25

9 On-site identification system architecture in operational phase 26
9.1 General sub-phases of on-site identification system architecture 26
9.2 On-site identification system architecture with local attribute storage 26
9.3 On-site identification system architecture with remote attribute storage 27

10 Remote identification system architecture in operational phase 28
10.1 Remote identification system architecture with local attribute storage 28
10.2 Remote identification system architecture with remote attribute storage 29

Annex A (informative) Examples of deployment options for Issuers in issuing phase 32

A.1 General 32

A.2 Deployment example for issuing with local user attribute storage 32

A.3 Deployment example for issuing with remote attribute storage 33

A.4 Deployment example for issuing with ID-Provisioning Entity 33

A.5 Deployment example for issuing with user identification service operated by issuer 34

A.6 Deployment example for issuing with Open Firmware Loader 35

A.7 Deployment example for installation phase with JavaCard Applets onto eSE 36

A.8 Deployment example for installation phase with JavaCard Applets onto eUICC 37

Annex B (informative) Identity proofing 39

Deleted: © ISO/IEC 2021 – All rights reserved iii¶

B.1 Introduction 39
B.2 Identity derivation based on secure electronic identity documents 39
B.2.1 General 39
B.2.2 Authentication of the identity data of the user 39
B.2.3 Binding between the identity data and the user 40
B.3 Identity derivation using secure identity documents 40
B.3.1 General 40
B.3.2 Optical authentication of secure identity document 40
B.3.3 Binding between the secure identity documents and the user 41
B.4 Security prospective: attended vs. unattended identity derivation 41
B.5 Example of enrolment procedure with additional physical factor of authentication 41
Annex C (informative) Additional physical factor(s) of authentication 43
C.1 Introduction 43
C.2 Electronic MRTD 43
C.3 Electronic identity card 43
C.4 Secure identity document with optical authentication features 45
C.5 Biometric authentication 45
Bibliography 47

Deleted:
Deleted: DIS
Deleted: 2021
Deleted: ¶
Deleted: iv © ISO/IEC 2021 – All rights reserved¶

Deleted: DIS

Deleted: 2021

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.

Deleted: ¶

Deleted: © ISO/IEC 2021 – All rights reserved v¶

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;

Deleted:
Deleted: DIS
Deleted: 2021
Deleted: today
Deleted: governmental
Deleted: -Cards
Deleted: private
Deleted: any kind of
Deleted: of
Deleted:
Deleted: may
Deleted: (SOURCE: NIST SP 800-157: Guidelines for Derived PIV Credentials)[
Deleted:
Deleted:
Deleted: this
Deleted: of standards
Deleted: (1
Deleted: , (2
Deleted: , (3
Deleted: , and (4
Deleted: vi © ISO/IEC 2021 – All rights reserved¶

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.

Deleted: DIS
Deleted: 2021
Deleted: In addition, it adds means to establish Trust On First Use (TOFU).¶
Deleted: seriesinherits
Deleted:
Deleted:),;
Deleted:
Deleted:),;
Deleted:
Deleted:);
Deleted:);—
Deleted:)..
Deleted: © ISO/IEC 2021 – All rights reserved vii¶

Deleted: DIS

Deleted: 2021

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.

Deleted: This document

2 Normative references

There are no normative references in this document.

Deleted: 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.¶ ¶

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]

Deleted:

Deleted: .]

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.]

Deleted:

Deleted: -

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

Deleted: © ISO/IEC 2021 – All rights reserved 1¶

[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

Deleted: DIS
Deleted: 2021
Deleted:
Deleted:
Deleted:
Deleted:
Deleted: -
Deleted: was deleted and
Deleted:
Deleted:
Deleted:
Deleted: .]
Deleted: ¶
Deleted: - added
Deleted: "holder
Deleted:
Deleted: 2 © ISO/IEC 2021 – All rights reserved¶

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 eID.

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 eID.

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

Deleted: DIS
Deleted: 2021
Deleted: (i
Deleted: (ii
Deleted: (iii
Deleted: (iv
Deleted: (v
Deleted: [14
Deleted: (3.19)
Deleted: documents
Deleted: Example
Deleted: 4 © ISO/IEC 2021 – All rights reserved¶

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

Deleted: DIS
Deleted: 2021
Deleted: ¶
Deleted: : Guidelines for Derived PIV Credentials]
Deleted: [SOURCE: SD Card Association, Technical Committee: SD Specifications Part 1 Physical Layer Simplified Specification, Version 6.00, April 10th, 2017.]¶
Deleted: :
Deleted: 2
Deleted: 2
Deleted: Provisioning Service
Deleted:
Deleted: 6 © ISO/IEC 2021 – All rights reserved¶

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 23220-2, ISO/IEC 23220-3, ISO/IEC 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

Deleted:
Deleted: DIS
Deleted: 44
Deleted: :
Deleted: Aabbreviated
Deleted: abbreviations
Deleted:
Deleted: parts 2 to 4 of ISO/IEC 23220 series [13][14][15].
Deleted: © ISO/IEC 2021 – All rights reserved 7¶