Technical Specification

ISO/IEC TS 23220-2

First edition
2024-11

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

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

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

Partie 2: Objets de données et règles d'encodage pour les systèmes eID génériques

Reference number
ISO/IEC TS 23220-2:2024(en)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

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

Introduction

Electronic ID-Applications (eID-Apps) are today 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, governmental 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 private sector with any kind of 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 of 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 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, being as generic as possible helps them 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 is performed by the available transmission channels. Typical local communication channels are Bluetooth Low Energy (BLE), Near Field Communication (NFC) and 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 extend the ISO/IEC 23220 series.

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

a) secure channel establishment;

b) API call serialization method;

c) data element naming convention; and

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 (mDL) applications whereby ensuring backward compatibility with ISO/IEC 18013-5.

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

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

1 Scope

This document specifies data objects and encoding rules of generic eID-Systems in terms of building blocks for mobile document system infrastructures, and standardizes generic data models for data exchanges between mdoc apps and verification applications.

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

2 Normative references

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

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

ISO 3166-2, *Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*

ISO/IEC 5218, *Information technology — Codes for the representation of human sexes*

ISO/IEC 7816-11, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 10646, *Information technology — Universal coded character set (UCS)*

ISO/IEC 18013-2:2020, *Personal identification — ISO-compliant driving licence — Part 2: Machine-readable technologies*

ISO/IEC 18013-5:2021, *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application*

ISO/IEC 19785-3, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794-4, *Information technology — Biometric data interchange formats — Part 4: Finger image data*

ISO/IEC 19794-5, *Information technology — Biometric data interchange formats — Part 5: Finger image data*

ISO/IEC 39794-4, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*

ISO/IEC 39794-5, *Information technology — Extensible biometric data interchange formats — Part 5: Face image data*

RFC 4648, *The Base16, Base32, and Base64 Data Encodings, October 2006*

RFC 7165, *Use Cases and Requirements for JSON Object Signing and Encryption (JOSE)*

RFC 7515, *JSON Web Signature*

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

ITU-T E.123, *Notation for national and international telephone numbers, e-mail addresses and web addresses*

ITU-T E.164, *The international public telecommunication numbering plan*

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
alphabetic character
A
hexadecimal ranges '41' – '5A' (Latin capital letters), '61' – '7A' (Latin small letters), 'C0' – 'D6', 'D8' – 'F6' and 'F8' – 'FF' of ISO/IEC 8859-1

3.2
boolean
logical values, TRUE and FALSE

3.3
byte string
bstr
sequence of bytes

3.4
label
identifier that is attached to a data element

3.5
numeric character
N
hexadecimal range '30' – '39' (digits 0 to 9) of ISO/IEC 8859-1

3.6
special character
S
hexadecimal ranges '20' – '2F' (<space> ! “ # $ % & ‘ ( ) * + , - . /), '3A' (:), '3C' – '40' (< = > ? @), '5B' – '60' ([\]^_`),'7B'–'7E'({|}~),'A1'–'AC'(¡¢£¤¥¦§¨©a«¬),'AE'–'A5'(®¯°±2 3´µ), and'A7'–'BF'(·¸ 1 ° » 1/4 1/2 3/4 ¿) of ISO/IEC 8859-1

3.7
text string
tstr
string of characters

3.8
unsigned integer
uint
binary value of a number of consecutive bits

4 Symbols and abbreviated terms

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

BCD	Binary Coded Decimal
CBEFF	Common Biometric Exchange Formats Framework
CBOR	Concise Binary Object Representation
CDDL	Concise Data Definition Language
eID	electronic IDentification
F	Fixed length
JSON	JavaScript Object Notation
JWS	JSON Web Signature
mDL	mobile driving license
mdoc	mobile document
URI	Uniform Resource Identifier
V	Variable length

5 General

ID documents are issued by binding an applicant with a real-life identity. An issuer collects evidence to verify the attributes provided by the applicant, and this process is called identity proofing. An applicant provides his or her attributes in specific application form. In such an application form, character formats of each data element are taken into account in order to avoid a mismatch with the ID document format. The issuer of the ID document verifies the attributes provided by the applicant with evidence and confirms the value of each attribute. ID documents issued by authoritative organisations are usually used as evidence.

Figure 1 illustrates an example of the issuing process of an eID document. An applicant provides an application form and evidence (e.g. ID cards issued by Authority) to the issuer. The issuer collects other evidence if needed and proves his or her identity and binds his or her identity with the holder and confirms the applicant by photo ID or by person of authority. As a result, his or her eID card is issued as "something you have", optionally together with "something you are (e.g. portrait)" and "something you know (e.g. password)", as defined in ISO/IEC TS 23220-5[1].

[1] Under preparation. Stage at the time of publication: ISO/IEC CD TS 23220-5

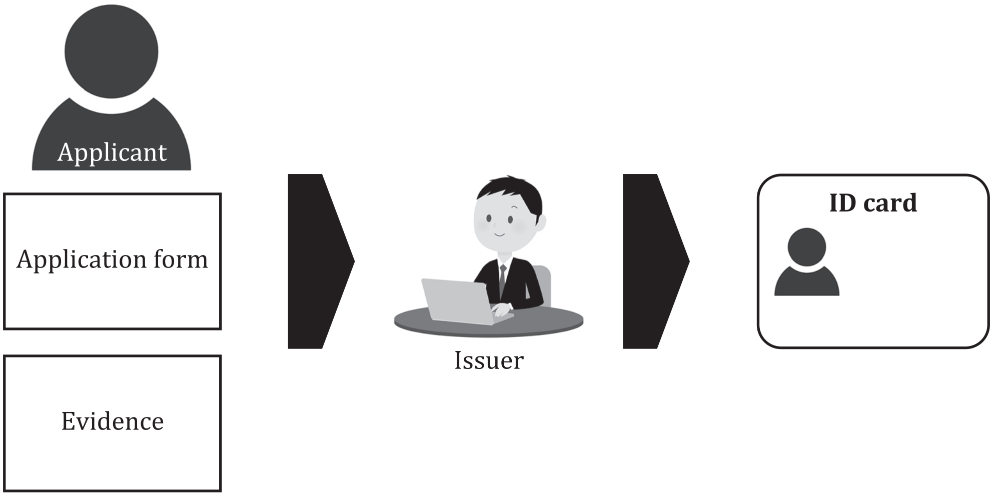

Figure 1 — Identity data collection and confirmation of its values

According to digitalisation of the issuing process, attributes used for application form and evidence are described as digital data. The specification of data elements and encoding rules for application form can be identical to that of Mobile eID. In case eID card or Mobile eID is used as evidence, a set of data elements and encoding rule is not always identical to Mobile eID. Character format, type and length are not always identical, and are out of scope of this document because they are specified by the issuer.

Figure 2 describes an example which shows a difference of attribute name between application form evidence and Mobile eID. Attributes for "Date of birth" and "Place of birth" are expressed by different attribute names in a different entity. The attribute "Date of birth" is expressed as "birth_date" in ISO/IEC 18013-5, whereas it is expressed as "birthdate" in OpenID connect standard claims.

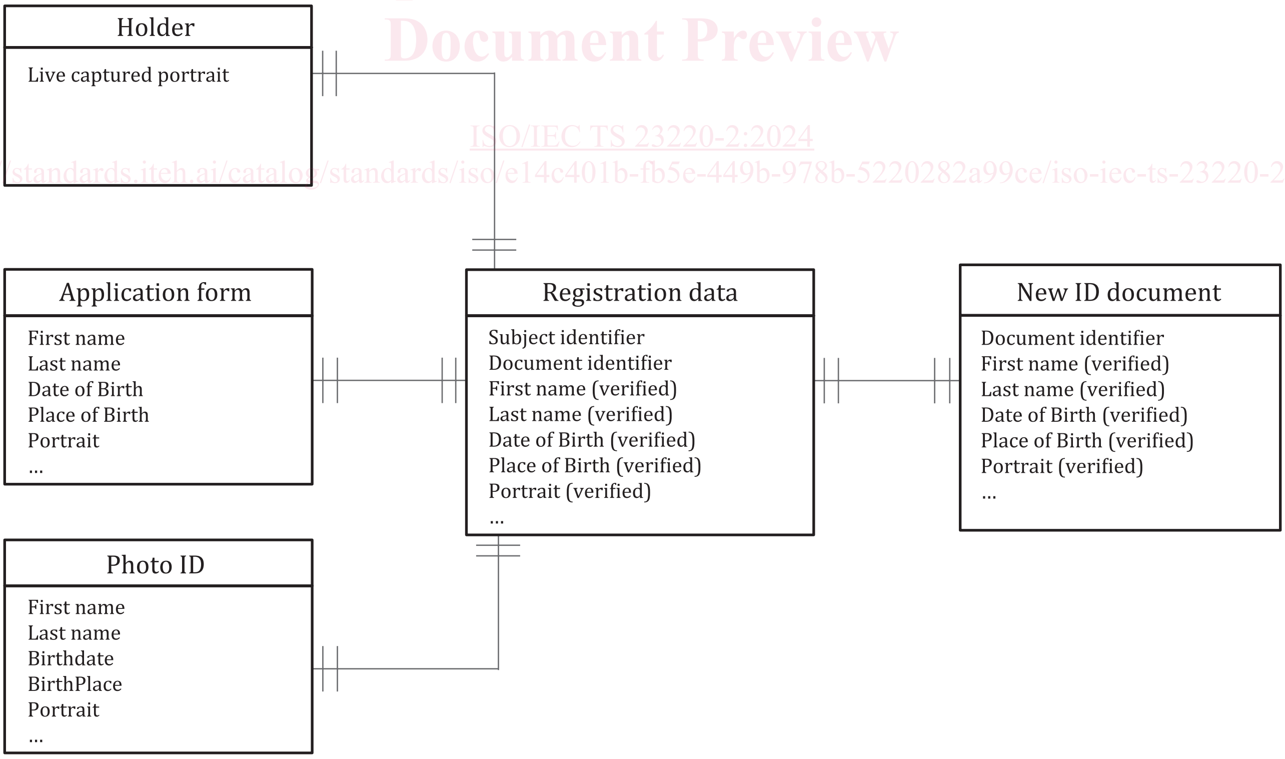

Figure 2 — Comparison of attribute names (example)

In this document, meta attributes are defined to clarify the same attributes with different identifiers to be used as a reference, supporting comparison and re-use of attribute name between two standards of eID data elements.

This document also specifies the requirement of ISO/IEC TS 23220-3[2] and ISO/IEC TS 23220-4[3] data elements as a generic extension of ISO/IEC 18013-5 specified for mDL. The data model for each ID document is specified by issuing authority and out of scope of this document.

6 Data model

6.1 General

Issuing authority should select data element identifiers from this document for interoperability if applicable. It makes it difficult for authorities to change such a specification because it sometimes requires an amendment of regulations. It results in a difference of document format, vocabulary and encoding rule.

In general, content of an eID document consists of four kinds of entities: person, document, issuer and proof. Each entity has attributes which are used to identify an instance of entity. Regardless of vocabulary, some attributes are commonly used for identifying an instance of entity. In this document, such attributes are defined as "meta-attribute".

Figure 3 shows an example of a basic data model and how an instance of an entity is identified by values for a set of attributes. In this document, such attributes are defined as personal attributes.

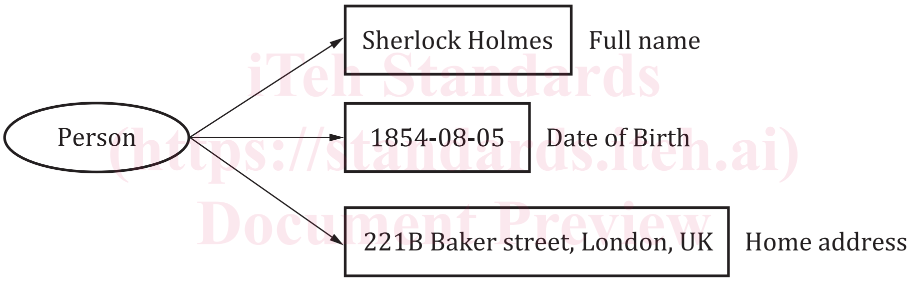

Figure 3 — Example of basic data model for identifying a person

Relationships with other persons (e.g. parental authority, proxy) can also be expressed with attributes. In this document, Figure 4 shows a relation between entity and attribute.

[2] Under preparation. Stage at the time of publication: ISO/IEC CD TS 23220-3.

[3] Under preparation. Stage at the time of publication: ISO/IEC CD TS 23220-4.