

---

---

**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*

This document is a preview generated by EUS



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>iv</b>
<b>Introduction</b>	<b>v</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Abbreviated terms</b>	<b>6</b>
<b>5 Design and privacy principles of mobile document systems</b>	<b>7</b>
5.1 Design principles	7
5.2 Privacy and security principles	8
5.2.1 General	8
5.2.2 Data minimization	8
5.2.3 Consent and choice	8
5.2.4 Accuracy and quality	8
5.2.5 Information security	9
<b>6 General life-cycle phases and components of mobile document systems</b>	<b>9</b>
6.1 Life-cycle phases of mobile document systems	9
6.2 Components of a mobile document system	10
6.2.1 Operational modes of components	10
6.2.2 Components of mobile document systems	11
<b>7 Generic system architectures of mobile document systems in installation phase</b>	<b>13</b>
<b>8 Generic system architectures of mobile document systems in issuing phase</b>	<b>15</b>
8.1 Source of user attributes	15
8.2 Generic sub-phases of issuing phase	15
8.3 System architectures in sub-phases user identification and mID-discovery	16
8.4 Architectures in sub-phase issuance	18
8.5 Monitoring service in issuing phase	20
<b>9 On-site identification system architecture in operational phase</b>	<b>21</b>
9.1 General sub-phases of on-site identification system architecture	21
9.2 On-site identification system architecture with local attribute storage	21
9.3 On-site identification system architecture with remote attribute storage	22
<b>10 Remote identification system architecture in operational phase</b>	<b>23</b>
10.1 General	23
10.2 Remote identification system architecture with local attribute storage	23
10.3 Remote identification system architecture with remote attribute storage	25
<b>Annex A (informative) Examples of deployment options for issuers in issuing phase</b>	<b>28</b>
<b>Annex B (informative) Examples of deployment options in installation phase</b>	<b>35</b>
<b>Annex C (informative) Examples of holder enrolment</b>	<b>39</b>
<b>Annex D (informative) Examples of additional physical factor(s) of authentication</b>	<b>43</b>
<b>Bibliography</b>	<b>47</b>

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://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);<sup>1)</sup>
- protocols and services for issuing phase (see ISO/IEC TS 23220-3);<sup>2)</sup>
- protocols and services for operational phase (see ISO/IEC TS 23220-4)<sup>3)</sup>;
- trust models and confidence levels (see ISO/IEC TS 23220-5)<sup>4)</sup>;
- mechanism for use of certification on trustworthiness of secure area (see ISO/IEC TS 23220-6).<sup>5)</sup>

---

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]