



Technical Specification

ISO/IEC TS 23220-6

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

Part 6: Mechanism for use of certification on trustworthiness of secure area

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

*Partie 6: Mécanisme pour l'utilisation de la certification
concernant la fiabilité de la zone protégée*

**First edition
2025-10**

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC TS 23220-6:2025

<https://standards.iteh.ai/catalog/standards/iso/70768449-697c-4fdc-a089-051c74b3bedd/iso-iec-ts-23220-6-2025>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Mechanism for use of certification on trustworthiness of secure area	3
6 List of elements describing capabilities of a secure area	6
6.1 General	6
6.2 Elements of trustworthiness characteristics for secure area	7
6.2.1 General	7
6.2.2 Secure Environment Vendor Name	7
6.2.3 Secure Environment Certification Information	7
6.2.4 Secure environment operating system and version	8
6.2.5 Secure environment operating system vendor	8
6.2.6 SA-Application Provider name	9
6.2.7 SA-Application Version	9
6.2.8 SA-Application Certification Information	9
6.2.9 Cryptographic key generation	10
6.2.10 Cryptographic key destruction	11
6.2.11 Cryptographic key derivation	11
6.2.12 Cryptographic operation	12
6.2.13 Random number generation	13
6.2.14 Information flow control functions (Simple security attributes)	14
6.2.15 Stored data integrity monitoring	15
6.2.16 Access control policy (Subset access control)	15
6.2.17 Access control functions	16
6.2.18 Timing of authentication	17
6.2.19 User authentication before any action	17
6.2.20 Re-authenticating	17
6.2.21 Security management of functions	18
6.2.22 Security roles	19
6.2.23 Management of security functionality data	19
6.2.24 Management of security attributes	20
6.2.25 Specification of management functions	21
6.2.26 Anonymity	21
6.2.27 Emanation	22
6.2.28 Resistance to physical attack	23
6.2.29 Testing	24
6.2.30 Failure with preservation of secure state	25
6.2.31 Trusted path/channels	25
7 Encoding Trustworthiness Characteristic information	26
7.1 General	26
7.2 Encoding trustworthiness certificate	27
Annex A (informative) Example of trustworthiness information of secure area	29
Annex B (informative) Certificate profile	33
Bibliography	35

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 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 international 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).

[Annex A](#) provides an example of trustworthiness information.

[Annex B](#) provides an example of a certificate profile.

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.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC TS 23220-6:2025](https://standards.iteh.ai/catalog/standards/iso/70768449-697c-4fdc-a089-051c74b3bedd/iso-iec-ts-23220-6-2025)

<https://standards.iteh.ai/catalog/standards/iso/70768449-697c-4fdc-a089-051c74b3bedd/iso-iec-ts-23220-6-2025>