Technical Specification

ISO/IEC TS 23220-3

First edition
2026-06

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

Part 3: Protocols and services for installation and issuing phase

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

Partie 3: Protocoles et services pour la phase d'installation et d'émission

Reference number
ISO/IEC TS 23220-3:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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 Symbols and abbreviations ... **2**
5 General principles ... **3**
5.1 Security principles ... 3
5.2 Design principles ... 3
5.3 Trust model ... 4
5.4 General requirements of protocols for mdoc issuing ... 4
5.5 General action flow diagram of issuing protocols ... 6
6 mdoc app descriptor and attestations ... **8**
6.1 General description of MCD ... 8
6.2 Data objects of mdoc app application descriptor ... 8
6.3 Data objects of SAAO ... 10
6.4 CDDL definition of MCD and SAAO ... 11
6.5 mdoc app attestations ... 13
6.5.1 General ... 13
6.5.2 Encodings of mdoc app attestation ... 13
7 Structures for device discovery ... **15**
7.1 Structure of Service Engagement Data ... 15
7.2 Provisioning code ... 16
7.3 Additional information structure ... 16
8 Structures for mdoc provisioning ... **18**
8.1 mdoc data structures ... 18
8.1.1 NameSpacedData structure ... 18
8.1.2 mdoc IssuerSignedDehydrated structure ... 18
8.1.3 Generation of IssuerSigned structure ... 20
8.2 Claim gathering structures ... 20
8.3 Session encryption ... 22
8.4 Issuer feedback structure ... 23
Annex A (informative) **Example of protocol for discovery services** ... **25**
Annex B (informative) **Example of issuing protocol with stateful RestAPI and E2EE** ... **31**
Annex C (informative) **Example of issuing protocol OID4VCI profile** ... **37**
Annex D (informative) **Issuing API Server-to-Server and example protocol** ... **46**
Annex E (informative) **BER-TLV encoding scheme for SAAO object** ... **59**
Annex F (informative) **Examples of deployment options** ... **61**
Annex G (informative) **Description of provisioning workflows and protocols** ... **64**
Annex H (normative) **HPKE profile of session encryption** ... **71**
Annex I (informative) **List of reason codes** ... **74**
Bibliography ... **81**

© ISO/IEC 2026 – All rights reserved

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.

© ISO/IEC 2026 – All rights reserved

Introduction

The ISO/IEC 23220 series consists of the following parts, under the general title Cards and security devices for personal identification — Building blocks for identity management via mobile devices:

— Part 1: Generic system architectures of mobile eID systems

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

— Part 3: Protocols and services for the installation and issuing phase

— Part 4: Protocols and services for the operational phase

— Part 5: Trust models and confidence level assessment

— Part 6: Mechanisms for use of certification on trustworthiness of secure area

— Part 7: Registration Authority Procedures for Mobile Documents

The objective of ISO/IEC TS 23220-3 is to:

— minimize the burden on issuers to engage in device discovery, device attestation, device binding;

— ease the process of categorizing a mdoc app implementation according to the issuer's policy;

— ease the process of provisioning mobile documents;

— rely on a third party for integral Mobile eID function characterization.

This document introduces data structures and APIs applicable for discoverability mechanisms and for mdoc provisioning purposes. Future versions of this document can specify normative protocols based on the data structures and APIs defined in this document that can be referenced by a profile identifier.

© ISO/IEC 2026 – All rights reserved

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

Part 3: Protocols and services for installation and issuing phase

1 Scope

This document provides building blocks for mobile eID-System infrastructures and normalizes protocols, interfaces and services for mdoc apps by:

— specifying interfaces for data interchange for installing of software in installation phase as well as issuing and deriving of attributes and credentials in issuing phase;

— specifying security and data protection mechanisms;

— applying privacy-enhancing mechanisms;

— specifying discoverability mechanisms.

Mechanisms for updating or revoking of attributes and credentials or mdocs are out of scope of this document and are provided by SA specific protocols.

This document 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

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/IEC TS 23220-2, *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*

ISO/IEC TS 23220-4, *Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 4: Protocols and services for operational phase*

ISO/IEC 7816-15, *Identification cards — Integrated circuit cards — Part 15: Cryptographic information application*

RFC 9360, *J. Schaad, CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates, February 2023*

IETF RFC draft 06, *OAuth 2.0 Attestation-Based Client Authentication, July 2025*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

© ISO/IEC 2026 – All rights reserved