Technical Specification

ISO/IEC TS 23220-4

First edition
2026-04

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

Part 4: Protocols and services for operational phase

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

Partie 4: Protocoles et services pour la phase opérationnelle

Reference number
ISO/IEC TS 23220-4:2026(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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **3**
4 Symbols and abbreviations **4**
5 Overview **4**
5.1 General 4
5.2 Operational sub-phases 4
5.3 Interfaces 6
5.3.1 Interface and protocols for the engagement sub-phase 6
5.3.2 Interface and protocols for the communication sub-phase 6
5.4 Additional methods and operations 6
5.5 Trust model 6
6 Data encoding and parsing of data structures and data elements **7**
6.1 General 7
6.2 CBOR encoding 7
6.3 JSON encoding 8
6.4 Parsing encoding information 8
6.5 Engagement for proximity transmission 8
6.5.1 General 8
6.5.2 Engagement structures 8
6.5.3 QR and QR reverse handover 16
6.5.4 NFC static and negotiated handover 16
6.5.5 Timeout 19
6.6 Browser to App engagement (over the Internet) 19
6.6.1 General 19
6.6.2 Engagement structures 19
6.6.3 Deep links URL with URISchemes 19
6.6.4 Deep link URLs that resolve to a specific App 20
6.6.5 Profile specific methods 20
7 Device retrieval **21**
7.1 General 21
7.1.1 Operation 21
7.1.2 End to end encryption 21
7.2 Operation messages 21
7.2.1 Device request 21
7.2.2 Device response 26
7.2.3 Device Engagement message 31
7.2.4 OID4VP Authorization request 32
7.2.5 Credential holder verification 32
7.3 E2EE transport messages 35
7.3.1 Session Establishment 35
7.3.2 Session data 35
7.3.3 JWT Secured Authorization Response Mode (JARM) 36
7.4 Device retrieval using proximity transport 36
7.4.1 NFC 36
7.4.2 BLE 37
7.4.3 Wi-Fi Aware 42
7.5 Device retrieval over the Internet 44
7.5.1 Device retrieval with E2EE for both request and response 44
7.5.2 OpenID for Verifiable Presentation 46

© ISO/IEC 2026 – All rights reserved

8 Server retrieval **46**
8.1 General 46
8.2 Data retrieval using WebAPI 47
8.2.1 Overview 47
8.2.2 Server retrieval mdoc request 48
8.2.3 server retrieval mdoc response 49
8.3 Data retrieval using OpenID connect (OIDC) 50
Annex A (normative) **Security mechanisms** **51**
Annex B (normative) **Creating a compliant profile** **70**
Annex C (informative) **Photo ID profile** **80**
Annex D (informative) **Engagement structures** **86**
Annex E (normative) **Device retrieval CDDL structures and examples** **88**
Annex F (informative) **Examples** **98**
Bibliography **104**

© 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

This document covers the operational phase introduced by ISO/IEC 23220-1. This document also expands on ISO/IEC 18013-5, especially regarding reader engagement, over the internet device retrieval operation and connections to other International Standards. It also expands operational data elements, such as for credential holder authentication, operations involving data elements from identical or different types of documents, and more.

Implementation conformant to ISO/IEC 18013-5 meets all requirements on selected building blocks specified in this document.

© ISO/IEC 2026 – All rights reserved

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

Part 4: Protocols and services for operational phase

1 Scope

This document specifies building blocks for the implementation of the operational phase of mobile eID systems and any other mdoc for national bodies or document-specific standards to create profiles according to their needs.

This document specifies the interface between the mdoc app and mdoc reader and the interface between the mdoc reader and the issuing authority infrastructure.

More specifically, this document defines transport protocols for various RF solutions and for over the internet. It defines the application layers, such as the request-response protocols between an mdoc app and mdoc reader and between an mdoc reader and issuing authority.

It further defines the security mechanism for issuer authentication, mdoc authentication and credential holder verification.

This document also specifies mechanisms enabling parties other than the issuing authority to:

— use a machine to obtain the mdoc data;

— bind the mdoc to the mdoc holder;

— authenticate the origin of the mdoc data;

— verify the integrity of the mdoc data.

The following items are out of scope for this document:

— provisioning of the mdoc data (this is covered by ISO/IEC TS 23220-3);

— how holder's consent to share data is obtained;

— requirements on storage of mdoc data and mdoc private keys.

Finally, it provides information to create a conformant profile.

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 7816-4:2020, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

© ISO/IEC 2026 – All rights reserved

ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR code bar code symbology specification*

ISO/IEC 23220-1:2023, *Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems*

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*

BSI TR-03111, *Elliptic Curve Cryptography (ECC)*

NIST SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*

RFC 4122:2005, *A Universally Unique IDentifier (UUID) URN Namespace*

RFC 4395, *Guidelines and Registration Procedures for New URI Schemes*

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

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

RFC 5280:2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5869, *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*

RFC 6066:2011, *Transport Layer Security (TLS) Extensions: Extension Definitions*

RFC 7515:2015, *JSON Web Signature (JWS)*

RFC 7518, *JSON Web Algorithms (JWA)*

RFC 7519:2015, *JSON Web Token (JWT)*

RFC 8152, *CBOR Object Signing and Encryption (COSE)*

RFC 8259, *JavaScript Object Notation (JSON)*

RFC 8422:2018, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*

RFC 8446:2018, *The Transport Layer Security (TLS) Protocol Version 1.3*

RFC 8610:2019, *Concise Data Definition Language (CDDL)*

RFC 8949:2020, *Concise Binary Object Representation (CBOR)*

RFC 9052, *CBOR Object Signing and Encryption (COSE): Structures and Process*

RFC 9053:2022, *CBOR Object Signing and Encryption (COSE): Initial Algorithms*

RFC 9112:2022, *HTTP/1.1*

RFC 9360, *CBOR Object Signing and Encryption (COSE)*

Bluetooth SIG, Bluetooth Core Specification, Version 5.2, December 2019

NFC Forum, CH 1.5, Connection handover technical specification

Wi-Fi Alliance, Neighbour awareness networking specification, Version 3.1

© ISO/IEC 2026 – All rights reserved

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 23220-1 and the following 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
credential
set of data presented as evidence of a claimed or asserted identity and/or entitlements

Note 1 to entry: 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.

Note 2 to entry: According to ISO/IEC 29115, an assertion is considered a stronger statement than a claim.

Note 3 to entry: Where identity is a set of attributes characteristic or property of an entity (see ISO/IEC 24760-1)

[SOURCE: ISO/IEC 29115:2013, 3.8, modified — Example added, Note 1 to entry replaced, Note 2 to entry added.]

3.2
device retrieval
process to retrieve user attribute(s) and credentials from the mdoc app

3.3
mdoc
mobile document (digital credential) issued by an issuing authority

3.4
PCD mode
mode in which a mobile device with NFC operates as a PCD

[SOURCE: ISO/IEC 14443-3:2018, 3.7, modified — The word “PXD” has been replaced with “mobile device with NFC”.]

3.5
PICC mode
mode in which a mobile device with NFC operates as a PICC

[SOURCE: ISO/IEC 14443-3:2018, 3.8, modified — The word “PXD” has been replaced with “mobile device with NFC”.]

3.6
server retrieval token
token identifying the mdoc holder and the mdoc app to the identity or attribute provider service

[SOURCE: ISO/IEC 18013-5:2021, 3.17, modified — App added after mdoc, "issuing authority" changed to the identity or attribute provider service.]

© ISO/IEC 2026 – All rights reserved