ISO/IEC TS 23220-3:2026-06 (E)

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

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**