ISO/IEC TS 23220-4:2026-04 (E)

Cards and security devices for personal identification - Building blocks for identity management via mobile devices - Part 4: Protocols and services for operational phase

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
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