ISO/IEC 18013-5:2021-09 (E)

Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 3

4 Abbreviated terms 5

5 Conformance requirement 6

6 mDL overview 6
6.1 Interfaces 6
6.2 Functional requirements 7
6.3 Technical requirements 8
6.3.1 Data model 8
6.3.2 Data exchange 8
6.3.3 Security mechanisms 13

7 mDL data model 15
7.1 mDL document type and namespace 15
7.2 mDL data 16
7.2.1 Overview 16
7.2.2 Portrait of mDL holder 21
7.2.3 Issuing authority 21
7.2.4 Categories of vehicles/restrictions/conditions 21
7.2.5 Age attestation: nearest "true" attestation above request 22
7.2.6 Biometric template 23
7.2.7 Signature or usual mark 23
7.2.8 Domestic data elements 23
7.3 Country codes 23

8 Transaction 23
8.1 Encoding of data structures and data elements 23
8.2 Device engagement 24
8.2.1 Device engagement information 24
8.2.2 Device engagement transmission technology 26
8.2.3 Device engagement time-out 28
8.3 Data retrieval 29
8.3.1 Data model 29
8.3.2 Data retrieval methods 29
8.3.3 Data retrieval transmission technologies 36

9 Security mechanisms 47
9.1 Device retrieval 47
9.1.1 Session encryption 47
9.1.2 Issuer data authentication 49
9.1.3 mdoc authentication 52

9.1.4 mdoc reader authentication 55
9.1.5 Session transcript and cipher suite 56
9.2 Server retrieval 58
9.2.1 TLS 58
9.2.2 JWS 58
9.3 Validation and inspection procedures 59
9.3.1 Inspection procedure for issuer data authentication 59
9.3.2 Inspection procedure for JWS 59
9.3.3 Certificate validation procedure 60

Annex A (informative) BLE L2CAP transmission profile 61

Annex B (normative) Certificate and CRL profiles 62

Annex C (informative) Verified issuer certificate authority list (VICAL) provider 90

Annex D (informative) Data structure examples 112

Annex E (informative) Privacy and security recommendations 135

Annex F (informative) IANA Considerations 149

Bibliography 153