

ISO/IEC TS 23220-2:2024-11 (E)

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

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and abbreviated terms	3
5	General	3
6	Data model	5
6.1	General	5
6.2	Data format and encoding rules	6
6.2.1	Identifier	6
6.2.2	Field format	6
6.2.3	Encoding	6
6.2.4	namespace	7
6.3	Standard meta-attributes	7
6.3.1	Meta attributes for person entity -- personal attributes	7
6.3.2	Attribute statement	11
6.3.3	Meta-attribute for issuer entity	13
6.3.4	Data elements for document entity	13
6.3.5	Data elements for document authenticity	14
6.4	Data element for level of confidence	14
7	Cipher suites	14
7.1	General	14
7.2	Elliptic curves	14
7.3	TLS	15
7.4	Digest algorithms	15
7.5	Signature algorithms	15
7.6	HMAC algorithm	16
8	Generic data models	16
8.1	General	16
8.2	mdoc data model	16
8.2.1	General	16
8.2.2	CBOR encoding	16
8.2.3	JSON conversion	17
8.3	JSON data model	19
8.3.1	General	19
8.3.2	Issuer-signed	19
8.3.3	Holder-signed	20
Annex A (informative) Examples		22
Bibliography		24