

ISO/IEC TS 23220-6:2025-10 (E)

Cards and security devices for personal identification - Building blocks for identity management via mobile devices - Part 6: Mechanism for use of certification on trustworthiness of secure area

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	3
5	Mechanism for use of certification on trustworthiness of secure area	3
6	List of elements describing capabilities of a secure area	6
6.1	General	6
6.2	Elements of trustworthiness characteristics for secure area	7
6.2.1	General	7
6.2.2	Secure Environment Vendor Name	7
6.2.3	Secure Environment Certification Information	7
6.2.4	Secure environment operating system and version	8
6.2.5	Secure environment operating system vendor	8
6.2.6	SA-Application Provider name	9
6.2.7	SA-Application Version	9
6.2.8	SA-Application Certification Information	9
6.2.9	Cryptographic key generation	10
6.2.10	Cryptographic key destruction	11
6.2.11	Cryptographic key derivation	11
6.2.12	Cryptographic operation	12
6.2.13	Random number generation	13
6.2.14	Information flow control functions (Simple security attributes)	14
6.2.15	Stored data integrity monitoring	15
6.2.16	Access control policy (Subset access control)	15
6.2.17	Access control functions	16
6.2.18	Timing of authentication	17
6.2.19	User authentication before any action	17
6.2.20	Re-authenticating	17
6.2.21	Security management of functions	18
6.2.22	Security roles	19
6.2.23	Management of security functionality data	19
6.2.24	Management of security attributes	20
6.2.25	Specification of management functions	21
6.2.26	Anonymity	21
6.2.27	Emanation	22
6.2.28	Resistance to physical attack	23
6.2.29	Testing	24
6.2.30	Failure with preservation of secure state	25
6.2.31	Trusted path/channels	25

7	Encoding Trustworthiness Characteristic information	26
7.1	General	26
7.2	Encoding trustworthiness certificate	27
	Annex A (informative) Example of trustworthiness information of secure area	29
	Annex B (informative) Certificate profile	33
	Bibliography	35