

ISO/IEC 24745:2022-02 (E)

Information security, cybersecurity and privacy protection - Biometric information protection

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	6
5	Biometric systems	7
5.1	General	7
5.2	Biometric system operations	9
5.3	Biometric references and identity references (IRs)	11
5.4	Biometric systems and identity management systems	11
5.5	Personally identifiable information (PII) and privacy	12
5.6	Societal considerations	12
6	Security aspects of a biometric system	13
6.1	Security requirements for biometric systems to protect biometric information	13
6.1.1	Confidentiality	13
6.1.2	Integrity	13
6.1.3	Renewability and revocability	13
6.1.4	Availability	14
6.2	Security threats and countermeasures in biometric systems	14
6.2.1	Threats and countermeasures against biometric system components	14
6.2.2	Threats and countermeasures during the transmission of biometric information	16
6.2.3	Renewable biometric references as countermeasure technology	17
6.3	Security of data records containing biometric information	19
6.3.1	Security for biometric information processing in a single database	19
6.3.2	Security for biometric information processing in separated databases	21
7	Biometric information privacy management	22
7.1	Biometric information privacy threats	22
7.2	Biometric information privacy requirements and guidelines	22
7.2.1	Irreversibility	22
7.2.2	Unlinkability	23
7.2.3	Confidentiality	23
7.3	Biometric information lifecycle privacy management	23
7.3.1	Collection	23
7.3.2	Transfer (disclosure of information to a third party)	24
7.3.3	Use	24
7.3.4	Storage	24
7.3.5	Retention	25
7.3.6	Archiving and data backup	25
7.3.7	Disposal	25
7.4	Responsibilities of a biometric system owner	25
8	Biometric system application models and security	26
8.1	Biometric system application models	26
8.2	Security in each biometric application model	27
8.2.1	General	27

8.2.2	Model A — Store on server and compare on server.....	28
8.2.3	Model B — Store on token and compare on server.....	29
8.2.4	Model C — Store on server and compare on client.....	31
8.2.5	Model D — Store on client and compare on client.....	32
8.2.6	Model E — Store on token and compare on client.....	34
8.2.7	Model F — Store on token and compare on token.....	36
8.2.8	Model G — Store distributed on token and server, compare on server	37
8.2.9	Model H — Store distributed on token and client, compare on client.....	38
8.2.10	Model I — Store on server, compare distributed	40
8.2.11	Model J — Store on token, compare distributed.....	41
8.2.12	Model K — Store distributed, compare distributed	43
Annex A (informative) Secure binding and use of separated DB_{IR} and DB_{BR}.....		45
Annex B (informative) Framework for renewable biometric references (RBRs).....		48
Annex C (informative) Technology examples for biometric information protection.....		52
Annex D (informative) Biometric watermarking		54
Annex E (informative) Biometric information protection using information splitting		56
Annex F (informative) Selection of biometric application models		58
Bibliography.....		61