

# ISO/IEC 27553-1:2022-11 (E)

## Information security, cybersecurity and privacy protection - Security and privacy requirements for authentication using biometrics on mobile devices - Part 1: Local modes

---

<b>Contents</b>	<b>Page</b>
Foreword .....	iv
Introduction .....	v
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	1
4 Abbreviated terms .....	5
5 Security challenges .....	5
5.1 General .....	5
5.2 Security challenges common to all biometric systems .....	5
5.3 Security challenges specific to authentication using biometrics on mobile devices .....	6
5.3.1 Diversity across mobile devices .....	6
5.3.2 Open computation environment .....	6
5.3.3 Operation in an unsupervised environment .....	6
6 System description .....	7
6.1 An example architecture .....	7
6.2 Entities and components .....	7
6.2.1 Biometric system .....	7
6.2.2 Relying party agent .....	8
6.2.3 Authentication agent .....	8
6.2.4 Relying party server .....	9
6.2.5 Authentication server .....	9
7 Information assets .....	9
8 Threat analysis .....	10
8.1 Threats to the biometric system .....	10
8.2 Threats to the authentication and relying party agents .....	10
9 Security requirements and recommendations .....	11
9.1 General .....	11
9.2 Biometric system .....	11
9.3 Mobile device .....	12
10 Privacy considerations .....	13
10.1 General .....	13
10.2 Privacy policy for biometric data .....	14
10.3 Other privacy considerations .....	14
Annex A (informative) Implementation example .....	15
Annex B (informative) Security issues related to communication between agents and servers for authentication using biometric on mobile devices .....	21
Annex C (informative) An example of authentication assurance and assurance levels .....	22
Bibliography .....	29