ISO/IEC 27553-2:2025-07 (E)

Information security, cybersecurity and privacy protection - Security and privacy requirements for authentication using biometrics on mobile devices - Part 2: Remote modes

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1
3.1 Biometrics 2
3.2 Authentication 4
3.3 System 4

4 Abbreviated terms 5

5 Security and privacy considerations 6
5.1 General 6
5.2 Security challenges common to all biometric systems 6
5.3 Reasons for and implications of choosing a remote mode instead of local mode 7
5.4 Security and privacy challenges specific to remote modes 8
5.4.1 General 8
5.4.2 Sharing biometric information with remote services 8
5.4.3 Security heterogeneity of remote services information system 8

6 System description 9
6.1 Generic architecture 9
6.2 Entities and components 9
6.2.1 Biometric system 9
6.2.2 RP agent 10
6.2.3 Authentication agent 10
6.2.4 RP server 10
6.2.5 Authentication server 10
6.3 Biometric system application models 10
6.4 Types of authentication workflow for remote mode 12

7 Information assets 12

8 Threat analysis 14
8.1 Threats related to the biometric system 14
8.2 Threats related to the authentication and RP agents 15
8.3 Threats related to the authentication and RP servers 17
8.4 Threats to communication between agents and servers 17

9 Security requirements and recommendations 18
9.1 General 18
9.2 Biometric system 18
9.3 Mobile device - side 20
9.4 Server-side 21
9.5 Communication between agents and server 22

10 Privacy requirements and recommendations 22

Annex A (informative) Implementation example 24

Annex B (informative) Authentication assurance and assurance level 32

Bibliography 39