ISO 19092:2023-03 (E)

Financial services - Biometrics - Security framework

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 2

4 Abbreviated terms 8

5 Biometricsinfinancialservicecontext 8
5.1 General 8
5.2 Generic security considerations 10
5.3 Personal device vulnerabilities and controls strategy 10
5.4 Biometric verification versus biometric identification 10

6 Biometric modalities and core systems 11
6.1 General 11
6.2 Modalities of biometrics 11
6.2.1 General 11
6.2.2 Fingerprint 11
6.2.3 Voice biometrics 12
6.2.4 Iris biometrics 12
6.2.5 Face biometrics 12
6.2.6 Signature biometrics 13
6.2.7 Vein biometrics 13
6.2.8 Palm print biometrics 14
6.2.9 Keystroke biometrics 14
6.3 Biometric system and its supporting systems 14
6.3.1 Overview 14
6.3.2 Core systems 15
6.3.3 Core biometric authentication usage scenarios 16

7 Financial biometric authentication systems -- usability considerations 20
7.1 General 20
7.2 Properties of biometric modalities 20
7.3 Properties and evaluation of biometric system 21
7.3.1 Recognition performance 21
7.3.2 Recognition performance evaluation 22
7.3.3 Presentation attack detection 23
7.3.4 Interoperability 23

8 Financial biometric authentication systems - architectures 24
8.1 Overview 24
8.2 Conceptual business architecture 24
8.3 Technical architecture 25
8.4 Registration architecture 25
8.5 PBP devices and associated biometric authentication architectures 26
8.5.1 PBP device operators 26
8.5.2 PBP device types 28

8.5.3 Point of biometric presentation (PBP) 28
8.5.4 Biometric authentication architecture 30

9 Financial biometric authentication systems - threats and vulnerabilities 34
9.1 Generic threat considerations 34
9.2 Biometric presentation vulnerabilities 35
9.2.1 Overview 35
9.2.2 Synthetic biometric presentation attack vulnerabilities 35
9.2.3 Improper PBP device calibration vulnerabilities 36
9.2.4 Fault injection 36
9.3 Comparison, decision and storage subsystem vulnerabilities 36
9.3.1 Overview 36
9.3.2 Improper threshold settings vulnerability 37
9.3.3 Score and threshold vulnerabilities 37
9.3.4 Reference refinement vulnerabilities 37
9.3.5 Self-targeted match search vulnerabilities 38
9.3.6 Other-party targeted match search vulnerabilities 38
9.3.7 Match collision vulnerabilities 38
9.3.8 Authentication result transmission vulnerabilities 38
9.3.9 Biometric storage vulnerabilities 38

10 Financial biometric authentication systems -- security requirements 38
10.1 General 38
10.2 Generic security requirements 38
10.2.1 Physical security requirements 38
10.2.2 Logical security requirements 39
10.3 Identity registration 40
10.3.1 Overview 40
10.3.2 Security requirements 40
10.4 Presentation 40
10.4.1 Overview 40
10.4.2 Security requirements 40
10.5 Data storage and handling 40
10.5.1 Overview 40
10.5.2 Reference splitting procedure 40
10.6 Comparison and decision 42
10.6.1 Overview 42
10.6.2 Security requirements 42
10.7 Enrolment 42
10.7.1 Overview 42
10.7.2 Security requirements 42
10.8 Re-enrolment 43
10.8.1 Overview 43
10.8.2 Security requirements 43
10.9 Refinement 43
10.9.1 Overview 43
10.9.2 Security requirements 43
10.10 Verification 43
10.10.1 Overview 43
10.10.2 Security requirements 44
10.11 Identification 44
10.11.1 Overview 44
10.11.2 Security requirements 44
10.12 Termination 45
10.12.1 Overview 45
10.12.2 Security requirements 45
10.13 Suspension and reactivation 45
10.13.1 Overview 45
10.13.2 Security requirements 45
10.14 Archiving 46
10.14.1 Overview 46

10.14.2 Security requirements 46
10.15 Security compliance verification 46

AnnexA(informative) Threats and vulnerabilities for biometric environments 47

AnnexB(informative) Biometric implementation scenarios 50

AnnexC(normative) Biometric security controls checklist 59

Bibliography 64