ISO/IEC TR 29156:2015-11 (E)

Information technology - Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 2

4 Abbreviated terms 3

5 Authentication factors 3
5.1 Overview 3
5.2 Security and usability of authentication mechanisms 4
5.3 Knowledge-based authentication (PIN, passwords) 5
5.3.1 General description with examples 5
5.3.2 Security considerations 6
5.3.3 Usability considerations 7
5.4 Possession based authentication (tokens, cards) 7
5.4.1 General description with examples 7
5.4.2 Security considerations 8
5.4.3 Usability considerations 9
5.5 Personal characteristic based authentication (biometrics) 9
5.5.1 General description with examples 9
5.5.2 Security considerations 11
5.5.3 Usability considerations 12
5.6 Multi-factor authentication 12
5.6.1 General 12
5.6.2 Example: token and PIN 13
5.6.3 Implementation options 13
5.6.4 Performance requirements for multi-factor authentication 14
5.7 Comparing security performance of authentication mechanisms 14
5.8 Summary comparison of authentication factors 15

6 Determining biometric authentication security requirements 15
6.1 General 15
6.2 Business requirements 15
6.3 Security-enhancing aspects 16
6.4 Suitable target figures for false acceptance rates 16
6.5 Other considerations in authentication security 16
6.6 Limits of authentication assurance 16

7 Determining biometric authentication usability requirements 17
7.1 General 17
7.2 Accessibility considerations 17
7.3 Throughput 17
7.4 Authentication failure rate for authorized users 18
7.5 Ease of use at point of authentication 19
7.6 Ease of use for enrolment 19
7.7 Other aspects of usability 19

8 Additionalconsiderationsindefiningbiometricsecurityandusabilityrequirements 19
8.1 Organization of requirements 19
8.2 Verification and identification modes of operation 20
8.3 Stages of authentication 20
8.4 Authentication assurance and standards 21
8.5 Application-specific performance considerations 21
8.5.1 Performance for business functionality 21
8.5.2 Performance for identity proofing and enrolment 22

8.5.3 Performance for identity verification 23
8.6 Additional security related requirements 23
8.7 Exception handling 24
8.8 Multi-factor authentication 24
8.8.1 General 24
8.8.2 Improved discrimination 24
8.8.3 Improvements in accessibility 25
8.8.4 Improvements in usability 25
8.8.5 Improvements in overall security 25
8.9 Dealing with security and usability shortfalls 25
8.10 Hypothetical example of quantitative performance requirements 26

9 Use cases 27
9.1 General 27
9.2 Time and attendance 27
9.3 Physical access control 27
9.4 Computer sign-on 28
9.5 Remote authentication 29

Annex A (informative) Risk assessment 31

Bibliography 40