ISO/IEC 24787:2010-12 (E)

Information technology - Identification cards - On-card biometric comparison

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Conformance 1

3 Normative references 2

4 Terms and definitions 2

5 Abbreviated terms 4

6 Architecture of biometric matching using an ICC 5
6.1 General 5
6.2 Off-card comparison 5
6.3 On-card comparison (sensor-off-card) 6
6.4 Work-sharing on-card comparison 7
6.5 System-on-card comparison 8

7 General framework for on-card comparison applications 8
7.1 Data for on-card comparison 8
7.1.1 General 8
7.1.2 Biometric reference object handling 8
7.1.3 Configuration data for biometric verification 9
7.1.4 Shared interface for multiple applications 11
7.1.5 Retry counter management 15
7.2 Standard processes for on-card comparison 15
7.2.1 Application identifier (AID) for on-card biometric comparison 15
7.2.2 Read biometric reference data 15
7.2.3 Enrolment 15
7.2.4 Verification 16
7.2.5 Termination of on-card comparison application 16
7.2.6 Comparison process and result output 16
7.2.7 Security requirements and biometric reference management 16
7.2.8 Threshold management 17

8 Work-sharing 17
8.1 Runtime work-sharing mechanism using WSR protocol 17
8.2 Work-sharing management 18
8.2.1 General 18
8.2.2 Work-sharing procedure discovery 19
8.2.3 Work-sharing procedure operation 19

Annex A (normative) Common TLV-structure of the file control parameter 20

Annex B (normative) Security policies for on-card biometric comparison 21

B.1 Introduction 21
B.2 Common security policies (CSP) for on-card biometric comparison 22
B.3 Security policies (SP1) for global comparison configuration data 22

B.4 Security policies (SP2) for local comparison configuration data 23

Annex C (informative) Sample APDU for on-card comparison 24

Annex D (informative) Software shareable interface for biometrics comparison 27

D.1 General 27
D.2 Shareable Interface Mechanism 27

Annex E (informative) Recommendation for security mechanisms in on-card comparison 29

E.1 General 29
E.2 Mutual authentication 29
E.3 Message integrity 29
E.4 Confidentiality 29
E.5 Prevention of replay attack using MAC with secret key 30

Annex F (informative) Architecture for work-sharing on-card comparison 31

F.1 General 31
F.2 Work-sharing architecture for on-card comparison 31
F.3 Types of work-sharing strategy used for on-card comparison 32
F.3.1 General 32
F.3.2 Pre-comparison computation 32
F.3.3 Work-sharing at runtime 32
F.4 Work-sharing computation protocol 32

Annex G (informative) Examples of implementations of on-card biometric comparison mechanisms 34

G.1 Introduction 34
G.2 Single Application, Homogeneous Usage 34
G.3 Single Application, Heterogeneous Usage 35
G.4 Multiple Applications 35

Annex H (informative) State diagram of a card performing a WSR session when needed 37

Bibliography 38