ISO/IEC 24787:2018 (E)

Information technology — Identification cards — On-card biometric comparison

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Conformance

6 Architecture of biometric comparison using an ICC

6.1 General
6.2 Off-card biometric comparison
6.3 On-card biometric comparison (sensor-off-card)
6.4 Work-sharing on-card biometric comparison
6.5 Biometric system-on-card

7 Framework for on-card comparison

7.1 General
7.2 Application selection (AID)
7.3 Data for on-card biometric comparison
7.3.1 General
7.3.2 Format of biometric reference
7.3.3 Data objects in the scope of biometric verification
7.3.3.1 General requirements
7.3.3.2 Data objects for biometric functionality information
7.3.3.3 Biometric comparison parameters
7.3.4 One biometric reference for multiple applications
7.4 Processes
7.4.1 Enrolment
7.4.2 Biometric verification
7.4.3 Comparison process and result output
7.4.3.1 Comparison process
7.4.3.2 Decision
7.5 Biometric comparison parameter management
7.6 Termination

8 Security policies for on-card biometric comparison

8.1 General
8.2 Common security policies for on-card biometric comparison
8.2.1 Minimum security policy
8.2.2 Security requirements and biometric reference management policy
8.2.3 Retry counter management
8.3 Security policies (SP1) for global biometric comparison parameters
8.4 Security policies (SP2) for application-specific biometric comparison parameters

9 Work-sharing on-card biometric comparison procedure

Annex A (informative) Sample APDU for on-card biometric comparison

Annex B (informative) Example of one biometric reference for multiple applications

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

- **C.1 General**
- **C.2 Single application, homogeneous usage**
- **C.3 Single application, heterogeneous usage**
- **C.4 Multiple applications**

Annex D (informative) Considerations for security mechanisms in on-card biometric comparison

- **D.1 General**
- **D.2 Mutual authentication**
- **D.3 Message integrity**
- **D.4 Confidentiality**
- **D.5 Prevention of replay attacks using the MAC with a secret key**

Page count: 27