INTERNATIONAL STANDARD

ISO/IEC 24787

First edition
2010-12-15

Information technology — Identification cards — On-card biometric comparison

Technologies de l'information — Cartes d'identification — Comparaison biométrique sur cartes

This document is a preview generated by EVS

Reference number
ISO/IEC 24787:2010(E)

© ISO/IEC 2010

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO/IEC 2010 – All rights reserved

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

This document is a preview generated by EVS

© ISO/IEC 2010 – All rights reserved

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**

This document is a preview generated by EVS

 © ISO/IEC 2010 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

ISO/IEC 24787 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

This document is a preview generated by EVS

© ISO/IEC 2010 – All rights reserved

Introduction

On-card biometric comparison, also known as *on-card matching* in ISO/IEC 7816-11:2004, is one privacy-enhanced solution employing integrated circuit cards (ICCs) and biometric technologies, and provides a more secure biometric authentication in that the biometric comparison process is executed inside the ICC. In contrast with off-card comparison (*off-card matching*), on-card comparison does not need the biometric reference data in the ICC to be transferred to interface devices. Therefore, even if the ICC is lost or stolen, the biometric reference data stored on the ICC cannot be copied and remains private.

ISO/IEC 7816-11 and ISO/IEC 19785-3 cover technologies concerning off-card comparison and simple on-card comparison. Most robust biometric comparison processes using biometric samples acquired in the "real" world require high computational intensity. In contrast, CPU performance and other resources available on the ICC progress more slowly because requirements for low power consumption, small geometry of the chip, demand of low-cost cards and so on are obstacles to their more rapid advancement. Biometric sensors embedded onto the ICCs are still presenting technical challenges.

As a result of these circumstances, industry requires a new International Standard for on-card comparison excluding off-card and system-on-card comparison. This International Standard specifies the requirements of and provides recommendations for the following:

— architectural description of on-card comparison processes;

— architectural description of work-sharing on-card comparison process that can reduce the work-load on the ICCs by pre-processing computation;

— management of threshold values and other security issues for on-card comparison.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning work-sharing given in Clause 8.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Exploit Technologies Pte Ltd.,
30 Biopolis Street,
#09-02 Matrix,
Singapore 138671

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

This document is a preview generated by EVS

 © ISO/IEC 2010 – All rights reserved

Information technology — Identification cards — On-card biometric comparison

This document is a preview generated by EVS

1 Scope

This International Standard establishes

— requirements for performing comparisons of biometric samples and returning decisions on an integrated circuit card, and

— security policies for on-card biometric comparison

It also establishes commands and rules to permit pre-comparison computations to be done off-card.

This International Standard does not establish

— requirements for off-card comparison implementations,

— requirements for system-on-card implementations, or

— modality-specific requirements for storage and comparison.

2 Conformance

An on-card comparison system claiming conformance to this International Standard shall conform to the requirements of 7.1.2 to 7.1.5, 7.2.1 to 7.2.8, 8.1, and 8.2.2 to 8.2.3, as applicable.

A card conforming to this International Standard shall

1. Be personalized with two sets of data:

   Biometric reference object handling data, as described in 7.1.2

   Configuration data for biometric verification, as described in 7.1.3

2. Support a shared interface for ICCs with multiple applications, as described in 7.1.4

3. Support retry counter management, as described in 7.1.5

4. Comply with the requirements set forth in 7.2.1 and 7.2.8 for on-card comparison implementations

5. Comply with the requirements set forth in 8.1, 8.2.2. and 8.2.3 for work-sharing implementations.

Biometric authentication might coexist with other authentication mechanisms, such as PIN. The rules for such coexistence shall comply with ISO/IEC 7816-4:2005.

The biometric data shall be organized and managed using either a file structure or data objects as per ISO/IEC 7816-4.

© ISO/IEC 2010 – All rights reserved

a) If the biometric data is organized as a file structure then the system shall also be fully compliant with the provisions in ISO/IEC 7816-11.

b) If the biometric data are organized and managed as data objects then the card shall comply with the provisions in ISO/IEC 7816-4 for data object handling.

The encoding of biometric data objects shall comply with ISO/IEC 7816-11 and ISO/IEC 19785-3.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 7816-11:2004, *Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods*

ISO/IEC 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3:2007, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

ISO/IEC 19794 (all parts), *Information technology — Biometric data interchange formats*

ISO/IEC 29794-1:2009, *Information technology — Biometric sample quality — Part 1: Framework*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1
auxiliary data
data that is dependent on biometric modality and related to the biometric reference but does not include the biometric reference or a biometric sample

EXAMPLE Data such as orientation, scaling, etc.

4.2
biometric, adj.
of or having to do with biometrics

[SC37 SD2 *Harmonised biometric vocabulary*]

NOTE "biometric" is never used as a noun.

4.3
biometrics
automated recognition of individuals based on their behavioral and biological characteristics

[SC37 SD2 *Harmonised biometric vocabulary*]

This document is a preview generated by EVS

 © ISO/IEC 2010 – All rights reserved