INTERNATIONAL STANDARD

ISO/IEC 17839-3

First edition
2016-11-01

Information technology — Identification cards — Biometric System-on-Card —

Part 3: Logical information interchange mechanism

Technologies de l'information — Cartes d'identification — Système biométrique sur carte —

Partie 3: Mécanisme d'échange de l'information logique

Reference number
ISO/IEC 17839-3:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and personal identification*.

A list of all parts in the ISO 17839 series can be found on the ISO website.

Introduction

A Biometric System-on-Card (BSoC) is a portable card size device including the following entities: biometric acquisition, image/signal processing, storage, comparison and decision. The use of a BSoC with such specifications is subject to an information flow and security mechanisms, which are detailed in this document.

ISO/IEC 17839-1 describes two types of BSoC. Type S1 is a fully flexible card compliant with ISO/IEC 7810. Type S2 deviates from some of the requirements of size and flexibility, while keeping the rest of the requirements intact, including the use of a contactless ICC interface. The logical interface and security mechanisms are independent on whether the BSoC is of type S1 or type S2, so the specifications stated in this document are applicable to both types of BSoC.

Information technology — Identification cards — Biometric System-on-Card —

Part 3: Logical information interchange mechanism

1 Scope

This document specifies

— logical data structures for a BSoC,

— enrolment procedures, and

— usage of commands and data structures defined in other ISO standards for BSoC.

This document does not define requirements for

— commands and data structures that apply to devices external to a BSoC, and

— commands and data structures that apply to logical interfaces inside a BSoC.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

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

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

ISO/IEC 14443-4, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 4: Transmission protocol*

ISO/IEC 18328-3, *Information technology — ICC-managed devices — Part 3: Organization, security and commands for interchange*

ISO/IEC 24787, *Information technology — Identification cards — On-card biometric comparison*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
biometric system-on-card
BSoC
card size device including biometric acquisition, data processing, storage, comparison and decision to compose a complete biometric verification system

3.2
feedback mechanism
mechanism of informing devices outside of a *BSoC* (3.1) of detailed error, warning or progress message complementing the status bytes by using card-originated byte strings defined in ISO/IEC 7816-4

3.3
on-card biometric comparison
performing comparison and decision making on an ICC where the biometric reference data is retained on-card in order to enhance security and privacy

4 Symbols and abbreviated terms

APDU	application protocol data unit
AT	control reference template for authentication
ATR	answer-to-reset
BER	basic encoding rules
BSoC	biometric system-on-card
CRT	control reference template
DO	BER-TLV data object
ICC	integrated circuit card
IFD	interface device
PBO	perform biometric operation
SW1-SW2	status bytes
SW1	first status byte
SW2	second status byte
TLV	tag, length, value

5 Conformance

A Biometric System-on-Card claiming conformance with this document shall conform to all mandatory requirements specified herein as applicable.

6 Logical data structures

6.1 BSoC capability

A biometric information template DO‘7F60’ may include data objects regarding BSoC capabilities specified in ISO/IEC 24787.

6.2 Biometric reference qualifier

An application in a BSoC may know which biometric reference data is used in the following ways:

— implicitly;

— commands for a biometric comparison, for example, reference data qualifier in P2 of VERIFY or PBO command;

— AT (control reference template valid for authentication) in a security environment (see ISO/IEC 7816-4);

— AT in FCI (file control information) for DF (dedicated file) (see ISO/IEC 7816-4).

6.3 Configuration data

A BSoC may use configuration data for BSoC comparison and decision (see Annex A). Each application may provide its own configuration data for a biometric reference template, as defined in ISO/IEC 24787. See ISO/IEC 7816-4 and ISO/IEC 7816-11 for generic handling of CRTs and biometric information template.

Regardless of individual configuration data, a BSoC shall implement a retry counter as defined in ISO/IEC 24787.

6.4 Enrolment procedures

6.4.1 Internal enrolment

Internal enrolment uses an on-card sensor for capturing biometric data (image or signal). Internal enrolment processes the capturing biometric data and extracts its features. Internal enrolment shall be executed by using the PBO CAPTURE AND STORE BIOMETRIC REFERENCE or PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE command.

The enrolment may use a single or multiple presentation of the biometric characteristic by the cardholder. The policy for single or multiple presentation is defined internally by the algorithm and application in the BSoC and not by command parameters.

The enrolment in a BSoC shall implement a feedback mechanism as specified in Clause 9, which includes status bytes (SW1-SW2) for the cases specified in Table 1.

Table 1 — Status bytes related to the operation of the BSoC

	SW1-SW2	Meaning
Normal processing	'90 00'	Enrolment successful
Warning processing	'62 XY' XY = '02' to '80'	State of non-volatile memory is unchanged Reason for warning provided in data object (see Clause 9)
	'63 XY'	State of non-volatile memory may have changed
Execution error	'64 XY' XY = '02' to '80'	State of non-volatile memory is unchanged Enrolment failed, reason for error provided in the data object (see Clause 9)
	'64 83'	Maximum time for acquisition has expired (timeout)
	'64 84'	Enrolment failed, non-matching sample

6.4.2 External enrolment

The application policy may decide to import reference data generated with an off-card sensor and applying different algorithm and parameters. This is called "external enrolment" in the context of BSoC.

External enrolment shall comply with the security policies defined in ISO/IEC 24787 for on-card biometric comparison.

NOTE External enrolment in a BSoC is equivalent to the enrolment in on-card biometric comparison.

6.5 Biometric comparison process

6.5.1 IFD initiated verification

The biometric comparison of a BSoC initiated by the IFD shall start with a VERIFY or PBO command specified in ISO/IEC 7816-4 and ISO/IEC 7816-11.

6.5.2 Self-initiated verification

The biometric comparison may be initiated by an on-card device with triggering capability (e.g. a mechanical switch) or by automatic detection of the presented biometric characteristic. Self-initiated verification assumes that the BSoC has power available.

Self-initiated verification performs a biometric comparison process on a stand-alone BSoC. The result of this comparison may be stored for usage in further processing in an IFD-controlled communication, i.e. by an application on the BSoC. The validity time of the comparison results needs to be configurable.

For this mechanism, a BSoC has an on-card input device, e.g. a button on a BSoC for triggering this mechanism. Although a power supply to a BSoC is needed for executing this mechanism, its specification is outside of the scope of this document. For executing a biometric comparison process, a pre-defined internal process flow is assumed. Mechanisms and definitions are outside of the scope of this document. Power control and duration management on keeping the result of biometric comparison shall be installed. These mechanisms ensure expiration of the result of biometric comparison using autonomous activation mechanism when low power or end of duration is detected. This duration shall be set at most for 1 min.

Example procedures for self-initiated activation of a BSoC are provided in Annex C.

7 Discovery of services

A BSoC may reveal its capability regarding biometric information process. A general feature management template DO'7F74' in EF.ATR/INFO and/or in the FCI of any application DF may indicate existing on-card services, e.g. on-card sensor. DO'81' under DO'7F74' indicates these on-card features

defined in ISO/IEC 7816-4. A device control parameter DO'62' may include device descriptor DO'82' defined in ISO/IEC 18328-3. A device control parameter can be retrieved by using ADDITIONAL DEVICE MANAGEMENT, GET DEVICE INFORMATION command.

A device control parameter DO'62' or a card management service template DO'7F64' may include BSoC related features and/or security.

8 Operational sequence

The BSoC functionality is activated either by issuing a PBO or VERIFY command from the IFD or by triggering a switch on the BSoC. Such switch may be a mechanical switch or an automatic detection of a biometric characteristic presented by the user. Opening, closing, disabling or otherwise manipulating sensor in a BSoC shall not be possible by the IFD. Operating the biometric capture device on a BSoC shall only be possible for the purpose of enrolment or verification initiated by a PBO or VERIFY command.

Table 2 lists the commands for executing a BSoC enrolment or verification. In addition, Annex B shows a comparison about these commands, and those used in store on card and on-card biometric comparison architectures. Both general use case and ACBio use cases are shown.

Table 2 — Commands used in BSoC for biometric-related operations

	General use case	ACBio use case
Enrolment (external)	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE
Enrolment (internal)	PBO CAPTURE AND STORE BIOMETRIC REFERENCE PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE	PBO CAPTURE AND STORE BIOMETRIC REFERENCE PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE
Verification	VERIFY PBO COMPARE BIOMETRIC PROBE PBO CAPTURE AND COMPARE BIOMETRIC PROBE	PBO COMPARE BIOMETRIC PROBE PBO CAPTURE AND COMPARE BIOMETRIC PROBE

NOTE 1 Intended use of PBO COMPARE BIOMETRIC PROBE for a BSoC architecture is PBO CAPTURE AND COMPARE BIOMETRIC PROBE similar to use of the VERIFY command (without data field) in the general use case.

NOTE 2 Verification in the context of a BSoC includes data capture, image/signal processing, on-card biometric comparison and decision.

9 Feedback mechanisms during biometric acquisition process

9.1 Feedback message data objects

The acquisition of the biometric sample during enrolment or verification requires a user interaction and the timing behaviour cannot be predicted. Therefore, the BSoC shall implement a feedback mechanism.

For the handling of the feedback mechanism, the following context specific DOs indicated in Table 3 are specified.