

---

---

**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*

IECNORM.COM : Click to view the full PDF of ISO/IEC 17839-3:2016

IECNORM.COM : Click to view the full PDF of ISO/IEC 17839-3:2016



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 .....	iv
Introduction .....	v
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>2</b>
<b>5 Conformance</b> .....	<b>2</b>
<b>6 Logical data structures</b> .....	<b>3</b>
6.1 BSoC capability .....	3
6.2 Biometric reference qualifier .....	3
6.3 Configuration data .....	3
6.4 Enrolment procedures .....	3
6.4.1 Internal enrolment .....	3
6.4.2 External enrolment .....	4
6.5 Biometric comparison process .....	4
6.5.1 IFD initiated verification .....	4
6.5.2 Self-initiated verification .....	4
<b>7 Discovery of services</b> .....	<b>4</b>
<b>8 Operational sequence</b> .....	<b>5</b>
<b>9 Feedback mechanisms during biometric acquisition process</b> .....	<b>5</b>
9.1 Feedback message data objects .....	5
9.2 Time management in a BSoC .....	6
9.3 Feedback messages .....	8
9.3.1 Successful completion of the command .....	8
9.3.2 Status feedback messages .....	9
9.3.3 Cancellation of the command by the ICC .....	9
<b>Annex A (informative) Sample APDU for Biometric System-on-Card comparison</b> .....	<b>10</b>
<b>Annex B (informative) Comparison of commands used among the different kinds of biometric-related implementations</b> .....	<b>11</b>
<b>Annex C (informative) Examples of self-initiated BSoC activation</b> .....	<b>12</b>
<b>Annex D (informative) Examples of command feedback message retrieving</b> .....	<b>13</b>
<b>Annex E (informative) State transitions for BSoC time management</b> .....	<b>14</b>
<b>Bibliography</b> .....	<b>15</b>

## 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](http://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](http://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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 17839-3:2016

[IECNORM.COM](http://IECNORM.COM) : Click to view the full PDF of ISO/IEC 17839-3:2016

# 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
<b>Normal processing</b>	'90 00'	Enrolment successful
<b>Warning processing</b>	'62 XY'	State of non-volatile memory is unchanged
	XY = '02' to '80'	Reason for warning provided in data object (see <a href="#">Clause 9</a> )
<b>Execution error</b>	'63 XY'	State of non-volatile memory may have changed
	'64 XY'	State of non-volatile memory is unchanged
	XY = '02' to '80'	Enrolment failed, reason for error provided in the data object (see <a href="#">Clause 9</a> )
	'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.

**Table 3 — Feedback message data objects under DO'7F61' (biometric information template group template)**

Tag	Length	Value and meaning
'8A'	'01'	Percentage of estimation of the progress of the acquisition process, with values between 0 and 100. If no specific information about the estimated progress is given, the value shall be 'FF'.
'8B'	'01'	Request for a new probe to be captured: '00' – in case of the ICC declaring a failure to acquire; '01' – in case of the card requiring a new probe as for a multiple sample enrolment process.
'8C'	'01'	Further qualification of execution error: '00' – insufficient quality of the acquired sample; '01' – sensor defect.

NOTE DO '8A' may be returned, for example, when the biometric capture process is slow and only partially finished.

## 9.2 Time management in a BSoC

A BSoC needs to manage timeout, both at the protocol level and also at the application level.

At the protocol level, a BSoC shall use the appropriate request for time extension (such as WTX) in order to return the SW1-SW2 status to the IFD, otherwise the IFD would assume the BSoC is dead.

The use of protocol level time extension alone does not convey any progress status to the IFD. The class of SW1 = '62' status is meant to convey progress or warning status.

When a BSoC returns a SW1 = '62', it is informing the IFD that there is progress, but it requires a time extension beyond the application timeout parameters specified by the IFD. This can happen, for example, when a BSoC has detected a finger, but data capture or signal processing has not been completed.

On the other hand, the SW1 = '64' status is used by the BSoC to inform the IFD that some problem has been detected (e.g. finger not present) and the BSoC is reporting a status for the IFD to decide whether the process should continue or be aborted.

Note that protocol level time extension is not mutually exclusive to application level time extension such as SW1 = '62'. Without appropriate protocol level time extension, the IFD will think that the BSoC is dead, and ignore or miss out the application level SW1 SW2.

If the BSoC operation cannot be completed within the maximum response time of the interface, the BSoC shall request waiting time extension using supervisory block or procedure byte as defined in ISO/IEC 7816-3 or ISO/IEC 14443-4.

In order to avoid infinite waiting during the biometric sample acquisition process, and to allow the IFD to cancel the acquisition process, the BSoC shall limit the maximum time to perform the operation (i.e. shall define the application level timeout). Therefore, before calling PBO CAPTURE AND STORE BIOMETRIC REFERENCE OR PBO CAPTURE AND COMPARE BIOMETRIC PROBE, the application level timeout may be defined by using PBO SET BIOMETRIC PARAMETER, with the DO'89' in command data field of PBO. DO'89' represents the amount of time requested to the BSoC before declaring a timeout, i.e. application level timeout. Coding of DO'89' value is specified in [Table 4](#).

**Table 4 — Application level timeout definition**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	RFU
0	x	x	x	x	x	x	x	b7 to b1 indicates the desired number of seconds
1	x	x	x	x	x	x	x	RFU

If DO'89' is not present, the application level timeout shall be implicitly known by the ICC.

If the acquisition process takes longer, the ICC shall respond with SW1-SW2 '62 xx', indicating to the IFD that the BSoC has reached its application level timeout and a mandatory feedback message object is available. In this case, the IFD may decide whether to continue or abort the acquisition process. Continuation is requested using PBO CONTINUE CAPTURE command. Cancellation is requested using PBO ABORT CAPTURE command. The IFD may read and interpret the feedback message object or ignore and issue commands for continuation or abort without reading the feedback message object (refer to [Tables 5](#) and [6](#)).

**Table 5 — Example of a successful biometric capture with application level timeout, feedback message object ignored**

IFD	ICC
PBO SET BIOMETRIC PARAMETER, with DO'89'	→
	← '90 00'; normal processing
...	
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→
	← '62 03'; execution warning: timeout, feedback message object available
PBO CONTINUE CAPTURE	→
	← '62 03'; execution warning: timeout, feedback message object available
PBO CONTINUE CAPTURE	→
	← '90 00'; normal processing

**Table 6 — Example of a biometric capture aborted by the IFD, feedback message object ignored**

IFD	ICC
PBO SET BIOMETRIC PARAMETER, with DO'89'	→
	← '90 00'; normal processing
...	
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→
	← '62 03'; execution warning: timeout, feedback message object available
PBO CONTINUE CAPTURE	→
	← '62 03'; execution warning: timeout, feedback message object available
PBO ABORT CAPTURE	→
	← '90 00'; normal processing

When the IFD receives a feedback message indicating incomplete process, the IFD may decide whether to continue or abort the acquisition process (refer to [Tables 7](#) and [8](#)).

Any other command except GET DATA and PBO CONTINUE CAPTURE should result in abort of PBO process.

**Table 7 — Example of a successful biometric capture with application level timeout, and further information returned**

IFD	ICC
PBO SET BIOMETRIC PARAMETER, with DO'89'	→
	← '90 00' ; normal processing
...	
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→
	← '62 03' ; execution warning: 03 bytes of feedback message available
GET DATA	→
	← {'8A'-'01'-'21'}-'90 00' ; 33 % completed
PBO CONTINUE CAPTURE	→
	← '62 03' ; execution warning: 03 bytes of feedback message available
GET DATA	→
	← {'8A'-'01'-'42'}-'90 00' ; 66 % completed
PBO CONTINUE CAPTURE	→
	← '90 00' ; normal processing

**Table 8 — Example of a biometric capture aborted by the IFD, and further information returned**

IFD	ICC
PBO SET BIOMETRIC PARAMETER, with DO'89'	→
	← '90 00' ; normal processing
...	
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→
	← '62 03' ; execution error: 03 bytes of feedback message available
GET DATA	→
	← {'8A'-'01'-'21'}-'90 00' ; 33 % completed
PBO CONTINUE CAPTURE	→
	← '62 03' ; execution error: 03 bytes of feedback message available
GET DATA	→
	← {'8A'-'01'-'42'}-'90 00' ; 66 % completed
PBO ABORT CAPTURE	→
	← '90 00' ; normal processing

State transitions for BSoC time management are provided in [Annex E](#).

### 9.3 Feedback messages

#### 9.3.1 Successful completion of the command

A successful completion of PBO CAPTURE AND STORE BIOMETRIC REFERENCE or a successful comparison in a PBO CAPTURE AND COMPARE BIOMETRIC PROBE shall return '90 00', as specified in ISO/IEC 7816-11. In both cases, the retry counter shall be re-established to the initial value (i.e. maximum values of consecutive attempts allowed).

In the case that the comparison has not been successful, the retry counter shall be decremented and the SW1-SW2 shall be returned as specified in ISO/IEC 7816-4 using SW1-SW2 '63 CX' with X indicating the remaining number of retries.

### 9.3.2 Status feedback messages

If the biometric acquisition process is taking longer than the application level timeout defined, the ICC may desire to provide feedback information to the external world, such as the following:

- Percentage of estimation of the progress of the acquisition process: send the SW1-SW2 '62 XY', being those XY bytes a biometric information template group template DO (i.e. '7F 61'), including a DO '8A'. That biometric DO is to be obtained by a subsequent call to GET DATA command;
- Request for time extension, without any further information on the progress percentage: send the SW1-SW2 '62 XY', returning {'8A'-'01'-'FF'} included in a DO '7F 61', when the IFD calls the GET DATA command;
- Request the user to present the biometric probe again, due to a failure to acquire: send the SW1-SW2 '62 XY', returning {'8B'-'01'-'00'} included in a DO '7F 61', when the IFD calls the GET DATA command;
- Request the user to present a new biometric probe (e.g. multiple samples acquired for enrolment): send the SW1-SW2 '62 XY', returning {'8B'-'01'-'01'} included in a DO '7F 61', when the IFD calls the GET DATA command.

After any of these messages, the process can be continued by calling PBO CONTINUE CAPTURE.

For examples of command feedback message retrieving, refer to [Annex D](#).

### 9.3.3 Cancellation of the command by the ICC

Messages indicating feedback information that also means that the process is aborted (for example, sample of not enough quality), the ICC shall return the SW1-SW2 '64 XY', being 'XY' the length of a biometric template group template DO (i.e. '7F 61'), which encapsulates the reason for the cancellation. Reasons and DOs for such cancellation are any of the following:

- insufficient quality (see [Table 3](#));
- sensor defect (see [Table 3](#)).

In order to obtain that feedback information, the IFD shall send a GET DATA command with the data, as defined in ISO/IEC 7816-4.

After any of these messages, the process cannot be continued, and a new call to PBO CAPTURE AND STORE BIOMETRIC REFERENCE or PBO CAPTURE AND COMPARE BIOMETRIC PROBE may be sent.

## Annex A (informative)

### Sample APDU for Biometric System-on-Card comparison

When ISO/IEC 7816-4 VERIFY command APDU is used to initiate the BSoC comparison, it has the following structure.

**Table A.1 — Command APDU structure, TLV-encoding**

CLA	INS	P1	P2	Lc	Data
0x00	0x21	0x00	0x00	0x03	0x5F 0x2E 0x00

NOTE 1 The Le field is absent in [Table A.1](#), because no response data is expected. Only the status word is returned to the IFD.

NOTE 2 The biometric in-use is indicated inside the biometric information template.

NOTE 3 Non-TLV encoding with INS = 0x20 and empty data field cannot be used since it would mean requesting indication of whether the authentication is required or status is already asserted according to ISO/IEC 7816-4.

## Annex B (informative)

### Comparison of commands used among the different kinds of biometric-related implementations

[Table B.1](#) shows the different commands that can be used when integrating biometrics and ICCs for the ISO/IEC 24787 defined architectures (except work-sharing).

**Table B.1 — Commands used in off-card biometric comparison, on-card biometric comparison, and BSoC systems**

		General use case	ACBio use case
<b>Off-card biometric comparison</b>	Enrolment	PUT DATA UPDATE BINARY UPDATE RECORD	PUT DATA UPDATE BINARY UPDATE RECORD PBO STORE BIOMETRIC REFERENCE
	Verification	GET DATA READ BINARY READ RECORD	GET DATA READ BINARY READ RECORD PBO RETRIEVE BIOMETRIC REFERENCE
<b>On-card biometric comparison</b>	Enrolment	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE
	Verification	VERIFY PBO COMPARE BIOMETRIC PROBE	PBO COMPARE BIOMETRIC PROBE
<b>BSoC</b>	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 Intended use of PBO COMPARE BIOMETRIC PROBE for a BSoC architecture is PBO CAPTURE AND COMPARE BIOMETRIC DATA similar to use of the VERIFY command (without data field) in the general use case.