ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59885— 2021 (ИСО/МЭК 17839-3: 2016)

Информационные технологии

БИОМЕТРИЧЕСКАЯ СИСТЕМА НА ИДЕНТИФИКАЦИОННОЙ КАРТЕ

Часть 3

Механизм обмена логической информацией

(ISO/IEC 17839-3:2016, Information technology — Identification cards — Biometric System-on-Card — Part 3: Logical information interchange mechanism, MOD)

Издание официальное

Москва
Российский институт стандартизации
2021

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией дополнительного профессионального образования «Учебный центр «ВНИИС» (АНО ДПО «Учебный центр «ВНИИС») и Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4, при консультативной поддержке Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 098 «Биометрия и биомониторинг»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 ноября 2021 г. № 1596-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 17839-3:2016 «Информационные технологии. Идентификационные карты. Биометрическая система на идентификационной карте. Часть 3. Механизм обмена логической информацией» (ISO/IEC 17839-3:2016 «Information technology — Identification cards — Biometric System-on-Card — Part 3: Logical information interchange mechanism», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом, а также путем изменения его структуры для приведения в соответствие с правилами, установленными в ГОСТ 1.5—2001 (подразделы 4.2 и 4.3). Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных и межгосударственного стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА.

Сопоставление структуры настоящего стандарта со структурой указанного международного стандарта приведено в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Федеральное агентство по техническому регулированию и метрологии не несет ответственности за установление подлинности каких-либо или всех таких патентных прав

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии (*gost.e-ecolog.ru

© ISO, 2016
© IEC, 2016
© Оформление. ФГБУ «РСТ», 2021

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 2
5 Соответствие 2
6 Структуры логических данных 3
6.1 Возможности BSoC 3
6.2 Квалификатор биометрических контрольных шаблонов 3
6.3 Данные конфигурации 3
6.4 Процедуры биометрической регистрации 3
6.5 Процесс биометрического сравнения 4
7 Обнаружение услуг 4
8 Последовательность действий 4
9 Механизмы обратной связи в процессе получения биометрических данных 5
9.1 Информационные объекты сообщений обратной связи 5
9.2 Управление временем в BSoC 5
9.3 Сообщения обратной связи 9
Приложение А (справочное) Пример APDU для сравнения в биометрической системе на идентификационной карте 10
Приложение *B* (справочное) Примеры активации BSoC по собственной инициативе 11
Приложение *C* (справочное) Сравнение команд, используемых среди разных видов реализаций, связанных с биометрией 12
Приложение *D* (справочное) Переходы состояний для управления временем BSoC 13
Приложение *E* (справочное) Примеры получения командных сообщений обратной связи 14
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственного стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 15
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта 16
Библиография 17

Введение

Биометрическая система на идентификационной карте (BSoC) — это портативное устройство размером с идентификационную карту, обеспечивающее получение биометрических данных, их обработку, хранение, сравнение и принятие решения. Использование BSoC с такими спецификациями зависит от информационного потока и механизмов безопасности, которые подробно описаны в настоящем стандарте.

В *ГОСТ Р ИСО/МЭК 17839-1* определены 2 типа BSoC. Тип S1 представляет собой полностью гибкую карту, соответствующую *ГОСТ Р ИСО/МЭК 7810*. Тип S2 отклоняется от некоторых требований к размеру и гибкости, сохраняя остальные требования неизменными, включая использование бесконтактного интерфейса ICC. Логический интерфейс и механизмы безопасности не зависят от того, относится ли BSoC к типу S1 или типу S2, поэтому спецификации, изложенные в настоящем стандарте, применимы к обоим типам BSoC.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЧЕСКАЯ СИСТЕМА НА ИДЕНТИФИКАЦИОННОЙ КАРТЕ

Часть 3

Механизм обмена логической информацией

Information technology. Biometric System-on-Card. Part 3. Logical information interchange mechanism

Дата введения — 2022—01—01

1 Область применения

Настоящий стандарт устанавливает:

- структуру логических данных для BSoC;
- процедуры биометрической регистрации;
- использование команд и структур данных, определенных в других стандартах для BSoC.

Настоящий стандарт не устанавливает требования для команд и структур данных, которые применяются:

- к устройствам, внешним по отношению к BSoC;
- логическим интерфейсам внутри BSoC.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ Р 58230 (ИСО/МЭК 24787:2010) Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте

ГОСТ Р 58671 (ИСО/МЭК 7816-11:2017) Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами

ГОСТ Р ИСО/МЭК 7816-3 Карты идентификационные. Карты на интегральных схемах. Часть 3. Карты с контактами. Электрический интерфейс и протоколы передачи

ГОСТ Р ИСО/МЭК 7816-4 Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена

ГОСТ Р ИСО/МЭК 14443-4 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 4. Протокол передачи

ГОСТ Р ИСО/МЭК 17839-1 Информационные технологии. Биометрическая система на идентификационной карте. Часть 1. Основные требования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого

Издание официальное

стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37, ГОСТ Р ИСО/МЭК 17839-1* и *ГОСТ Р 58230*, а также следующий термин с соответствующим определением:

3.1 **механизм обратной связи** (feedback mechanism): Механизм информирования устройств за пределами BSoC путем предоставления детализированного сообщения об ошибке, предупреждающего сообщения или сообщения о выполнении, дополняющего байты состояния посредством строк байтов, инициированных идентификационной картой.

Примечание — Строки байтов определены в *ГОСТ Р ИСО/МЭК 7816-4*.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

АСБио — аутентификационный статус для биометрии (authentication context for biometrics);

APDU — блок данных прикладного протокола (application protocol data unit);

AT — шаблон управляющих ссылок аутентификации (control reference template for authentication);

ATR — ответ на восстановление (answer-to-reset);

BER — базовые правила кодирования (basic encoding rules);

BSoC — биометрическая система на идентификационной карте (biometric system-on-card);

CRT — шаблон управляющих ссылок (control reference template);

DF — *назначенный файл (dedicated file);*

DO — информационный объект BER-TLV (BER-TLV data object);

ICC — карта на интегральной схеме (integrated circuit card);

IFD — устройство сопряжения (interface device);

FCI — *контрольная информация файла (file control information);*

PBO — выполнение биометрической операции (perform biometric operation);

SW1-SW2 — байты состояния (status bytes);

SW1 — первый байт состояния;

SW2 — второй байт состояния;

TLV — тэг, длина, значение.

5 Соответствие

Биометрическая система на идентификационной карте, претендующая на соответствие настоящему стандарту, должна соответствовать всем обязательным требованиям, указанным в настоящем стандарте.

6 Структуры логических данных

6.1 Возможности BSoC

Шаблон биометрической информации DO'7F60' может включать в себя информационные объекты, касающиеся возможностей BSoC, определенных в *ГОСТ Р 58230*.

6.2 Квалификатор биометрических контрольных шаблонов

Приложение в BSoC может знать, какие данные биометрических контрольных шаблонов используют следующими способами:

- в неявном виде;
- с помощью команд для биометрического сравнения, например, используя квалификатор данных биометрических контрольных шаблонов в параметре P2 команды VERIFY или PBO;
- с помощью AT безопасной среды (см. *ГОСТ Р ИСО/МЭК 7816-4*);
- с помощью AT в FCI для DF (см. *ГОСТ Р ИСО/МЭК 7816-4*).

6.3 Данные конфигурации

BSoC может использовать данные конфигурации для сравнения и принятия решения в BSoC (см. приложение А). Каждое приложение может предоставлять собственные данные конфигурации для биометрического контрольного шаблона, как определено в *ГОСТ Р 58230*. В *ГОСТ Р ИСО/МЭК 7816-4* и *ГОСТ Р 58671* приведена общая информация о CRT и биометрическом контрольном шаблоне.

Независимо от индивидуальных данных конфигурации BSoC должна реализовать счетчик повторов, как определено в *ГОСТ Р 58230*.

6.4 Процедуры биометрической регистрации

6.4.1 Внутренняя биометрическая регистрация

При внутренней биометрической регистрации для сбора биометрических данных (изображения или сигнала) используется датчик на идентификационной карте. При внутренней биометрической регистрации осуществляется сбор биометрических данных и извлечение биометрических признаков. Внутренняя биометрическая регистрация должна быть выполнена с помощью операции CAPTURE AND STORE BIOMETRIC REFERENCE или CAPTURE AND UPDATE BIOMETRIC REFERENCE команды PBO.

Биометрическая регистрация может осуществляться с использованием однократного или многократного предъявления биометрической характеристики владельцем идентификационной карты. Политика однократного или многократного предъявления определяется внутренним алгоритмом и приложением в BSoC, а не параметрами команды.

При биометрической регистрации в BSoC должен быть внедрен механизм обратной связи, как указано в разделе 9, который включает в себя байты состояния (SW1-SW2) для случаев, указанных в таблице 1.

Таблица 1 — Байты состояния, связанные с функционированием BSoC

Состояние обработки	SW1-SW2	Смысловое содержание
Нормальная обработка	‘90 00’	Биометрическая регистрация завершилась успешно
Обработка с предупреждением	‘62 *XY*’ *XY* = от ‘02’ до ‘80’	Состояние энергонезависимой памяти без изменений. Причина предупреждения представлена в информационном объекте (см. раздел 9)
	‘63 *XY*’	Состояние энергонезависимой памяти изменено
Ошибка выполнения	‘64 *XY*’ *XY* = от ‘02’ до ‘80’	Состояние энергонезависимой памяти без изменений. Биометрическая регистрация завершилась неуспешно, причина ошибки представлена в информационном объекте (см. раздел 9)
	‘64 83’	Максимальное время получения истекло (тайм-аут)
	‘64 84’	Биометрическая регистрация завершилась неуспешно, неподходящий биометрический образец

6.4.2 Внешняя биометрическая регистрация

Политика приложения может позволять импортировать данные биометрических контрольных шаблонов, полученные с помощью датчика вне идентификационной карты и применяющие различные алгоритмы и параметры. В контексте BSoC этот процесс называется внешней биометрической регистрацией.

Внешняя биометрическая регистрация должна соответствовать политике безопасности для биометрического сравнения на идентификационной карте, определенной в *ГОСТ Р 58230*.

Примечание — Внешняя биометрическая регистрация в BSoC эквивалентна биометрической регистрации при биометрическом сравнении на идентификационной карте.

6.5 Процесс биометрического сравнения

6.5.1 Биометрическая верификация, инициированная IFD

Биометрическое сравнение в BSoC, инициированное IFD, должно начинаться с команды VERIFY или PBO, указанной в *ГОСТ Р ИСО/МЭК 7816-4* и *ГОСТ Р 58671*.

6.5.2 Биометрическая верификация по собственной инициативе

Биометрическое сравнение может быть инициировано устройством на идентификационной карте с возможностью запуска (например, механическим переключателем) или путем автоматического определения предъявленной биометрической характеристики. Биометрическая верификация по собственной инициативе предполагает, что BSoC располагает доступной мощностью.

При биометрической верификации по собственной инициативе процесс биометрического сравнения выполняется в автономной BSoC. Результат биометрического сравнения может быть сохранен для использования в дальнейшем при контролируемом IFD взаимодействии, т. е. приложением в BSoC. Время действия результатов биометрического сравнения должно быть настраиваемым.

Для запуска процесса биометрического сравнения BSoC имеет устройство ввода на идентификационной карте, например кнопку запуска. Хотя для выполнения этого механизма требуется источник питания для BSoC, его спецификация выходит за рамки настоящего стандарта. Для выполнения процесса биометрического сравнения предполагается заранее определенная внутренняя технологическая цепочка. Механизмы и определения этого процесса выходят за рамки настоящего стандарта. Должны быть установлены контроль мощности и управление продолжительностью сохранения результата биометрического сравнения. Эти механизмы обеспечивают истечение срока действия результата биометрического сравнения с использованием механизма автономной активации при обнаружении низкой мощности или окончания продолжительности сохранения результата. Эта продолжительность должна составлять не более чем 1 мин.

Примеры активации BSoC по собственной инициативе приведены в приложении *B*.

7 Обнаружение услуг

BSoC может раскрыть свои возможности в отношении биометрической информации. Общий шаблон управления функциями DO'7F74' в EF.ATR/INFO и/или в *FCI* любого приложения *DF* может указывать на существующие услуги на идентификационной карте, например: датчик на идентификационной карте. DO'81', относящийся к DO'7F74', указывает на функции идентификационной карты, определенные в *ГОСТ Р ИСО/МЭК 7816-4*. Контрольный параметр устройства DO'62' может включать дескриптор устройства DO'82', определенный в *[1]*. Контрольный параметр устройства может быть получен с помощью команд ADDITIONAL DEVICE MANAGEMENT и GET DEVICE INFORMATION.

Контрольный параметр устройства DO'62' или шаблон услуг управления идентификационной карты DO'7F64' могут включать связанные с BSoC функции и/или безопасность.

8 Последовательность действий

Функциональность BSoC активируется либо путем получения команды PBO или VERIFY от IFD, либо путем запуска переключателя на BSoC. Это может быть механический переключатель или автоматическое определение биометрической характеристики, предъявленной пользователем. Открытие, закрытие, отключение или иное манипулирование датчиком на BSoC с помощью IFD не должно быть возможным. Эксплуатация устройства сбора биометрических данных в BSoC должна быть возможна только с целью биометрической регистрации или биометрической верификации, инициированной командой PBO или VERIFY.

В таблице 2 перечислены команды для выполнения биометрической регистрации или биометрической верификации в BSoC. Кроме того, в приложении С показано сравнение этих команд, а также тех команд, которые используются в архитектурах хранения и биометрического сравнения на идентификационной карте. Показаны как общие варианты использования, так и варианты использования АСБио.

Таблица 2 — Команды, используемые в BSoC для биометрических операций

Биометрическая операция	Общий вариант использования	Вариант использования АСБио
Биометрическая регистрация (внешняя)	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE
Биометрическая регистрация (внутренняя)	PBO CAPTURE AND STORE BIOMETRIC REFERENCE PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE	PBO CAPTURE AND STORE BIOMETRIC REFERENCE PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE
Биометрическая верификация	VERIFY PBO COMPARE BIOMETRIC PROBE PBO CAPTURE AND COMPARE BIOMETRIC PROBE	PBO COMPARE BIOMETRIC PROBE PBO CAPTURE AND COMPARE BIOMETRIC PROBE

Примечания

1 Предполагаемое использование операции COMPARE BIOMETRIC PROBE команды PBO для архитектуры BSoC — это использование операции CAPTURE AND COMPARE BIOMETRIC PROBE команды PBO, аналогичное использованию команды VERIFY (без поля данных) в общем варианте использования.

2 Биометрическая верификация в контексте BSoC включает сбор биометрических данных, обработку изображений/сигналов, биометрическое сравнение на идентификационной карте и принятие решения.

9 Механизмы обратной связи в процессе получения биометрических данных

9.1 Информационные объекты сообщений обратной связи

Получение биометрического образца во время биометрической регистрации или биометрической верификации требует взаимодействия с пользователем, поэтому продолжительность этих операций не может быть предсказана, поэтому в BSoC должен быть предусмотрен механизм обратной связи.

Для взаимодействия с механизмом обратной связи определены следующие информационные объекты (DO), зависящие от контекста и указанные в таблице 3.

Таблица 3 — Информационные объекты сообщений обратной связи, относящиеся к DO'7F61' (шаблон группы шаблонов биометрической информации)

Тэг	Длина	Значение и смысловое содержание
‘8A’	‘01’	Процент оценки выполнения процесса получения биометрических данных со значениями от 0 до 100. При отсутствии конкретной информации о выполнении значение должно быть ‘FF’
‘8B’	‘01’	Запрос на сбор новой биометрической пробы: ‘00’ — если ICC сообщает о неудачной попытке получения биометрических данных; ‘01’ — если идентификационная карта требует новую биометрическую пробу, например в процессе биометрической регистрации нескольких биометрических образцов
‘8C’	‘01’	Дополнительные квалификационные ошибки выполнения: '00' — недостаточное качество полученного биометрического образца; '01' — дефект датчика

Примечание — DO'8A' может быть возвращен, например, когда процесс сбора биометрических данных осуществляется медленно и только частично завершен.

9.2 Управление временем в BSoC

BSoC должна управлять тайм-аутом как на уровне протокола, так и на уровне приложения.

На уровне протокола BSoC должна использовать соответствующий запрос на продление времени (например, WTX), чтобы вернуть IFD состояние SW1-SW2, в противном случае IFD будет считать, что BSoC не работает.

Использование только продления времени на уровне протокола не передает IFD никакого состояния выполнения. Класс состояния SW1 = '62' предназначен для передачи состояния выполнения или предупреждения.

Когда BSoC возвращает SW1 = '62', она информирует IFD о том, что выполнение идет, но требуется продление времени сверх параметров тайм-аута приложения, указанных IFD. Это может произойти, например, когда BSoC обнаружила палец, но сбор биометрических данных или обработка сигналов не были завершены.

С другой стороны, состояние SW1 = ‘64’ используется BSoC для информирования IFD о том, что была обнаружена какая-то проблема (например, палец отсутствует), и BSoC сообщает состояние IFD, чтобы решить, следует ли продолжать процесс или прервать его.

Следует обратить внимание, что продление времени на уровне протокола и на уровне приложения, такое как SW1 = ’62’, не являются взаимоисключающими. Без соответствующего продления времени на уровне протокола IFD будет думать, что BSoC не работает, и игнорировать или пропускать SW1-SW2 на уровне приложения.

Если функционирование BSoC не может быть завершено в течение максимального времени отклика интерфейса, BSoC запрашивает продление времени ожидания с использованием контролирующего блока или процедурного байта, как определено в *ГОСТ Р ИСО/МЭК 7816-3* или *ГОСТ Р ИСО/МЭК 14443-4*.

Для того чтобы избежать бесконечного ожидания во время процесса получения биометрических образцов и позволить IFD отменить процесс получения, BSoC должна ограничить максимальное время для выполнения операции (т. е. определить тайм-аут на уровне приложения). Поэтому прежде вызова операции CAPTURE AND STORE BIOMETRIC REFERENCE или CAPTURE AND COMPARE BIOMETRIC PROBE команды PBO тайм-аут на уровне приложения может быть определен с помощью операции SET BIOMETRIC PARAMETER команды PBO с DO‘89’ в поле данных. DO'89' представляет собой количество времени, запрошенное BSoC перед объявлением тайм-аута, т. е. тайм-аут на уровне приложения. Кодировка значения DO'89' указана в таблице 4.

Таблица 4 — Определение тайм-аута на уровне приложения

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое содержание
0	0	0	0	0	0	0	0	Зарезервировано для будущего использования
0	x	x	x	x	x	x	x	Значения от b7 до b1 указывают предпочтительное количество секунд
1	x	x	x	x	x	x	x	Зарезервировано для будущего использования

Если DO'89' отсутствует, то тайм-аут на уровне приложения должен быть неявно известен ICC.

Если процесс получения биометрических данных занимает больше времени, ICC должна ответить в формате SW1-SW2 62 XX’, указывая IFD, что BSoC достигла своего тайм-аута на уровне приложения и обязательный объект сообщения обратной связи доступен. В этом случае IFD может принять решение о продолжении или прекращении процесса получения биометрических данных. Продолжение запрашивается с помощью операции CONTINUE CAPTURE команды PBO. Отмена запрашивается с помощью операции ABORT CAPTURE команды PBO. IFD может читать и интерпретировать объект сообщения обратной связи или игнорировать и выдавать команды для продолжения или прерывания без чтения объекта сообщения обратной связи (см. таблицы 5 и 6).

Таблица 5 — Пример успешного сбора биометрических данных с тайм-аутом на уровне приложения при игнорировании объекта сообщения обратной связи

IFD		ICC
PBO SET BIOMETRIC PARAMETER с DO ‘89’	→	
	←	‘90 00’; нормальная обработка
...		
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→	
	←	‘62 03’; предупреждение о выполнении: тайм-аут, доступен объект сообщения обратной связи
PBO CONTINUE CAPTURE	→	
	←	‘62 03’; предупреждение о выполнении: тайм-аут, доступен объект сообщения обратной связи
PBO CONTINUE CAPTURE	→	
	←	‘90 00’; нормальная обработка

Таблица 6 — Пример сбора биометрических данных, прерванного IFD, при игнорировании объекта сообщения обратной связи

IFD		ICC
PBO SET BIOMETRIC PARAMETER с DO ‘89’	→	
	←	‘90 00’; нормальная обработка
...		
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→	
	←	’62 03’; предупреждение о выполнении: тайм-аут, доступен объект сообщения обратной связи
PBO CONTINUE CAPTURE	→	
	←	‘62 03’; предупреждение о выполнении: тайм-аут, доступен объект сообщения обратной связи
PBO ABORTE CAPTURE	→	
	←	‘90 00’; нормальная обработка

Когда IFD получает сообщение обратной связи, указывающее на незавершенность процесса, оно может принять решение о продолжении или прекращении процесса получения биометрических данных (см. таблицы 7 и 8).

Любая другая команда, кроме команд GET DATA и операции CONTINUE CAPTURE команды PBO, должна привести к прерыванию процесса PBO.

Таблица 7 — Пример успешного сбора биометрических данных с тайм-аутом на уровне приложения и возвращением дополнительной информации

IFD		ICC
PBO SET BIOMETRIC PARAMETER с DO '89'	→	
	←	'90 00'; нормальная обработка
...		
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→	
	←	'62 03'; предупреждение о выполнении: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8A'-'01'-'21'}-'90 00' ; 33 % завершено
PBO CONTINUE CAPTURE	→	
	←	'62 03'; предупреждение о выполнении: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8A'-'01'-'42'} - '90 00' ; 66 % завершено
PBO CONTINUE CAPTURE	→	
	←	'90 00'; нормальная обработка

Таблица 8 — Пример сбора биометрических данных, прерванного IFD, с возвращением дополнительной информации

IFD		ICC
PBO SET BIOMETRIC PARAMETER с DO '89'	→	
	←	'90 00'; нормальная обработка
...		
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→	
	←	'62 03'; предупреждение о выполнении: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8A'-'01'-'21'}-'90 00' ; 33 % завершено
PBO CONTINUE CAPTURE	→	
	←	'62 03'; предупреждение о выполнении: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8A'-'01'-'42'}-'90 00' ; 66 % завершено
PBO ABORT CAPTURE	→	
	←	'90 00'; нормальная обработка

Переходы состояний для управления временем BSoC приведены в приложении D.

9.3 Сообщения обратной связи

9.3.1 Успешное выполнение команды

При успешном выполнении операции CAPTURE AND STORE BIOMETRIC REFERENCE или CAPTURE AND COMPARE BIOMETRIC PROBE команды PBO должно возвращаться значение '90 00', как указано в *ГОСТ Р 58671*. В обоих случаях счетчик повторов должен быть восстановлен до исходного значения (т. е. максимально допустимых значений последовательных попыток).

Если сравнение было неуспешным, счетчик повторов должен быть уменьшен и должны быть возвращены SW1-SW2, как указано в *ГОСТ Р ИСО/МЭК 7816-4*, используя значение SW1-SW2 '63 *CX*', где *X* указывает на оставшееся количество повторов.

9.3.2 Сообщения обратной связи о состоянии

Если процесс получения биометрических данных занимает больше времени, чем определенный тайм-аут на уровне приложения, ICC может предоставить информацию обратной связи внешнему миру, например:

- процент оценки выполнения процесса получения биометрических данных: отправить значение SW1-SW2 '62 *XY*', где *XY* — байты DO (т. е. '7F 61') шаблона группы шаблонов биометрической информации, в том числе DO'8A'. Этот биометрический DO должен быть получен при последующем вызове команды GET DATA;
- запрос на продление времени, без какой-либо дополнительной информации о выполнении в процентах: отправить значение SW1-SW2 '62 *XY*' с возвращением {'8A'-'01'-'FF'}, включенным в DO '7F 61', когда IFD вызывает команду GET DATA;
- запрос пользователя о повторном предъявлении биометрической пробы из-за неудачной попытки получения биометрических данных: отправить значение SW1-SW2 '62 *XY*' с возвращением {'8B'-'01'-'00'}, включенным в DO '7F 61', когда IFD вызывает команду GET DATA;
- запрос пользователя о предъявлении новой биометрической пробы (например, для получения нескольких биометрических образцов при биометрической регистрации): отправить значение SW1-SW2 '62 *XY*' с возвращением {'8B'-'01'-'01'}, включенным в DO' 7F 61', когда IFD вызывает команду GET DATA.

После любого из этих сообщений процесс можно продолжить, вызвав операцию CONTINUE CAPTURE команды PBO.

Примеры получения командных сообщений обратной связи приведены в приложении *E*.

9.3.3 Отмена команды ICC

Посылая сообщение с указанием информации обратной связи, которое также означает, что процесс прерван (например, из-за недостаточного качества биометрического образца), ICC должна возвратить значение SW1-SW2 '64 *XY*', где *XY* — длина DO шаблона группы шаблонов биометрических шаблонов (т. е. '7F 61'), которое инкапсулирует причину отмены. Причинами и DO для такой отмены являются следующие:

- недостаточное качество (см. таблицу 3);
- дефект датчика (см. таблицу 3).

Для того чтобы получить эту информацию обратной связи, IFD должно отправить команду GET DATA с данными, как определено в *ГОСТ Р ИСО/МЭК 7816-4.*

После любого из этих сообщений процесс не может быть продолжен, и должен быть отправлен новый запрос с помощью команды операции CAPTURE AND STORE BIOMETRIC REFERENCE или CAPTURE AND COMPARE BIOMETRIC PROBE команды PBO.

Приложение А
(справочное)

Пример APDU для сравнения в биометрической системе на идентификационной карте

Когда для инициирования сравнения в BSoC используется APDU команды VERIFY в соответствии с *ГОСТ Р ИСО/МЭК 7816-4*, то он имеет следующую структуру.

Таблица А.1 — Структура APDU команды, закодированной в TLV

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

Примечания

1 Поле Le отсутствует в таблице А.1, поскольку данные ответа не ожидаются. В IFD возвращается только слово состояния.

2 Используемая биометрическая информация указывается внутри шаблона биометрической информации.

3 Кодирование без TLV с INS = 0x20 и пустым полем данных не может быть использовано, так как это означало бы запрос того, требуется ли аутентификация или состояние уже заявлено в соответствии с *ГОСТ Р ИСО/МЭК 7816-4.*

Приложение *В*
(справочное)

Примеры активации BSoC по собственной инициативе

Пример выполнения процедуры на BSoC с помощью механизма активации по собственной инициативе заключается в следующем:

- нажать кнопку на BSoC;
- активация BSoC выполняется без каких-либо выходных данных;
- заранее определить внутреннюю технологическую цепочку, например выбрать приложение, после чего биометрическое сравнение выполняется без вывода каких-либо данных из этой BSoC во внешний мир;
- результат сценария, например установленное условие безопасности, связанное с биометрическим сравнением, VA (область действия), состояние ошибки, может быть сохранен для последующей обработки.

Ниже приведены некоторые примеры последующей обработки:

- выполняется активация по собственной инициативе этой BSoC, и результаты биометрического сравнения сохраняются в BSoC;
- выполняется приложение на этой BSoC, включая биометрическое сравнение, так же, как и в заранее определенной внутренней технологической цепочке;
- если отклик процесса биометрического сравнения показывает:
  - успешную биометрическую верификацию, то BSoC сообщает о нормальной обработке (SW1-SW2 = = '90 00'),
  - результаты, отличные от успешной биометрическую верификации, то BSoC снова выполняет биометрическое сравнение, а затем выдает результат.

Приложение *С*
(справочное)

Сравнение команд, используемых среди разных видов реализаций, связанных с биометрией

В таблице С.1 показаны различные команды, которые могут быть использованы при интеграции биометрии и ICC для определенных в *ГОСТ Р 58230* архитектур (за исключением распределения нагрузки).

Таблица С.1 — Команды, используемые при биометрическом сравнении вне идентификационной карты, биометрическом сравнении на идентификационной карте и в BSoC

Архитектура	*Биометрическая операция*	Общий вариант использования	Вариант использования АСБио
Биометрическое сравнение вне идентификационной карты	Биометрическая регистрация	PUT DATA UPDATE BINARY UPDATE RECORD	PUT DATA UPDATE BINARY UPDATE RECORD PBO STORE BIOMETRIC REFERENCE
	Биометрическая верификация	GET DATA READ BINARY READ RECORD	GET DATA READ BINARY READ RECORD PBO RETRIEVE BIOMETRIC REFERENCE
Биометрическое сравнение на идентификационной карте	Биометрическая регистрация	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE
	Биометрическая верификация	VERIFY PBO COMPARE BIOMETRIC PROBE	PBO COMPARE BIOMETRIC PROBE
BSoC	Биометрическая регистрация (внешняя)	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE	PBO STORE BIOMETRIC REFERENCE PBO UPDATE BIOMETRIC REFERENCE
	Биометрическая регистрация (внутренняя)	PBO CAPTURE AND STORE BIOMETRIC REFERENCE PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE	PBO CAPTURE AND STORE BIOMETRIC REFERENCE PBO CAPTURE AND UPDATE BIOMETRIC REFERENCE
	Биометрическая верификация	VERIFY PBO COMPARE BIOMETRIC PROBE PBO CAPTURE AND COMPARE BIOMETRIC PROBE	PBO COMPARE BIOMETRIC PROBE PBO CAPTURE AND COMPARE BIOMETRIC PROBE

Примечание — Предполагаемое использование операции COMPARE BIOMETRIC PROBE команды PBO для архитектуры BSoC — это операция CAPTURE AND COMPARE BIOMETRIC DATA команды PBO, аналогичное использованию команды VERIFY (без поля данных) в общем варианте использования.

Приложение *D*
(справочное)

Переходы состояний для управления временем BSoC

На рисунке D.1 показаны переходы состояний с точки зрения процессов на уровне системы при выполнении биометрической операции.

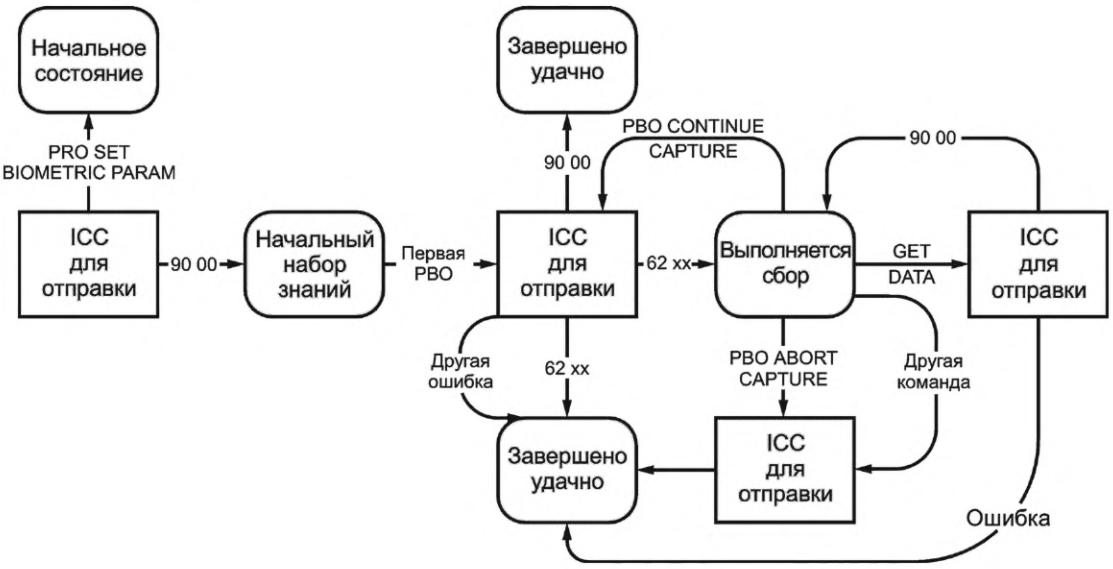


Рисунок D.1 — Переходы состояний

Приложение *E*
(справочное)

Примеры получения командных сообщений обратной связи

В таблицах Е.1 и Е.2 представлены некоторые примеры использования обмена сообщениями обратной связи.

Таблица Е.1 — Пример ошибочного сбора биометрических данных

IFD		ICC
PBO SET BIOMETRIC PARAMETER c DO '89'	→	
	←	'90 00'; нормальная обработка
...		
PBO CAPTURE AND COMPARE BIOMETRIC PROBE	→	
	←	'62 03'; обработка с предупреждением: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8A'-'01'-'FF'}-'90 00'; требуется больше времени
PBO CONTINUE CAPTURE	→	
	←	'64 03'; ошибка выполнения: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8C'-'01'-'00'}-'90 00' ; прервано, ошибка качества

Таблица Е.2 — Пример повторного сбора биометрических данных после неудачной попытки получения биометрических данных

IFD		ICC
PBO SET BIOMETRIC PARAMETER c DO '89'	→	
	←	'90 00'; нормальная обработка
...		
PBO CAPTURE AND SET BIOMETRIC REFERENCE PROBE	→	
	←	'62 03'; обработка с предупреждением: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8A'-'01'-'FF'}-'90 00'; требуется больше времени
PBO CONTINUE CAPTURE	→	
	←	'64 03'; обработка с предупреждением: доступны 03 байта сообщения обратной связи
GET DATA	→	
	←	{'8B'-'01'-'00'}-'90 00'; неудачная попытка получения биометрических данных, запрос нового биометрического образца
PBO CONTINUE CAPTURE	→	
	←	'90 00'; нормальная обработка

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных и межгосударственного стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р 58230—2018 (ИСО/МЭК 24787:2010)	MOD	ISO/IEC 24787:2010 «Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте»
ГОСТ Р 58671—2019 (ИСО/МЭК 7816-11:2017)	MOD	ISO/IEC 7816-11:2017 «Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами»
ГОСТ Р ИСО/МЭК 7816-3—2013	IDT	ISO/IEC 7816-3:2006 «Карты идентификационные. Карты на интегральных схемах. Часть 3. Карты с контактами. Электрический интерфейс и протоколы передачи»
ГОСТ Р ИСО/МЭК 7816-4—2013	IDT	ISO/IEC 7816-4:2005 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
ГОСТ Р ИСО/МЭК 14443-4—2014	IDT	ISO/IEC 14443-4:2008 «Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 4. Протокол передачи»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичные стандарты; - MOD — модифицированные стандарты.		

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта

Таблица ДБ.1

Структура настоящего стандарта	Структура международного стандарта ИСО/МЭК 17839-3:2016
Приложение B Примеры активации BSoC по собственной инициативе (приложение C)	Приложение B Сравнение команд, используемых среди разных видов реализаций, связанных с биометрией
Приложение C Сравнение команд, используемых среди разных видов реализаций, связанных с биометрией (приложение B)	Приложение C Примеры активации BSoC по собственной инициативе
Приложение D Переходы состояний для управления временем BSoC (приложение E)	Приложение D Примеры получения командных сообщений обратной связи
Приложение E Примеры получения командных сообщений обратной связи (приложение D)	Приложение E Переходы состояний для управления временем BSoC
Приложение ДА Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	—
Библиография	—
Примечания 1 Сопоставление структуры стандартов приведено начиная с приложения B, так как предыдущие разделы стандартов идентичны. 2 После заголовков приложений настоящего стандарта приведены в скобках обозначения аналогичных им приложений международного стандарта.	

Библиография

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

УДК 004.93'1:006.89:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, идентификационная карта, биометрическая система на идентификационной карте, биометрическое сравнение на идентификационной карте, механизм обратной связи

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *И.Ю. Литовкиной*

Сдано в набор 30.11.2021. Подписано в печать 28.12.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч-изд. л. 2,23.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru