ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58671— 2019 (ИСО/МЭК 7816-11:2017)

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 11

Верификация личности биометрическими методами

(ISO/IEC 7816-11:2017, MOD)

Издание официальное

Москва
Стандартинформ
2020

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «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 Акционерного общества «Ангстрем-Т» (АО «Ангстрем-Т») и 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 20 ноября 2019 г. № 1198-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 7816-11:2017 «Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами» (ISO/IEC 7816-11:2017 «Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

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

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 7816-11—2013

6 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут 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 в сети Интернет (www.gost.ru)

Содержание

Введение

Серия стандартов «Карты идентификационные. Карты на интегральных схемах» определяет карты на интегральных схемах и использование таких карт для обмена данными. Эти карты являются идентификационными картами, предназначенными для обмена информацией, согласованной между внешними устройствами и интегральной схемой на карте. В результате обмена информацией карта передает информацию (результат вычислений, сохраненные данные) и/или изменяет ее содержимое (хранение данных, запоминание события).

Пять стандартов серии «Карты идентификационные. Карты на интегральных схемах» описывают карты с гальваническими контактами, и три из них определяют электрические интерфейсы:

- *ГОСТ Р ИСО/МЭК 7816-1* устанавливает физические характеристики карт с контактами;
- *ГОСТ Р ИСО/МЭК 7816-2* — размеры и расположение контактов;
- *ГОСТ Р ИСО/МЭК 7816-3* — электрический интерфейс и протоколы передачи для асинхронных карт;
- *ГОСТ Р ИСО/МЭК 7816-10* — электрический интерфейс на восстановление для синхронных карт;
- *[1]* — электрический интерфейс и рабочие процедуры для USB-карт.

Другие стандарты не зависят от технологии физического интерфейса и применяются к тем картам, доступ к которым осуществлен с помощью контактов и/или радиочастоты:

- *ГОСТ Р ИСО/МЭК 7816-4* определяет организацию, защиту и команды для обмена информацией;
- *[2]* — провайдеров прикладных программ;
- *ГОСТ Р ИСО/МЭК 7816-6* — элементы данных для межотраслевого обмена;
- *ГОСТ Р ИСО/МЭК 7816-7* — команды для языка структурированных запросов для карты;
- *ГОСТ Р ИСО/МЭК 7816-8* — команды, обеспечивающие операции по защите информации;
- *ГОСТ Р ИСО/МЭК 7816-9* — команды для управления картами;
- *ГОСТ Р ИСО/МЭК 7816-11* — верификацию личности биометрическими методами;
- *ГОСТ Р ИСО/МЭК 7816-13* — команды для управления жизненным циклом приложения;
- *[3]* — приложение с криптографической информацией.

Серия стандартов *ГОСТ Р ИСО/МЭК 10536* определяет доступ при помощи поверхностного действия; серия стандартов *ГОСТ Р ИСО/МЭК 14443* и *ГОСТ Р ИСО/МЭК 15693* — радиочастотный доступ. Такие карты известны также как бесконтактные карты. *В серии стандартов ГОСТ Р ИСО/МЭК 17839 представлена биометрическая система на идентификационной карте.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 11

Верификация личности биометрическими методами

Identification cards. Integrated circuit cards.
Part 11. Personal verification through biometric methods

Дата введения — 2020—06—01

1 Область применения

Настоящий стандарт устанавливает межотраслевые команды, связанные с системой защиты и используемые для биометрической верификации личности с помощью карт на интегральных схемах. В настоящем стандарте также определены структура данных и методы доступа к данным для использования карты в качестве носителя биометрического контрольного шаблона и/или устройства, позволяющего выполнить верификацию биометрической пробы владельца карты (т. е. биометрическое сравнение на идентификационной карте). Биометрическая идентификация личности, *а также требования к криптографической защите информации, которые используются для обеспечения подлинности, целостности и конфиденциальности хранимых и передаваемых биометрических данных*, выходят за рамки настоящего стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 7.67 (ИСО 3166-1:1997) Система стандартов по информации, библиотечному и издательскому делу. Коды названий стран

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

ГОСТ ISO/IEC 7812-1 Карты идентификационные. Идентификация эмитентов. Часть 1. Система нумерации

ГОСТ Р ИСО/МЭК 7816-4—2013 Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена

ГОСТ Р ИСО/МЭК 7816-6 Карты идентификационные. Карты на интегральных схемах. Часть 6. Межотраслевые элементы данных для обмена

ГОСТ Р ИСО/МЭК 8825-1 Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования

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

ГОСТ Р 58294 (ИСО/МЭК 19785-3:2015) Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 3. Спецификации формата ведущей организации

Издание официальное

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 стандарта с учетом всех внесенных в данную версию изменений. Если изменен 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* и *ГОСТ Р ИСО/МЭК 7816-4*, а также следующие термины с соответствующими определениями:

3.1 **биометрическая информация** (biometric information): Информация, необходимая для внешних устройств при создании биометрической пробы.

3.2 **динамическая биометрическая верификация** (dynamic biometric verification): Биометрическая верификация, в процессе которой от человека требуется принятие динамического действия.

Примечание — Примерами динамических действий являются речь, данные временных рядов подписи и т. д. с динамично изменяющимися образцами. Эти действия могут быть использованы для статической биометрической верификации с фиксированными образцами.

3.3 **обработка биометрической регистрации** (enrolment processing): Акт создания и сохранения биометрического контрольного шаблона в соответствии с политикой биометрической регистрации.

3.4 **собранный извне** (externally-captured): Собранный без использования карты на интегральной схеме путем получения биометрических данных.

3.5 **механизм обратной связи** (feedback mechanism): Механизм информирования устройств без использования биометрической системы на идентификационной карте путем предоставления детализированного сообщения об ошибке, предупреждающего сообщения или сообщения о выполнении, дополняющего байты состояния посредством байтовых строк, инициированных идентификационной картой.

3.6 **собранный внутри** (internally-captured): Собранный на карте на интегральной схеме путем получения биометрических данных.

3.7 **необработанные данные** (raw data): Биометрический образец, собранный путем получения биометрических данных.

3.8 **сигнал** (signal): Последовательность аналоговых или цифровых выходных данных, изменения которых представляют собой закодированную информацию.

3.9 **статическая биометрическая верификация** (static biometric verification): Биометрическая верификация, в процессе которой от человека требуется предоставление физиологических (т. е. статических) характеристик или выполнение зарегистрированного, заранее определенного, действия.

Примечания

1 Примерами физиологических характеристик являются лицо, отпечаток пальца, радужная оболочка глаза и т. д.

2 Примерами выполнения зарегистрированных, заранее определенных действий являются походка, речь, данные временных рядов подписи с фиксированными образцами.

3.10 **шаблон** (template): Множество информационных объектов BER-TLV для формирования поля значения составного информационного объекта BER-TLV.

Примечание — Термин «шаблон» — это поле значений составного объекта данных, а не обработанный образец биометрических данных.

[*ГОСТ Р ИСО/МЭК 7816-4—2013, пункт 3.44*, модифицирован]

4 Обозначения и сокращения

В настоящем стандарте применены обозначения и сокращения по *ГОСТ Р ИСО/МЭК 7816-4*, а также следующие сокращения и обозначения:

AID — идентификатор приложения (Application Identifier);

BER — базовые правила кодирования ASN.1 (Basic Encoding Rules of ASN.1);

BHT — шаблон биометрического заголовка (Biometric Header Template, BHT);

ЕСФОБД — единая структура форматов обмена биометрическими данными (Common Biometric Exchange Formats Framework, CBEFF);

DF — назначенный файл (Dedicated File);

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

ICC — карта на интегральной схеме;

L — поле длины DO TLV (Length field of TLV DO);

OID — идентификатор объекта (Object identifier);

PBO — «выполнить биометрическую операцию» (PERFORM BIOMETRIC OPERATION);

RFU — зарезервировано для будущего использования ИСО/МЭК СТК 1/ПК 17 (Reserved for Future Use by ISO/IEC JTC 1/SC 17);

TLV — тег, длина, значение (Tag, Length, Value);

VIDO — объект данных информации о требованиях к верификации (Verification requirement Information Data Object);

VIT — шаблон информации о требованиях к верификации (Verification requirement Information Template).

5 Команды для процессов, связанных с биометрической верификацией

5.1 Общие положения

Команда `PERFORM BIOMETRIC OPERATION (PBO)`, определенная в 5.4, описывает биометрические операции для регистрации (хранения биометрических данных на ICC) и верификации (сравнения биометрических данных с данными биометрического контрольного шаблона, хранящимися на ICC). Как хранение, так и сравнение биометрических данных могут быть также реализованы с помощью команд, приведенных в *ГОСТ Р ИСО/МЭК 7816-4* (например, `PUT DATA`, `UPDATE BINARY` — для хранения, `VERIFY` — для сравнения).

5.2 Команды для процесса статической биометрической верификации

Командой, используемой в процессе статической биометрической верификации (см. приложение А), является команда `VERIFY`, определенная в *ГОСТ Р ИСО/МЭК 7816-4*, или команда `PBO` с соответствующими операциями, например путем сравнения биометрической пробы, как указано в 5.4. При использовании команды `VERIFY` и внешнем сборе биометрических данных команда должна содержать биометрические данные в виде биометрической пробы для сравнения в своем поле данных, закодированном в соответствии с *6.1* и *6.2*. Идентификатор биометрического алгоритма должен быть:

- неявно известным, либо
- определен в безопасной среде (SE) в контрольном шаблоне управляющих ссылок для аутентификации (AT), либо
- определен в данных команд в шаблоне биометрической информации (см. *ГОСТ Р 58230)*, или
- определен в данных команд в контрольном шаблоне управляющих ссылок для аутентификации.

Классификатор биометрических шаблонов может быть определен:

- в SE в контрольном шаблоне управляющих ссылок для аутентификации, либо
- параметре P2 команды `VERIFY` или `PBO`, либо
- данных команды в шаблоне биометрической информации (см. 7.1), либо
- данных команды в шаблоне биометрических данных (см. 7.2), либо
- данных команды в контрольном шаблоне управляющих ссылок для аутентификации.

Биометрическая проба может быть записана в шаблоне биометрической информации (см. *6.1*) или в шаблоне группы шаблонов биометрической информации (см. *6.1*). Биометрическая проба может быть закодирована как объект данных BER-TLV (см. *6.2*).

Биометрические данные, собранные на ICC или без ее использования, можно сравнить. В случае сравнения биометрической пробы, собранной извне, должен быть реализован механизм обратной связи, определенный в *[4]*, с операциями PBO, приведенными в 5.4.6.

5.3 Команды для процесса динамической биометрической верификации

Для того чтобы создать задачу, для которой требуется ответ пользователя (см. приложение А), необходимо использовать команду GET CHALLENGE, определенную в *ГОСТ Р ИСО/МЭК 7816-4*, или команду PBO (см. 5.4).

Как указано в *ГОСТ Р ИСО/МЭК 7816-4*, значение P1, равное '00', подразумевает, что информация не предоставляется, т. е. биометрический алгоритм известен перед выполнением команды. Другие значения P1 являются RFU.

Тип задачи в процессе биометрической верификации, например фраза для регистрации голоса или клавиатурного почерка, зависит от биометрического алгоритма. Если задача запрашивается с помощью команды GET CHALLENGE, параметр P1 команды GET CHALLENGE должен идентифицировать биометрический алгоритм. Если задача запрашивается с помощью команды PBO, то биометрический алгоритм должен быть:

- неявно известным или
- определен в SE в контрольном шаблоне управляющих ссылок для аутентификации.

Соответствующий алгоритм может быть выбран альтернативно с помощью команды MSE (например, опция SET с AT, используя DO квалификатора и DO алгоритма в поле данных команды).

После получения биометрического вызова команда EXTERNAL AUTHENTICATE или команда PBO должны быть отправлены на ICC. Поле данных команды передает соответствующую биометрическую пробу.

5.4 Команда PBO

5.4.1 Основное определение команды PBO

Одна или несколько команд PBO могут быть использованы для биометрической верификации и связанных с ней процессов. Она инициирует различные виды биометрических операций и другие относящиеся к ним операции в соответствии со значением, указанным в P1.

В таблице 1 P1 указывает на одну операцию, связанную с биометрией.

Таблица 1 — Пара «команда PERFORM BIOMETRIC OPERATION — ответ»

Поле	Описание
CLA	Как определено в 5.4.1 *ГОСТ Р ИСО/МЭК 7816-4—2013*
INS	'2E'
P1	Номер функции и вариант применения (см. *5.4.3*)
P2	См. таблицу 2
Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Отсутствует или присутствует в соответствии с P1
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$
Поле данных	Отсутствует или присутствует в соответствии с P1
SW1-SW2	Как определено в таблицах 5 и 6 *ГОСТ Р ИСО/МЭК 7816-4—2013*, например '6281', '6282', '6700', '6981', '6982', '6A81', '6A82', '6A83'

В таблице 2 P2 квалифицирует биометрический контрольный шаблон тем же способом, что и для основной команды регуляции безопасности, определенной в *ГОСТ Р ИСО/МЭК 7816-4*.

Таблица 2 — P2 команды PBO

P2								Значение
b8	b7	b6	b5	b4	b3	b2	b12	
0	0	0	0	0	0	0	0	Информация не приводится
0	—	—	—	—	—	—	—	Глобальный биометрический контрольный шаблон (например, определен MF)
1	—	—	—	—	—	—	—	Определенный биометрический контрольный шаблон (например, определен DF приложения)
—	x	x	—	—	—	—	—	00 (любое другое значение — это RFU)
—	—	—	x	x	x	x	x	Квалификатор, то есть число биометрических контрольных шаблонов

Команде PBO может предшествовать команда MSE для установки соответствующих параметров. Например, команда MSE задает контрольный шаблон управляющих ссылок, пригодный для аутентификации в SE. Когда выполняется команда PBO, SE может транспортировать индикацию аутентификации биометрического пользователя с помощью квалификатора его биометрического контрольного шаблона.

5.4.2 Операции команды PBO

В нижеприведенном перечне описаны функциональные возможности операций команды PBO (см. также таблицы 3 и 4):

- SET INITIAL VALUES:
  - операция SET INITIAL VALUES команды PBO предназначена для задания начальных значений биометрии;
- STORE BIOMETRIC REFERENCE,
- UPDATE BIOMETRIC REFERENCE:
  - операции STORE BIOMETRIC REFERENCE и UPDATE BIOMETRIC REFERENCE команды PBO предназначены для регистрации собранных извне биометрических данных;
- CAPTURE AND STORE BIOMETRIC REFERENCE,
- CAPTURE AND UPDATE BIOMETRIC REFERENCE:
  - операции CAPTURE AND STORE BIOMETRIC REFERE и CAPTURE AND UPDATE BIOMETRIC REFERENCE команды PBO предназначены для регистрации собранных внутри биометрических данных;
- COMPARE BIOMETRIC PROBE:
  - операция COMPARE BIOMETRIC PROBE команды PBO предназначена для сравнения собранной извне биометрической пробы с биометрическим контрольным шаблоном;
- CAPTURE AND COMPARE BIOMETRIC PROBE:
  - операция CAPTURE AND COMPARE BIOMETRIC PROBE команды PBO предназначена для сравнения собранной внутри биометрической пробы с биометрическим контрольным шаблоном;
- RETRIEVE BIOMETRIC REFERENCE:
  - операция RETRIEVE BIOMETRIC REFERENCE команды PBO предназначена для извлечения биометрического контрольного шаблона из ICC;
- GENERATE BIOMETRIC VALIDATION CERTIFICATE:
  - операция GENERATE BIOMETRIC VALIDATION CERTIFICATE команды PBO предназначена для генерации валидированного биометрического сертификата;
- GENERATE CONTROL VALUE:
  - операция GENERATE CONTROL VALUE команды PBO предназначена для генерации контрольного значения для биометрии;
- STORE BIOMETRIC INFORMATION:
  - операция STORE BIOMETRIC INFORMATION команды PBO предназначена для внешнего сохранения сгенерированного сертификата для биометрического контрольного шаблона;
- GET BIOMETRIC CHALLENGE:

- операция GET BIOMETRIC CHALLENGE команды PBO предназначена для получения биометрической задачи перед операциями COMPARE BIOMETRIC PROBE и CAPTURE AND COMPARE BIOMETRIC PROBE в случае процесса динамической биометрической верификации;
- SET BIOMETRIC PARAMETER,
- CONTINUE CAPTURE,
- ABORT CAPTURE:
- операции SET BIOMETRIC PARAMETER, CONTINUE CAPTURE и ABORT CAPTURE команды PBO предназначены для механизма обратной связи.

Таблица 3 — Поле данных команды и ответа команды PBO

Операция	Поле данных команды		Поле данных ответа	
SET INITIAL VALUES	DO'73'	Шаблон начальных значений биометрии	—	Отсутствует
STORE BIOMETRIC REFERENCE	DO'7F2E' DO'7F60' DO'7F61'	Биометрический контрольный шаблон: - биометрических данных; - биометрической информации; - группы шаблонов биометрической информации	—	Отсутствует
UPDATE BIOMETRIC REFERENCE	DO'7F2E' DO'7F60' DO'7F61'	Биометрический контрольный шаблон: - биометрических данных; - биометрической информации; - группы шаблонов биометрической информации	—	Отсутствует
CAPTURE AND STORE BIOMETRIC REFERENCE	—	Отсутствует	—	Отсутствует
CAPTURE AND UPDATE BIOMETRIC REFERENCE	—	Отсутствует	—	Отсутствует
COMPARE BIOMETRIC PROBE	DO'7F2E' DO'7F60' DO'7F61'	Биометрическая проба: - биометрических данных; - биометрической информации; - группы шаблонов биометрической информации	—	Отсутствует
CAPTURE AND COMPARE BIOMETRIC PROBE	—	Отсутствует	—	Отсутствует
RETRIEVE BIOMETRIC REFERENCE	—	Отсутствует	DO'7F60' DO'7F61'	Биометрический контрольный шаблон: - биометрической информации; - группы шаблонов биометрической информации

Окончание таблицы 3

Операция	Поле данных команды		Поле данных ответа	
GENERATE BIOMETRIC VALIDATION CERTIFICATE	DO'53'/ DO'73'/—	Квалификатор данных биометрического контрольного шаблона, шаблон квалификатора данных биометрического контрольного шаблона или отсутствует	DO'73'	Шаблон биометрического сертификата
GENERATE CONTROL VALUE	—	Отсутствует	DO'73'	Шаблон контрольных значений
STORE BIOMETRIC INFORMATION	DO'A5'	Биометрическая информация	—	Отсутствует
GET BIOMETRIC CHALLENGE	—	Отсутствует	DO'53'/ DO'73'	Шаблон биометрической задачи (простой/ составной)
SET BIOMETRIC PARAMETER	DO'B1'	Объекты данных для элементов данных конфигурации	—	Отсутствует
CONTINUE CAPTURE	—	Отсутствует	—	Отсутствует
ABORT CAPTURE	—	Отсутствует	—	Отсутствует

Примечания

1 Шаблон биометрических данных DO'7F2E' определен в *6.2*.

2 Шаблон биометрической информации DO'7F60' приведен в *6.1*.

3 Шаблон группы шаблонов биометрической информации определен в *6.1*.

4 DO'B1'инкапсулирован в шаблон биометрической информации DO'7F60' как объект данных для элементов данных конфигурации, определенный в *ГОСТ Р 58230*.

8-й бит P1, установленный на 0, предназначен для общего применения операции; 8-й бит P1, установленный на 1, — для определенных применений (см. таблицу 4).

Таблица 4 — Кодирование P1 команды PBO

P1								Операция
b8	b7	b6	b5	b4	b3	b2	b1	
0	x	x	x	x	x	x	x	Общее применение
1	x	x	x	x	x	x	x	Определенное применение
x	0	0	0	0	0	0	1	SET INITIAL VALUES
x	0	0	0	0	0	1	0	STORE BIOMETRIC REFERENCE
x	0	0	0	0	0	1	1	UPDATE BIOMETRIC REFERENCE
x	0	0	0	0	1	0	0	CAPTURE AND STORE BIOMETRIC REFERENCE
x	0	0	0	0	1	0	1	CAPTURE AND UPDATE BIOMETRIC REFERENCE
x	0	0	0	0	1	1	0	COMPARE BIOMETRIC PROBE
x	0	0	0	0	1	1	1	CAPTURE AND COMPARE BIOMETRIC PROBE

Окончание таблицы 4

P1								Операция
b8	b7	b6	b5	b4	b3	b2	b1	
x	0	0	0	1	0	0	0	RETRIEVE BIOMETRIC REFERENCE
x	0	0	0	1	0	0	1	GENERATE BIOMETRIC VALIDATION CERTIFICATE
x	0	0	0	1	0	1	0	GENERATE CONTROL VALUE
x	0	0	0	1	0	1	1	STORE BIOMETRIC INFORMATION
x	0	0	0	1	1	0	0	GET BIOMETRIC CHALLENGE
x	0	0	0	1	1	0	1	SET BIOMETRIC PARAMETER
x	0	0	0	1	1	1	0	CONTINUE CAPTURE
x	0	0	0	1	1	1	1	ABORT CAPTURE
x	x	x	x	x	x	x	x	Остальные значения являются RFU

5.4.3 Регистрация биометрического контрольного шаблона

5.4.3.1 Регистрация собранных извне биометрических данных

Операции STORE BIOMETRIC REFERENCE и UPDATE BIOMETRIC REFERENCE команды PBO, определенные в таблицах 3 и 4, предназначены для регистрации собранных извне биометрических данных и для сохранения результирующего биометрического контрольного шаблона с соответствующей биометрической информацией в ICC.

5.4.3.2 Регистрация собранных внутри биометрических данных

Операции CAPTURE AND STORE BIOMETRIC REFERENCE команды PBO, определенные в таблицах 3 и 4, предназначены для регистрации собранных внутри биометрических данных и для сохранения результирующего биометрического контрольного шаблона с соответствующей биометрической информацией в ICC.

5.4.4 Извлечение биометрического контрольного шаблона

Операция RETRIEVE BIOMETRIC REFERENCE команды PBO, определенная в таблицах 3 и 4, предназначена для извлечения биометрического контрольного шаблона из ICC.

5.4.5 Сравнение биометрической пробы

5.4.5.1 Сравнение собранной извне биометрической пробы

Операция COMPARE BIOMETRIC PROBE команды PBO, определенная в таблицах 3 и 4, предназначена для сравнения собранной извне биометрической пробы с биометрическим контрольным шаблоном. В случае процесса динамической биометрической верификации операция GET BIOMETRIC CHALLENGE команды PBO, приведенная в таблицах 3 и 4, применена для получения биометрической задачи перед операцией COMPARE BIOMETRIC PROBE.

5.4.5.2 Сравнение собранной внутри биометрической пробы

Операция CAPTURE AND COMPARE BIOMETRIC PROBE команды PBO, определенная в таблицах 3 и 4, предназначена для сравнения собранной внутри биометрической пробы с биометрическим контрольным шаблоном. В случае процесса динамической биометрической верификации операция GET BIOMETRIC CHALLENGE команды PBO, приведенная в таблицах 3 и 4, применена для получения биометрической задачи перед операцией CAPTURE AND COMPARE BIOMETRIC PROBE.

5.4.6 Механизм обратной связи во время процесса получения биометрических данных

Получение биометрических данных во время регистрации или сравнения требует взаимодействия с пользователем, поэтому предсказать его поведение, требующее контроля времени, не представляется возможным. В связи с чем следует использовать механизм обратной связи, определенный в *[4]*. Операции SET BIOMETRIC PARAMETER, CONTINUE CAPTURE и ABORT CAPTURE команды PBO, приведенные в таблицах 3 и 4, предназначены для механизма обратной связи.

В таблице 5 указаны детали операции SET BIOMETRIC PARAMETER команды PBO для управления временем ожидания на уровне приложения, определенном в *[4]*.

Таблица 5 — Время ожидания на уровне приложения установки с помощью операции SET BIOMETRIC PARAMETER команды PBO

Операция	P1	Поле данных команды		Поле данных ответа	
SET BIOMETRIC PARAMETER (время ожидания на уровне приложения установки)	'0D'	DO'89'	Время ожидания на уровне приложения, определенное в *[4]*. В случае пустого объекта данных время ожидания приложения известно неявно	—	Отсутствует

6 Элементы данных

6.1 Биометрическая информация

Шаблон биометрической информации предоставляет наглядную информацию по соответствующим биометрическим данным. Он предусмотрен картой в ответ на команду извлечения, предшествующую процессу биометрической верификации (см. приложение А). В таблицах *6* и *7* определены DO биометрической информации.

Шаблон биометрической информации может содержать биометрические данные (см. 6.2). В случае биометрического сравнения вне идентификационной карты биометрический контрольный шаблон в качестве биометрических данных должен быть включен в шаблон биометрической информации, так как для биометрической верификации без использования идентификационной карты требуется как биометрический контрольный шаблон, так и его информация. В случае сравнения на идентификационной карте и в том случае, когда система вне идентификационной карты запрашивает информацию о биометрическом контрольном шаблоне, биометрический контрольный шаблон без биометрических данных и биометрические данные в качестве биометрического контрольного шаблона должны храниться отдельно на ICC, так как данный биометрический контрольный шаблон должен быть защищен от извлечения.

Таблица 6 — DO биометрической информации в шаблоне биометрической информации (неявное кодирование распределения тегов)

Тег		L	Значение	Наличие
Шаблон биометрической информации				
'7F60' (переменная длина)	'80'	1	Ссылка на алгоритм для биометрической верификации	Необязательно
	'83'	1	Квалификатор данных биометрического контрольного шаблона для биометрической верификации	Необязательно
	'A0'	Переменная	RFU для DO биометрической информации, определенный в настоящем стандарте	Необязательно
	'06'	Переменная	Орган распределения тегов (см. *ГОСТ Р ИСО/МЭК 7816-6*): - идентификатор объекта (OID, кодирование определено в *ГОСТ Р ИСО/МЭК 8825-1*);	Один из этих DO является обязательным, если 'A1' присутствует
	'41'	Переменная	- код страны (кодирование определено в *ГОСТ 7.67)* и дополнительные данные;	
	'42'	Переменная	- идентификационный номер эмитента (кодирование и регистрация определены в *ГОСТ ISO/IEC 7812-1*) и дополнительные данные эмитента;	
	'4F'	Переменная	- идентификатор приложения (AID, кодирование определено *ГОСТ Р ИСО/МЭК 7816-4*) Орган распределения тегов по умолчанию — ИСО/МЭК СТК 1/ПК 37 *(на международном уровне)* и *ТК 098 (на национальном уровне)*	

Окончание таблицы 6

Тег		L	Значение	Наличие
'7F60' (переменная длина)	'A1'	Переменная	DO биометрической информации, заданные органом распределения тегов (указание обязательно, см. выше) См. TLV-закодированный формат ведущей организации, определенный в *ГОСТ Р 58294*	Обязательно, если 'A0' не присутствует
	'8x'/'Ax'	Переменная	DO, указанные органом распределения тегов (простые/составные)	Зависит от DO
	'9x'/'Bx'	Переменная	DO, указанные органом распределения тегов: простые/составные)	Зависит от DO
	'5F-2E'/ '7F-2E'	Переменная	Биометрические данные (см. *6.2*)	Обязательно в качестве биометрической пробы или извлеченного биометрического контрольного шаблона в случае биометрического сравнения вне идентификационной карты

Таблица 7 — DO биометрической информации в шаблоне биометрической информации (явное кодирование распределения тегов)

Тег		L	Значение	Наличие
Шаблон биометрической информации				
'7F60' (переменная длина)	'80'	1	Ссылка на алгоритм для биометрической верификации	Необязательно
	'83'	1	Квалификатор данных биометрического контрольного шаблона для биометрической верификации	Необязательно
	'A0'	Переменная	RFU для DO биометрической информации, определенный в настоящем стандарте	Необязательно
	'A1'	Переменная	DO биометрической информации, определенные другим документом (*см. таблицу 7.1*)	Обязательно, если 'A0' не присутствует
	'5F2E'/ '7F2E'	Переменная	Биометрические данные (см. *6.2*)	Обязательно в качестве биометрической пробы или извлеченного биометрического контрольного шаблона в случае биометрического сравнения вне идентификационной карты

Таблица 7.1 — DO биометрической информации, определенный другим документом, в шаблоне биометрической информации (явное кодирование распределения тегов)

Тег		L	Значение	Наличие
DO биометрической информации, определенные другим документом				
'A1'	'78'	Переменная	Совместимый орган распределения тегов	Обязательно, если 'A1' присутствует
	'06'	Переменная	Идентификатор объекта (OID, кодирование определено в *ГОСТ Р ИСО/МЭК 8825-1*)	Как правило, присутствует один из данных DO
	'41'	Переменная	Код страны (кодирование определено в *ГОСТ 7.67*) и дополнительные данные	
	'42'	Переменная	Идентификационный номер эмитента (кодирование и регистрация определены в *ГОСТ ISO/IEC 7812-1*) и дополнительные данные эмитента	
	'4F'	Переменная	Идентификатор приложения (AID, кодирование определено в *ГОСТ Р ИСО/МЭК 7816-4*)	
	'70'	Переменная	DO биометрической информации, заданные органом распределения тегов	Необязательно
Примечание — Если DO'78' под DO'A1' совместимого органа распределения тегов не существует, то орган распределения тегов по умолчанию ИСО/МЭК СТК 1/ПК 37 *(на международном уровне)* и *ТК 098 (на национальном уровне)*.				

Если несколько шаблонов биометрической информации присутствуют в рамках одного приложения, то они должны быть сгруппированы, как показано в таблице 8.

Дальнейшие примеры шаблонов биометрической информации приведены в приложении В.

Теги, указанные в приложении С, могут содержаться в шаблоне биометрической информации в случае явного кодирования распределения тегов (см. таблицу 7 и *таблицу 7.1*).

Таблица 8 — Шаблон группы шаблонов биометрической информации

Тег		L	Значение	Наличие
Шаблон группы шаблонов биометрической информации				
'7F61' (переменная длина)	'02'	Переменная	Число шаблонов биометрической информации в группе	Обязательно
	'7F60'	Переменная	Шаблон биометрической информации 1	Необязательно
	—	—	...	—
	'7F60'	Переменная	Шаблон биометрической информации 2	Необязательно

6.2 Биометрические данные

Биометрические данные закодированы в DO'5F2E' или DO'7F2E', как определено в *ГОСТ Р ИСО/МЭК 7816-6*. В таблице *9* указаны DO биометрических данных, которые могут быть включены в шаблон биометрической информации (см. *6.1*).

Таблица 9 — DO биометрических данных

Тег		L	Значение	Наличие
Шаблон биометрических данных				
'7F2E' (переменная длина)	'80'/ 'A0'	Переменная	Задача для подсказки держателю карты (см. 6.3.2 для 'A0')	Необязательно для динамической биометрической верификации
	'5F2E'		Биометрические данные	Как правило, присутствует один из данных DO, если используется шаблон. Тот же номер тега может присутствовать несколько раз в одном шаблоне
	'81'/ 'A1'		Биометрические данные в стандартизованном формате (простые/составные)	
	'82'/ 'A2'		Биометрические данные в проприетарном формате (простые/составные)	
	'83'	1	—	Если шаблон биометрических данных не является шаблоном биометрической информации, то может присутствовать этот DO

Как показано в таблице 9, биометрические данные могут быть разделены на данные в стандартизованном формате и на данные в проприетарном формате, при этом данные в проприетарном формате могут быть использованы, например, для повышения качества работы и/или для применения внутренних ресурсов. Использование биометрических данных в стандартизованном и проприетарном форматах показано на рисунке 1. Данный пример описывает соответственно два вида ссылок на алгоритмы, внедренные на картах. Оба алгоритма принадлежат к одному и тому же биометрическому типу, например отпечатку пальца, но могут вычислять результаты биометрической верификации посредством различных проприетарных биометрических данных так же, как и стандартизованных биометрических данных. Когда устройство интерфейса поддерживает только алгоритм А, оно может определить биометрическую пробу для поля данных команды VERIFY в соответствии со ссылкой на алгоритм, возвращенной от ICC.

Структура и кодирование биометрического контрольного шаблона и биометрической пробы держателя карты в стандартизованном формате зависят от биометрического типа (например, изображение лица, отпечаток пальца) и выходят за рамки настоящего стандарта.

Биометрическая задача для подсказки для держателя карты должна быть закодирована в DO'A0' или DO'80' для динамической биометрической верификации (см. 5.3). Образец шаблона биометрической задачи показан в таблице 10.

6.3 Информация о верификации

6.3.1 Назначение

Текущая информация о верификации обеспечивается:

- объектом данных информации о верификации (VIDO) (тег '96', простой) либо
- шаблоном информации о верификации (VIT) (тег 'A6', составной).

VIDO или VIT могут содержаться в контрольной информации файла соответствующего DF, как определено в *ГОСТ Р ИСО/МЭК 7816-4*, или хранить в EF, содержащем расширение контрольной информации файла. Для этой цели в *ГОСТ Р ИСО/МЭК 7816-4* определен DO'87' в качестве идентификатора EF, содержащего расширение контрольной информации файла под DO'62' шаблона контрольного параметра файла (FCP) для DF. VIDO и VIT содержат информацию, которая указывает включение/отключение требования верификации с использованием биометрического контрольного шаблона. Для переключения этого состояния информации о верификации можно применять команду ENABLE VERIFICATION REQUIREMENT/DISABLE VERIFICATION REQUIREMENT, определенную в *ГОСТ Р ИСО/МЭК 7816-4*. В VIDO и VIT также приведена информация относительно того, раз-

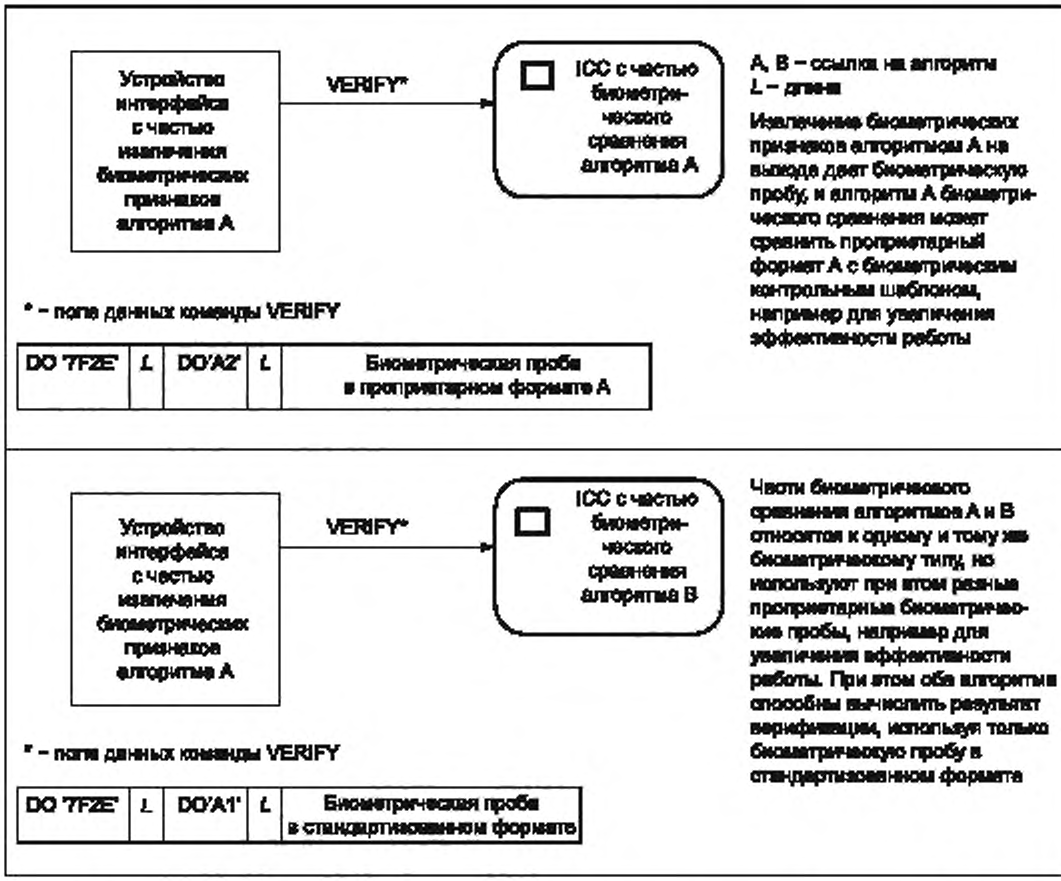

Рисунок 1 — Пример использования биометрических данных в стандартизованном и проприетарном форматах

Таблица *10* — Шаблон биометрической задачи

Тег		*L*	Значение
Шаблон биометрической задачи			
'A0' (переменная длина)	'90'	Переменная	Квалификатор задачи: '00' — информация не приводится (не определено); '01' — кодирование UTF8 (по умолчанию); другие значения — RFU
	'80'	Переменная	Задача

решены (применимо)/запрещены (неприменимо) дальнейшие попытки верификации. Если установлено максимальное число попыток биометрической верификации и достигнуто максимальное число последовательных неудачных попыток биометрической верификации, биометрический контрольный шаблон становится неприменимым. Для переключения состояния неприменимости в состояние применимости может быть использована команда RESET RETRY COUNTER, если это позволяет атрибут секретности.

Примечание — В поле P2 команд ENABLE VERIFICATION REQUIREMENT и DISABLE VERIFICATION REQUIREMENT приведен квалификатор, т. е. количество данных шаблона или пароль. Квалификатор использования в шаблоне управляющих ссылок, допустимый для аутентификации (AT) в текущей SE, может указывать, на чем основана аутентификация пользователя — на пароле (секретная) или на биометрии (биометрический контрольный шаблон). Этот квалификатор использования в текущей SE может быть обработан с помощью команды MANAGE SECURITY ENVIRONMENT (MSE).

6.3.2 Объект данных информации о верификации (VIDO)

Первый байт поля значений в объекте данных информации о верификации (VIDO) указывает информацию о верификации биометрического контрольного шаблона (см. таблицы *11* и *12*). Бит b8 этого байта указывает разрешение/запрещение информации о верификации биометрического контрольного шаблона, на которую ссылается третий байт поля значений в VIDO, при его наличии. Каждый бит, за которым следует b8, указывает информацию о верификации биометрического контрольного шаблона, на которую ссылается каждый байт, за которым следует 3-й байт.

Второй байт поля значений в VIDO определяет применимые биометрические контрольные шаблоны (см. таблицу *13*). Бит b8 этого байта указывает применимость/неприменимость биометрического контрольного шаблона, на который ссылается третий байт поля значений VIDO, если он присутствует. Каждый бит, за которым следует b8, определяет применимость биометрического контрольного шаблона, на который ссылается каждый байт, за которым следует третий байт.

В поле значений VIDO содержится не более восьми квалификаторов биометрических контрольных шаблонов. Если число квалификаторов биометрических контрольных шаблонов менее восьми, допустимо число битов из b8 в первом и втором байтах.

Таблица *11* — Кодирование DO информации о верификации

Тег	*L*	Значение			
		Первый байт	Второй байт	Третий байт	...
'96'	От 3 до 10	Байт информации о верификации	Байт применимого биометрического контрольного шаблона	Квалификатор биометрического контрольного шаблона. Относящиеся к b8 1-й и 2-й байты	...

Таблица *12* — Кодирование байта информации о верификации

b8	b7	b6	b5	b4	b3	b2	b1	Значение
1	—	—	—	—	—	—	—	Разрешенная биометрическая информация, использующая биометрический контрольный шаблон, на который ссылается 3-й байт, если присутствует
—	1	—	—	—	—	—	—	То же самое для 4-го байта
—	—	1	—	—	—	—	—	То же самое для 5-го байта
—	—	—	1	—	—	—	—	То же самое для 6-го байта
—	—	—	—	1	—	—	—	То же самое для 7-го байта
—	—	—	—	—	1	—	—	То же самое для 8-го байта
—	—	—	—	—	—	1	—	То же самое для 9-го байта
—	—	—	—	—	—	—	1	То же самое для 10-го байта

Таблица *13* — Кодирование байта применимого биометрического контрольного шаблона

b8	b7	b6	b5	b4	b3	b2	b1	Значение
1	—	—	—	—	—	—	—	Применимый биометрический контрольный шаблон, на который ссылается 3-й байт, если присутствует

Окончание таблицы 13

b8	b7	b6	b5	b4	b3	b2	b1	Значение
—	1	—	—	—	—	—	—	То же самое для 4-го байта
—	—	1	—	—	—	—	—	То же самое для 5-го байта
—	—	—	1	—	—	—	—	То же самое для 6-го байта
—	—	—	—	1	—	—	—	То же самое для 7-го байта
—	—	—	—	—	1	—	—	То же самое для 8-го байта
—	—	—	—	—	—	1	—	То же самое для 9-го байта
—	—	—	—	—	—	—	1	То же самое для 10-го байта

6.3.3 Шаблон информации о верификации (VIT)

Шаблон биометрической информации предназначен для поддержки более чем восьми квалификаторов биометрических контрольных шаблонов (см. таблицу *14*). Он состоит из одного или более DO'A4' шаблонов аутентификации, основанных на биометрии. DO'A4' шаблон аутентификации, основанный на биометрии, состоит из DO'81' объектов данных требований к верификации, DO'82' объектов данных квалификаторов применимых биометрических контрольных шаблонов и DO'83' объектов данных квалификаторов биометрических контрольных шаблонов. Каждый из DO'81', DO'82' и DO'83' содержится в DO'A4' как минимум один раз. В DO'A4' могут быть другие DO.

Таблица *14* — Кодирование шаблона информации о верификации

Тег		L	Значение
Шаблон информации о верификации (VIT)			
'A6' (переменная длина)	'A4'	Переменная	Шаблон аутентификации, основанный на биометрии
	'81'	1	Объект данных требований к биометрической верификации: - '00' — требование запрещенной биометрической верификации; - '01' — требование разрешенной биометрической верификации; - другое значение — RFU
	'82'	1	Объект данных квалификаторов применимых биометрических контрольных шаблонов: - '00' — квалификатор неприменимого биометрического контрольного шаблона; - '01' — квалификатор применимого биометрического контрольного шаблона; - другое значение — RFU
	'83'	1	Объект данных квалификаторов биометрических контрольных шаблонов
	'A4'	Переменная	Шаблон аутентификации, основанный на биометрии

Приложение А
(справочное)

Процесс биометрической верификации

А.1 Процессы биометрической регистрации

На рисунках А.1 и А.2 показаны общие (упрощенные) схемы процессов биометрической регистрации.

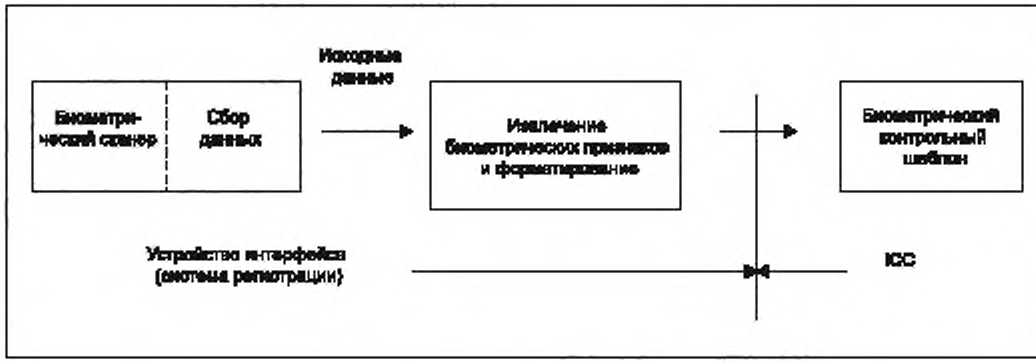

Рисунок А.1 — Общая схема процесса биометрической регистрации собранных извне биометрических данных

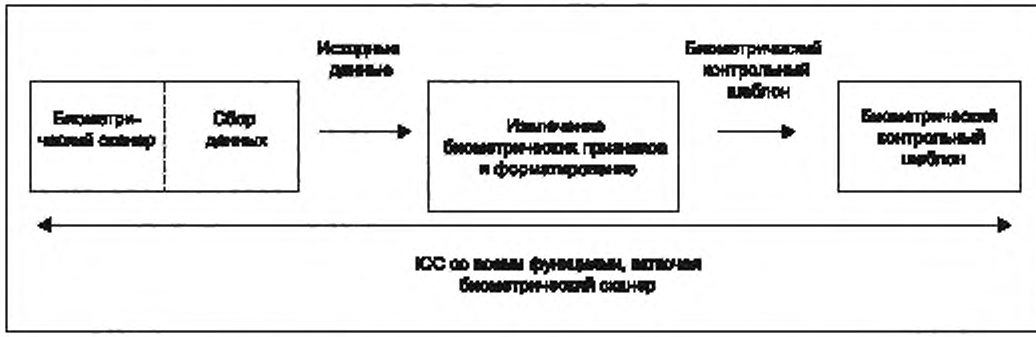

Рисунок А.2 — Общая схема процесса биометрической регистрации собранных внутри биометрических данных

В случае биометрической регистрации собранных извне биометрических данных (см. рисунок А.1) биометрический образец, как правило, обрабатывается вне идентификационной карты из-за значительного размера биометрического образца. Во время этой обработки биометрические признаки извлекаются и форматируются для последующего использования. В процессе регистрации или на более позднем этапе биометрический контрольный шаблон отправляется безопасным способом на карту для хранения и применения в дальнейшем.

Существуют ICC, содержащие биометрический сканер и модуль получения данных, которые могут зарегистрировать полученные внутри биометрические данные (см. рисунок А.2). В этом случае они собирают биометрический образец, обрабатывают его и сохраняют биометрический контрольный шаблон на карте.

Для обеих схем параметры, связанные с биометрической верификацией, могут быть сохранены в процессе регистрации.

Биометрические контрольные шаблоны могут быть сохранены на карту:

- в течение фазы персонализации карты;
- после выдачи карты держателю карты.

В *ГОСТ Р 58230* приведены упрощенные схемы для верификации.

А.2 Классификация методов биометрической верификации

Биометрические модальности можно разделить на два типа.

Основными характеристиками первого биометрического типа (типа А) являются:

- уникальность, неизменяемость;
- выбираемость, если существует несколько экземпляров того же класса (например, большой палец, указательный палец);
- открытость, если соответствующий признак (например, лицо, отпечаток пальца) каждого человека может быть зарегистрирован и измерен, т. е. соответствующая биометрическая проба должна быть представлена карте аутентичным способом.

Основными характеристиками второго биометрического типа (типа В) являются:

- уникальность, но изменяемость;
- зависимость от задачи, если используется динамическая биометрическая верификация.

Примеры биометрического типа А:

- черты лица;
- геометрия пальцев;
- отпечаток пальца;
- геометрия кисти руки;
- радужная оболочка глаза;
- геометрия ладони;
- сетчатка глаза;
- рисунок вен.

Примеры биометрического типа В:

- клавиатурный почерк;
- движение губ;
- изображение подписи;
- спектр речевых сигналов (запись голоса);
- динамика письма (динамика рукописной подписи).

На рисунках А.3 и А.4 показаны различия между статической и динамической биометрической верификацией в интерфейсе карты в случае выполнения процессов биометрического сравнения и принятия решений на карте.

Рисунок А.3 — Пример процедуры статической биометрической верификации, использующей биометрическое сравнение на идентификационной карте

Рисунок А.4 — Пример процедуры динамической биометрической верификации, использующей биометрическое сравнение на идентификационной карте

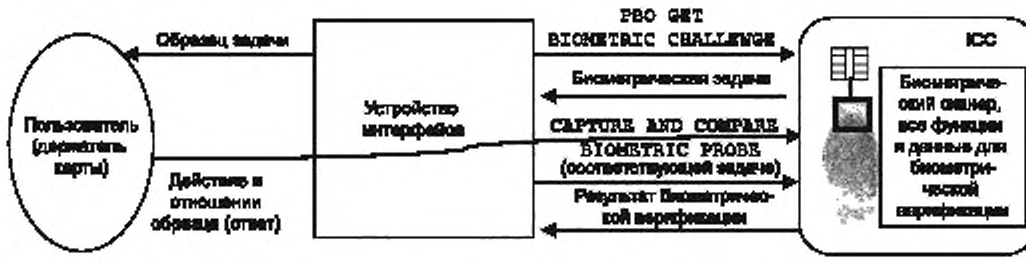

Рисунок А.5 — Пример процедуры динамической биометрической верификации, использующей сравнение на идентификационной карте

Приложение В
(справочное)

Примеры объектов данных биометрической информации

В настоящем приложении определены объекты данных биометрической информации, основанные на ЕСФОБД (см. формат ведущей организации, основанный на TLV, определенный в *ГОСТ Р 58294*).

До начала выполнения процесса верификации информация может быть извлечена из карты, предоставляющей детали, которые можно наблюдать с помощью внешних устройств при выполнении процесса биометрической верификации. В таблице В.1 показан пример шаблона группы шаблонов биометрической информации, который может включать несколько шаблонов биометрической информации. Один из шаблонов биометрической информации может содержать биометрическую информацию, представленную в формате ведущей организации, основанном на TLV (ЕСФОБД), определенном *в ГОСТ Р 58294*.

Таблица В.1 — Шаблон биометрической информации с вложенными ВНТ для биометрической пробы в стандартизованном и проприетарном форматах

Тег		L	Значение
Шаблон биометрической информации			
'7F60' (переменная длина)	'80'	1	Ссылка на алгоритм
	'83'	1	Квалификатор данных шаблона
	'A1'	Переменная	ВНТ (уровень 1)
	'A1'	Переменная	ВНТ (уровень 2)
	'87'	2	Владелец формата биометрической пробы, например идентификатор владельца формата ИСО/МЭК СТК 1/ПК 37 или *ТК 098*
	'88'	2	Тип формата биометрической пробы, определенный владельцем формата
	'A2'	Переменная	ВНТ (уровень 2)
	'87'	2	Владелец формата биометрической пробы, например изготовитель карты
	'88'	2	Тип формата биометрической пробы, определенный владельцем формата

Когда необходимо верифицировать несколько биометрических признаков (мультимодальная или комбинированная биометрия), например для того, чтобы получить доступ к конкретным данным или специальному ключу, применяют шаблон группы шаблонов биометрической информации с вложенными шаблонами биометрической информации, и верификация выполняется при передаче нескольких команд `VERIFY` или команд `PBO`. Пример приведен в таблице В.2. Атрибуты секретности (см. *ГОСТ Р ИСО/МЭК 7816-4*), связанные с соответствующим защищенным объектом, определяют, какая комбинация биометрических признаков должна быть успешно верифицируема.

Таблица В.2 — Шаблон группы шаблонов биометрической информации с вложенными шаблонами биометрической информации для приложений с несколькими биометрическими пробами, имеющими собственный квалификатор данных шаблона

Тег		L	Значение
Шаблон группы шаблонов биометрической информации			
'7F61' (переменная длина)	'02'	1	'02' — Число шаблонов биометрической информации
	'7F60'	Переменная	Шаблон биометрической информации 1
	'80'	1	Ссылка на алгоритм
	'83'	1	Квалификатор данных шаблона
	'A1'	Переменная	ВНТ
	'81'	1-3	Биометрический тип, например отпечаток пальца
	'82'	1	Биометрический подтип, например правый указательный палец
	'87'	2	Владелец формата биометрической пробы
	'88'	2	Тип формата биометрической пробы, определенный владельцем формата
	'7F60'	Переменная	Шаблон биометрической информации 2
	'80'	1	Ссылка на алгоритм
	'83'	1	Квалификатор данных шаблона
	'A1'	Переменная	ВНТ
	'81'	1-3	Биометрический тип, например отпечаток пальца
	'82'	1	Биометрический подтип, например левый указательный палец
	'87'	2	Владелец формата биометрической пробы
	'88'	2	Тип формата биометрической пробы, определенный владельцем формата

Приложение С
(справочное)

Перечень тегов объектов биометрических данных в шаблоне биометрической информации

В настоящем приложении приведен перечень тегов биометрических данных (см. таблицу С.1), определенных ЕСФОБД [см. формат ведущей организации, основанный на TLV, определенный в *ГОСТ Р 58294—2018 (ИСО/МЭК 19785-3:2015)*]. Эти теги применяют для использования детальной информации во время биометрической обработки в шаблоне биометрической информации, определенной в таблицах *6* и *7*.

Таблица С.1 — Перечень тегов объектов данных биометрической информации в шаблоне биометрической информации

Тег	Биометрический DO	Наличие
'53'/'73'	Биометрическая полезная нагрузка (простая/составная)	Необязательно
'80'	Ссылка на алгоритм биометрической верификации	Необязательно
'83'	Квалификатор данных шаблона	Необязательно
'A0'	RFU для DO биометрической информации, определенные в настоящем стандарте	Необязательно
'A1'	DO биометрической информации, определенные в другом документе	Обязательно, если 'A0' не присутствует
Использование исключительно в DO'A1'		
'78'	Совместимый орган распределения тегов	Обязательно, если 'A1' не присутствует
'70'	DO биометрической информации, определенные органом распределения тегов	Необязательно
Использование исключительно в DO'78'		
'06'	Идентификатор объекта (кодирование определено в *ГОСТ Р ИСО/МЭК 8825-1*)	Как правило, один из приведенных
'41'	Код страны (кодирование определено в *ГОСТ 7.67)* и дополнительные данные	
'42'	Идентификационный номер эмитента (кодирование и регистрация определены в *ГОСТ Р ИСО/МЭК 7816-1*), идентификатор приложения (AID, кодирование определено в *ГОСТ Р ИСО/МЭК 7816-4*)	
'4F'	Идентификатор приложения (AID, кодирование определено в *ГОСТ Р ИСО/МЭК 7816-4*)	
Использование исключительно в DO'70' (*см. ГОСТ Р 58294*)		
'80'	Версия заголовка ведущей организации	Обязательно (если отсутствует, применяется значение по умолчанию)
'81'	Биометрический тип	Необязательно
'82'	Биометрический подтип	Необязательно, используется только с биометрическим типом
'83'	Дата создания (YYYYMMDDHHMMSS)	Необязательно

Окончание таблицы С.1

Тег	Биометрический DO	Наличие
'84'	Создатель	Необязательно
'85'	Период действия (YYYYMMDDHHMMSS)	Необязательно
'86'	ID продукта (конкатенация владельца продукта и типа продукта, идентифицирующая продукт, который создал биометрический контрольный шаблон)	Необязательно
'87'	Владелец формата (владелец формата биометрических данных)	Обязательно, если 'A1' присутствует
'88'	Тип формата (тип формата биометрических данных, определенный владельцем формата)	Обязательно, если 'A1' присутствует
'90'	Индекс (уникальный идентификатор, используемый для ссылки на этот набор биометрических данных в контексте приложения вне идентификационной карты)	Необязательно
'91'/'B1'	Параметры алгоритма биометрического сравнения (простые/составные)	Необязательно

Приложение ДА
(справочное)

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

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование соответствующего международного стандарта
ГОСТ 7.67—2003 (ИСО 3166-1:1997)	MOD	ISO 3166-1:1997 «Коды для представления названий стран и единиц их административно-территориального деления. Часть 1. Коды стран»
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»
ГОСТ ISO/IEC 7812-1—2014	IDT	ISO/IEC 7812-1:2017 «Карты идентификационные. Идентификация эмитентов. Часть 1. Система нумерации»
ГОСТ Р ИСО/МЭК 7816-4—2013	IDT	ISO/IEC 7816-4:2013 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
ГОСТ Р ИСО/МЭК 7816-6—2013	IDT	ISO/IEC 7816-6:2013 «Карты идентификационные. Карты на интегральных схемах. Часть 6. Межотраслевые элементы данных для обмена»
ГОСТ Р ИСО/МЭК 8825-1—2003	IDT	ISO/IEC 8825-1 «Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования»
ГОСТ Р 58230—2018 (ИСО/МЭК 24787:2010)	MOD	ISO/IEC 24787:2010 «Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте»
ГОСТ Р 58294—2018 (ИСО/МЭК 19785-3:2015)	MOD	ISO/IEC 19785-3:2015 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 3. Спецификации формата ведущей организации»
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 ISO/IEC 7816-11.2017
—	6 Команды для определенных применений биометрической верификации и связанных с ней процессов
6 Элементы данных	7 Элементы данных
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в применяемом международном стандарте	
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	
Примечание — Сопоставление структуры стандартов приведено начиная с раздела 6, так как предыдущие разделы стандартов идентичны.	

Библиография

[1] ISO/IEC 7816-12, Identification cards - Integrated circuit cards — Part 12: Cards with contacts — USB electrical interface and operating procedures

[2] ISO/IEC 7816-5, Identification cards — Integrated circuit cards — Part 5: Registration of application providers

[3] ISO/IEC 7816-15, Identification cards — Integrated circuit cards — Part 15: Cryptographic information application

[4] ISO/IEC 17839-3, Information technology — Identification cards — Biometric System-on-Card — Part 3: Logical information interchange mechanism

УДК 004.93'1:006.89:006.354 ОКС 35.240.15

Ключевые слова: карты идентификационные, карты на интегральных схемах, биометрическая верификация, биометрия

БЗ 12—2019/112

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 28.11.2019. Подписано в печать 11.02.2020. Формат 60 × 84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 2,98.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru