ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58230.1— 2026 (ИСО/МЭК 24787-1:2024)

Информационные технологии

БИОМЕТРИЯ

Биометрическое сравнение на идентификационной карте

Часть 1

Общие требования

(ISO/IEC 24787-1:2024, Information technology — On-card biometric comparison — Part 1: General principles and specifications, MOD)

Издание официальное

Москва
Российский институт стандартизации
2026

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») 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

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 30 января 2026 г. № 63-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 24787-1:2024 «Информационные технологии. Биометрическое сравнение на идентификационной карте. Часть 1. Общие принципы и спецификации» (ISO/IEC 24787-1:2024 «Information technology — On-card biometric comparison — Part 1: General principles and specifications», MOD) путем изменения отдельных фраз (слов, значений, показателей, ссылок), которые выделены в тексте курсивом, а также путем исключения отдельных положений, обозначений, разделов 5 и 6, терминологических статей 3.6, 3.7, 3.8, 3.10, 3.11 и 3.16 и 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 межгосударственных 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 ВЗАМЕН ГОСТ Р 58230—2018 (ИСО/МЭК 24787:2010)

*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 (*gost.e-ecolog.ru

© ISO, 2024
© IEC, 2024
© Оформление. ФГБУ «Институт стандартизации», 2026

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 Обозначения и сокращения 3
5 Структура биометрического сравнения с использованием ICC 3
5.1 Общие положения 3
5.2 Биометрическое сравнение вне идентификационной карты 4
5.3 Биометрическое сравнение на идентификационной карте (считыватель вне идентификационной карты) 4
5.4 Биометрическое сравнение на идентификационной карте с распределением нагрузки 5
5.5 Биометрическое сравнение в системе на идентификационной карте 6
6 Общая структура приложений биометрического сравнения на идентификационной карте 7
6.1 Общие положения 7
6.2 Выбор приложения с использованием AID 7
6.3 Данные для биометрического сравнения на идентификационной карте 7
6.4 Процессы 13
6.5 Завершение *приложения биометрического сравнения на идентификационной карте* 14
7 Политика безопасности для биометрического сравнения на идентификационной карте 14
7.1 Минимальные требования политики безопасности 14
7.2 Политика безопасности для нескольких приложений биометрического сравнения на идентификационной карте 15
Приложение *A* (справочное) Примеры модели переходов статуса безопасности 18
Приложение *B* (справочное) Рекомендации для механизмов обеспечения безопасности при биометрическом сравнении на идентификационной карте 21
Приложение *C* (справочное) Пример шаблона биометрической информации, включающего элементы данных CBEFF-3 22
Приложение *D* (справочное) Пример реализации глобального биометрического контрольного шаблона 25
Приложение *E* (справочное) Типовой APDU для биометрического сравнения на идентификационной карте 30
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 33
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта 35

Введение

Биометрическое сравнение на идентификационной карте обеспечивает повышенную конфиденциальность и более высокую защиту данных при проведении процесса биометрического распознавания по сравнению с биометрическим сравнением без использования защищенного криптографического устройства. Данные биометрического контрольного шаблона, сохраненные на карте на интегральной схеме (ICC), недоступны для внешних интерфейсов, поэтому данные не могут быть скопированы и останутся конфиденциальными.

В *ГОСТ Р 58671* и *ГОСТ Р 58294* установлены требования к технологиям биометрического сравнения вне идентификационной карты и простого биометрического сравнения на идентификационной карте; в *ГОСТ Р ИСО/МЭК 17839-1, ГОСТ Р 58290 и ГОСТ Р 59885* — требования к технологиям биометрической системы на идентификационной карте.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Биометрическое сравнение на идентификационной карте

Часть 1

Общие требования

Information technology. Biometrics. On-card biometric comparison. Part 1. General requirements

Дата введения — 2026—06—01

1 Область применения

Настоящий стандарт устанавливает требования, общие принципы и спецификации методологии биометрического сравнения на идентификационной карте.

Настоящий стандарт устанавливает:

- требования к описанию структуры процесса биометрического сравнения на идентификационной карте;
- требования к процедуре биометрического сравнения на идентификационной карте для биометрических систем с устройством сбора данных вне идентификационной карты и для биометрических систем на идентификационной карте;
- принципы обеспечения безопасности при биометрическом сравнении на идентификационной карте.

Настоящий стандарт не устанавливает требования:

- к процедуре биометрического сравнения вне идентификационной карты;
- системе на идентификационной карте;
- биометрическому сравнению на идентификационной карте с механизмом распределения;
- хранению и процессу сравнения применительно к конкретным биометрическим модальностям.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

ГОСТ ISO/IEC 19794-1 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура

ГОСТ Р 58290 (*ИСО/МЭК 17839-2:2015*) *Информационные технологии. Биометрическая система на идентификационной карте. Часть 2. Физические характеристики*

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

ГОСТ Р 58295 (ИСО/МЭК 19794-6:2011) Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

ГОСТ Р 58298 (ИСО/МЭК 19794-4:2011) Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ГОСТ Р 58668.2 (ИСО/МЭК 39794-4:2019) Информационные технологии. Биометрия. Расширяемые форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца

ГОСТ Р 58668.3 (ИСО/МЭК 39794-5:2019) Информационные технологии. Биометрия. Расширяемые форматы обмена биометрическими данными. Часть 3. Данные изображения лица

ГОСТ Р 58668.4 (ИСО/МЭК 39794-6:2021) Информационные технологии. Биометрия. Расширяемые форматы обмена биометрическими данными. Часть 4. Данные изображения радужной оболочки глаза

Издание официальное

ГОСТ Р 58668.8 (ИСО/МЭК 19794-9:2011) Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения сосудистого русла

ГОСТ Р 58668.11 (ИСО/МЭК 19794-13:2018) Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Данные голоса

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

ГОСТ Р 59885 (*ИСО/МЭК 17839-3:2016*) *Информационные технологии. Биометрическая система на идентификационной карте. Часть 3. Механизм обмена логической информацией*

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

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

ГОСТ Р ИСО/МЭК 19794-2 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки

ГОСТ Р ИСО/МЭК 19794-3 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-5 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ГОСТ Р ИСО/МЭК 19794-7 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи

ГОСТ Р ИСО/МЭК 19794-8 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения отпечатка пальца — остов

ГОСТ Р ИСО/МЭК 19794-10 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки

ГОСТ Р ИСО/МЭК 19794-11 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи

ГОСТ Р ИСО/МЭК 19794-14 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК

ГОСТ Р ИСО/МЭК 29794-1 Информационные технологии. Биометрия. Качество биометрического образца. Часть 1. Структура

ГОСТ Р ИСО/МЭК 29794-6 Информационные технологии. Биометрия. Качество биометрического образца. Часть 6. Данные изображения радужной оболочки глаза

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 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 и ГОСТ Р 58671*, а также следующие термины с соответствующими определениями:

3.1 **действие** (action): Операция, предпринятая в соответствии с результатами принятия решения биометрической системой.

Примечания

1 В контексте биометрического сравнения на идентификационной карте действие представляет собой изменение статуса безопасности

2 Настоящий стандарт не определяет действия, основанные на результате биометрического сравнения на идентификационной карте.

3.2 **биометрические вспомогательные данные** (biometric auxiliary data): Данные, зависящие от особенностей биометрической модальности и связанные с биометрическим контрольным шаблоном, но не содержащие биометрический контрольный шаблон или биометрический образец.

Примечание — Вспомогательными данными являются такие данные, как ориентация, масштабирование и т. п.

3.3 **параметры биометрического сравнения** (biometric comparison parameters): Параметры, специфичные для приложения и необходимые для выполнения биометрического сравнения с соответствующим биометрическим контрольным шаблоном.

3.4 **информация о биометрической функциональности** (biometric functionality information): Информация о возможностях биометрического сравнения на идентификационной карте, предоставляемая операционной системой карты на интегральной схеме.

3.5 **биометрический информационный шаблон** (biometric information template): Информация, содержащая описание связанных биометрических данных.

3.6 **решение** (decision): Результат сравнения степени схожести с установленным значением порога с целью классификации биометрического заявления как подлинного владельца идентификационной карты или как самозванца.

3.7 **распределение нагрузки** (work-sharing): Разделение вычислительной нагрузки процесса сравнения между ICC и биометрическим устройством сопряжения (IFD).

4 Обозначения и сокращения

В настоящем стандарте применены следующие обозначения и сокращения:

ВЛС — вероятность ложного совпадения (false match rate, FMR);

ПИН — персональный идентификационный номер (personal identification number, PIN);

AID — идентификатор приложения (application identifier);

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

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

BER — базовые правила кодирования (basic encoding rules);

BHT — биометрический шаблон заголовка (biometric header template);

BIDO — объект данных биометрической информации (biometric information data object);

CBEFF-3 — структура общих форматов обмена биометрическими данными. Часть 3. Спецификации формата клиента (Common biometric exchange formats framework. Part 3. Patron format specifications);

CRT — шаблон управляющих ссылок (*control reference template*);

DF — назначенный файл (dedicated file);

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

EF — элементарный файл (elementary file);

FCI — контрольная информация файла (file control information);

MAC — код аутентификации сообщения (message authentication code);

MF — главный файл (master file);

OID — идентификатор объекта (object identifier);

PBO — ВЫПОЛНИТЬ БИОМЕТРИЧЕСКУЮ ОПЕРАЦИЮ (PERFORM BIOMETRIC OPERATION);

RFU — зарезервированы для будущего использования (reserved for future use);

SEID — идентификатор безопасной среды (*security environment identifier*);

SW1, SW2 — байты состояния (status bytes);

TLV — значение длины тега (tag length value);

Var — переменная (variable).

5 Структура биометрического сравнения с использованием ICC

*5.*1 Общие положения

В следующих подразделах подробно описаны четыре структуры биометрического сравнения с использованием ICC и ICC с системой биометрической верификации. Положения *5.*3 входят в раздел 1.

Информация, представленная в *5.*2, предназначена для пояснения взаимосвязи между методами биометрического сравнения на идентификационной карте, рассматриваемыми в настоящем стандарте, и методами биометрического сравнения вне идентификационной карты, выходящими за рамки настоящего стандарта.

Биометрический контрольный шаблон хранится в ICC до выполнения биометрического сравнения.

Биометрическая верификация может сосуществовать с другими механизмами аутентификации, такими как ПИН, в соответствии с положениями *ГОСТ Р ИСО/МЭК 7816-4*.

5.2 Биометрическое сравнение вне идентификационной карты

Биометрическое сравнение вне идентификационной карты означает, что процесс биометрической верификации протекает в системе биометрической верификации. ICC в данном случае выступает в роли хранилища для биометрического контрольного шаблона *(или нескольких биометрических контрольных шаблонов)* пользователя. Схема процесса представлена на рисунке 1.

Для выполнения попытки биометрической верификации система биометрической верификации должна получить доступ к ICC и считать данные биометрического контрольного шаблона *пользователя. Система биометрической верификации в данном случае предназначена для регистрации биометрического образца и выполнения биометрической верификации.* При положительном результате биометрической верификации система биометрической верификации изменит свой статус безопасности. *Этот процесс может включать считывание дополнительной информации с ICC для последующих транзакций. В случае отрицательного результата дальнейший доступ будет запрещен.*

Пример — Рассмотрим систему контроля доступа, в которой биометрический контрольный шаблон и код доступа хранятся на ICC. Система биометрической верификации считывает биометрический контрольный шаблон с идентификационной карты и выполняет биометрическую верификацию. В случае положительного результата биометрической верификации система считывает код доступа с идентификационной карты и передает его серверной системе, которая открывает дверь.

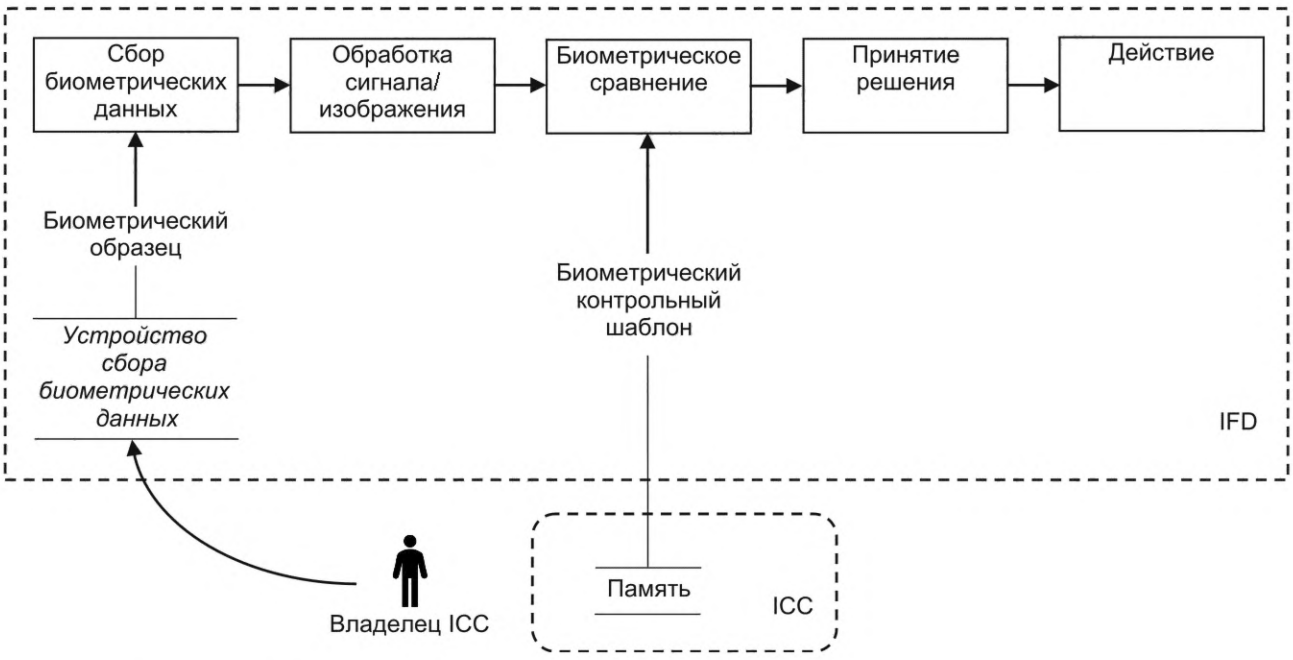

Рисунок 1 — Общая архитектура биометрического сравнения вне идентификационной карты

5.3 Биометрическое сравнение на идентификационной карте (считыватель вне идентификационной карты)

Биометрическое сравнение на идентификационной карте означает, что верификация биометрического образца проходит на ICC, на которой хранятся данные биометрического контрольного шаблона.

Процессор ICC должен иметь достаточную вычислительную мощность для выполнения сравнения. Схема процесса представлена на рисунке 2. Считыватель расположен на IFD за пределами ICC, поэтому сбор биометрических данных происходит вне ICC. Процесс биометрической регистрации совпадает или аналогичен процессу биометрической регистрации при биометрическом сравнении вне идентификационной карты.

Для защиты процесса обмена данными между системой биометрической верификации и ICC рекомендуется использовать *проверенный* защищенный канал (с использованием безопасного обмена сообщениями в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*).

Примечание — В приложении *А* приведены примеры реализации сравнения биометрических данных на идентификационной карте с соответствующими переходами статуса безопасности ICC. Реализация механизма обеспечения безопасности при сравнении биометрических данных на идентификационной карте представлена в приложении *В*.

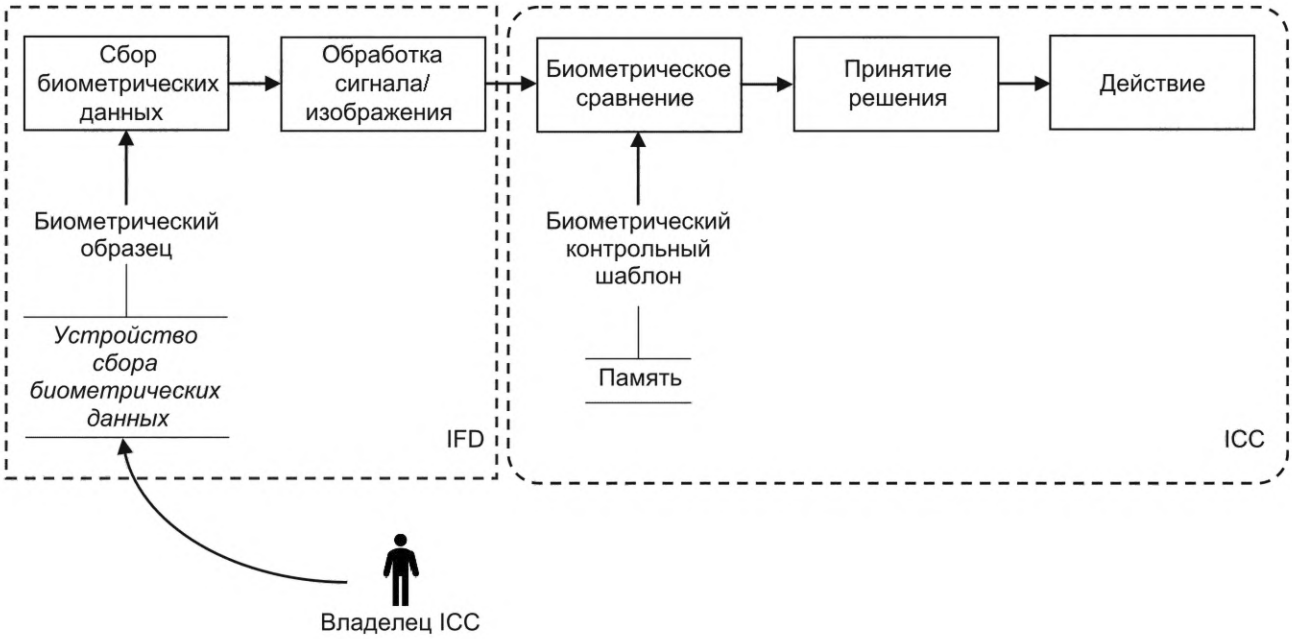

Рисунок 2 — Общая архитектура биометрического сравнения на идентификационной карте (считыватель вне идентификационной карты)

5.4 Биометрическое сравнение на идентификационной карте с распределением нагрузки

Биометрическое сравнение на идентификационной карте с распределением нагрузки аналогично биометрическому сравнению на идентификационной карте, за исключением процедуры сравнения, которая сопровождается внешней обработкой. Данный способ сравнения предназначен для использования с ICC, которые не обладают достаточными вычислительными возможностями для выполнения сравнения биометрических данных.

Процесс биометрического сравнения *на ICC с распределением нагрузки* разделен на несколько подпроцессов, которые выполняются на IFD и ICC. На рисунке 3 показан пример этого процесса с одной итерацией обратной связи. Биометрические вспомогательные данные хранятся на одной части ICC, а биометрический контрольный шаблон — на ее другой части. Биометрические вспомогательные данные, в отличие от биометрического контрольного шаблона, могут быть извлечены из ICC. Биометрические вспомогательные данные предоставляют для ускорения процесса биометрического сравнения.

Общая процедура биометрического сравнения на идентификационной карте с распределением нагрузки выглядит следующим образом:

- перед началом процедуры биометрического сравнения система биометрической верификации на IFD собирает биометрический образец держателя карты;
- перед процедурой биометрического сравнения из ICC могут быть получены вспомогательные биометрические данные;
- система биометрической верификации на IFD запускает первый процесс процедуры биометрического сравнения, а затем последовательно запускает выполнение следующих процессов:
  1) когда обработка происходит на ICC, она может использовать биометрический контрольный шаблон при необходимости,
  2) когда обработка происходит на IFD, ICC может передавать информацию предыдущего процесса биометрического сравнения в IFD в качестве входных данных;

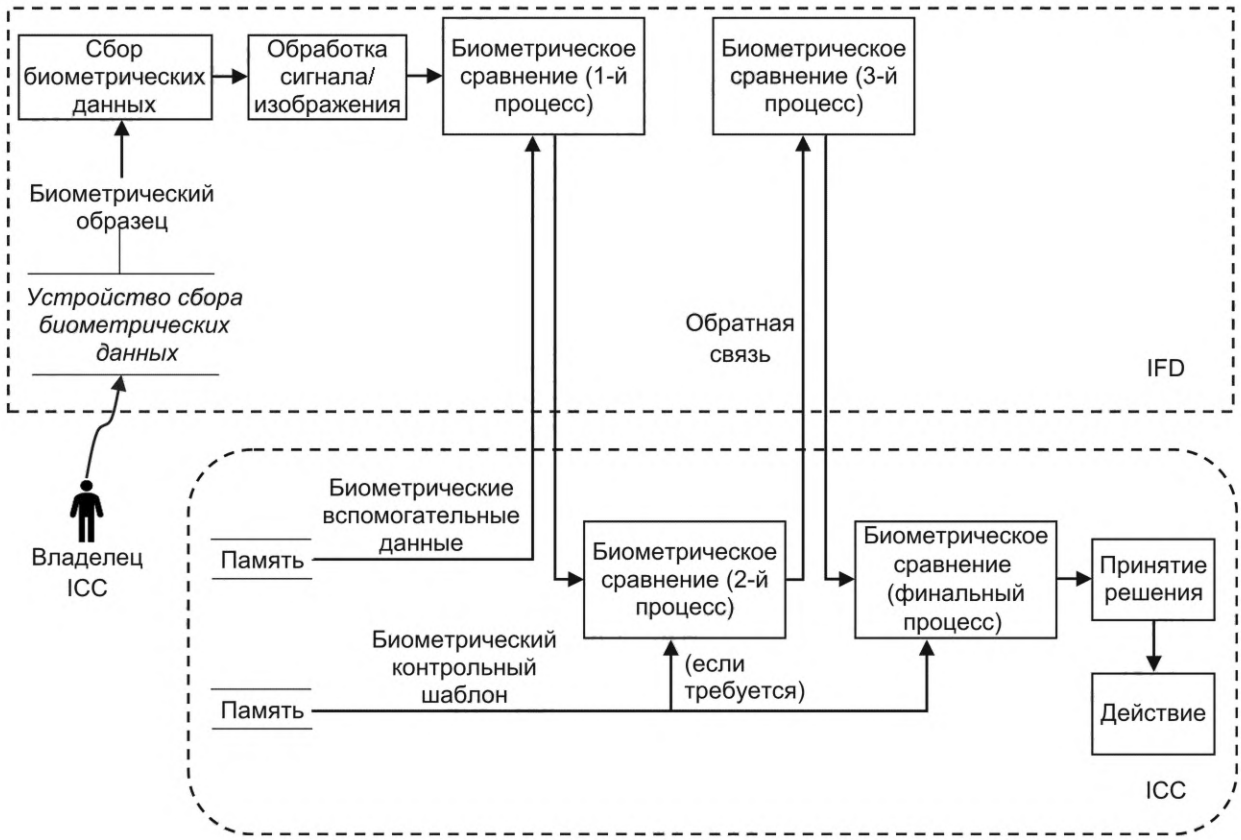

Рисунок 3 — Пример архитектуры биометрического сравнения на идентификационной карте с распределением нагрузки

- заключительный процесс процедуры биометрического сравнения выполняют на ICC;
- после завершения заключительного процесса процедуры биометрического сравнения следуют процедуры принятия решения и выполнения соответствующего действия.

Дополнительные сведения о вспомогательных биометрических данных зависят от биометрической модальности и не рассмотрены в настоящем стандарте.

5.5 Биометрическое сравнение в системе на идентификационной карте

Биометрическое сравнение в системе на идентификационной карте включает весь процесс верификации биометрического образца, выполняемый на ICC. Схема процесса представлена на рисунке 4.

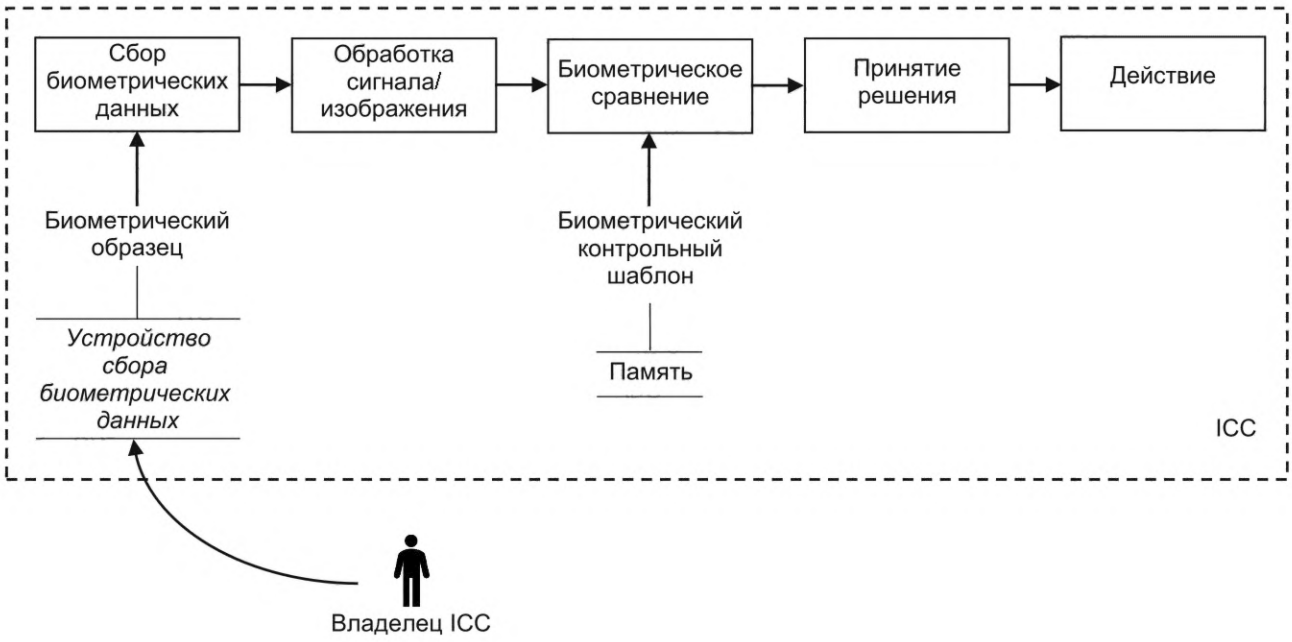

Рисунок 4 — Общая архитектура биометрического сравнения в системе на идентификационной карте

6 Общая структура приложений биометрического сравнения на идентификационной карте

6.1 Общие положения

Требования настоящего подраздела применяют к биометрическому сравнению на идентификационной карте (считыватель вне карты) (см. *5*.3), биометрическому сравнению на идентификационной карте с распределением нагрузки (см. *5*.4) и биометрическому сравнению в системе на идентификационной карте (см. *5*.5).

6.2 Выбор приложения с использованием AID

Биометрическое сравнение на идентификационной карте может быть реализовано как самостоятельное приложение. В таком случае это приложение должно быть идентифицировано с помощью AID в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*. Приложение биометрического сравнения на идентификационной карте может быть выбрано при помощи AID с использованием идентификатора объекта '28 81 C1 53 01' (т. е. 'E8 28 81 C1 53 01' + специфичное для приложения расширение AID).

Примечание — Расширение AID для конкретного приложения — RFU.

6.3 Данные для биометрического сравнения на идентификационной карте

6.3.1 Общие положения

В настоящем стандарте определены объекты данных для конфигурации биометрической верификации (т. е. информация о биометрической функциональности и параметры биометрического сравнения), которые могут быть встроены в шаблон биометрической информации, определенный в *ГОСТ Р 58671*.

Существует два типа кодирования данных, а именно: явное и неявное кодирования распределения тегов. В настоящем стандарте использовано явное кодирование распределения тегов. DO'A1' следует использовать для объектов данных, определенных в *ГОСТ Р 58294*, а DO'A2' — для BIDO, связанных с биометрическим сравнением на идентификационной карте. В таблице *1* определен шаблон биометрической информации с использованием спецификации кодирования явного распределения тегов с включением DO, определенных в настоящем стандарте и в *ГОСТ Р 58294*. В настоящем стандарте тег 'A0' в '7F60' не рассмотрен, поэтому использование тегов 'A1' и 'A2' обязательно.

Пример шаблона биометрической информации, который включает элементы данных, определенные в *ГОСТ Р 58294* в BHT в теге 'A1', приведен в приложении *С*.

Подробная информация о кодировании распределения тегов приведена в *ГОСТ Р 58671* и *ГОСТ Р 58294*.

Таблица *1* — Шаблон биометрической информации с DO, определенными для биометрического сравнения на идентификационной карте

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="6">Значение</th><th rowspan="2">Наличие</th></tr>
<tr><td rowspan="18">'7F60'</td><td rowspan="18">Var</td><td colspan="6">Шаблон биометрической информации по ГОСТ Р 58671</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="4">Значение</td></tr>
<tr><td>'80'</td><td rowspan="2">1</td><td colspan="4">Ссылка на алгоритм для использования в команде VERIFY / EXT. AUTHENTICATE / MANAGE SE по ГОСТ Р ИСО/МЭК 7816-4</td><td rowspan="2">Опционально</td></tr>
<tr><td>'83'</td><td colspan="4">Ссылка на квалификатор данных для использования в команде VERIFY / EXT. AUTHENTICATE / MANAGE SE по ГОСТ Р ИСО/МЭК 7816-4</td></tr>
<tr><td>'A1'</td><td rowspan="16">Var</td><td colspan="4">BIDO, не указанные в ГОСТ Р 58671. В настоящем стандарте данный DO зарезервирован для BIDO для CBEFF-3 по ГОСТ Р 58294</td><td>Обязательно при наличии DO по ГОСТ Р 58294</td></tr>
<tr><td rowspan="14">'A2'</td><td colspan="4">BIDO, не указанные в ГОСТ Р 58671. В настоящем стандарте данный DO зарезервирован для BIDO, указанных в настоящем стандарте</td><td>Обязательно</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="3">Значение</td><td>Наличие</td></tr>
<tr><td rowspan="3">'78'</td><td rowspan="3">9</td><td colspan="3">Совместимый орган распределения тегов</td><td>Обязательно</td></tr>
<tr><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td>'06'</td><td>7</td><td>'28 81 C1 53 01 8F 68'</td><td>Обязательно. OID настоящего стандарта</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="3">Значение</td><td>Наличие</td></tr>
<tr><td rowspan="4">'70'</td><td rowspan="4">Var</td><td colspan="3">BIDO, указанные в настоящем стандарте</td><td>Обязательно</td></tr>
<tr><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td>'91' или 'B1'</td><td>Var</td><td>Параметры биометрического сравнения, указанные в таблице 3</td><td>По крайней мере один DO</td></tr>
<tr><td>'92' или 'B2'</td><td>Var</td><td>Информация о биометрической функциональности, приведенная в таблице 2</td><td>По крайней мере один DO</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="4">Значение</td><td>Наличие</td></tr>
<tr><td>'5F2E' или '7F2E'</td><td>Var</td><td colspan="4">Биометрические данные (первичные/созданные)</td><td>Обязательно, если биометрические данные хранятся в DO'7F60'</td></tr>
</table>

6.3.2 Формат биометрических данных

С целью обеспечения совместимости данных биометрического контрольного шаблона для отправки биометрических данных в ICC необходимо использовать биометрические данные в формате, определенном в *ГОСТ Р 58671*.

Если биометрические данные хранятся в шаблоне биометрической информации DO'7F60', следует использовать DO'5F2E' или DO'7F2E'.

Рекомендуется использовать компактные форматы карт, описанные в *ГОСТ ISO/IEC 19794-1*, *ГОСТ Р 58295*, *ГОСТ Р 58298*, а также в *ГОСТ Р ИСО/МЭК 19794-2, ГОСТ Р ИСО/МЭК 19794-3, ГОСТ Р ИСО/МЭК 19794-5, ГОСТ Р ИСО/МЭК 19794-7, ГОСТ Р ИСО/МЭК 19794-8*, *ГОСТ Р ИСО/МЭК 19794-10*, *ГОСТ Р ИСО/МЭК 19794-11*, *ГОСТ Р ИСО/МЭК 19794-14, ГОСТ Р 58668.2*, *ГОСТ Р 58668.3*, *ГОСТ Р 58668.4*, *ГОСТ Р 58668.8*, *ГОСТ Р 58668.11*.

Возможны случаи, когда биометрические данные (первичные/созданные) исключены из шаблона биометрической информации: например, когда биометрический контрольный шаблон используется несколькими приложениями (см. *6*.3.4) или когда он не может быть извлечен из ICC с механизмом биометрического сравнения на идентификационной карте в связи с действием политики безопасности (см. *7*.2.1).

6.3.3 Специальные объекты данных

6.3.3.1 Общие положения

Параметры биометрического сравнения и информация о биометрической функциональности могут быть представлены в формате объекта данных TLV или в наборе элементов данных не в формате объекта данных TLV.

В формате объекта данных TLV эти данные инкапсулируются в DO'B1' и DO'B2' соответственно, под DO'70' в пределах BIDO DO'A2', включенных в шаблон биометрической информации DO'7F60'.

В наборе элементов данных не в формате объекта данных TLV они инкапсулируются в DO'91' и DO'92' соответственно, под DO'70' в пределах BIDO DO'A2', включенных в шаблон биометрической информации DO'7F60'.

6.3.3.2 Информация о биометрической функциональности

Информация о предельных значениях для биометрической функциональности каждой модальности приведена в DO'92' или DO'B2' шаблона биометрической информации (см. таблицу *1*). Элементы данных, хранящиеся в DO'B2', определены в таблице *2*.

Информация о биометрической функциональности может быть считана из ICC, но не может быть изменена во время рабочего состояния ICC. Извлечение информации о биометрической функциональности может быть подвергнуто связанным атрибутам секретности.

При наличии поддержки нескольких биометрических модальностей в ICC может быть указана информация о биометрической функциональности для каждой биометрической модальности.

Информация о возможности повторной биометрической регистрации приведена в DO'83'. В соответствии со значением DO'83' ICC контролирует повторную биометрическую регистрацию соответствующей биометрической модальности.

6.3.3.3 Параметры биометрического сравнения

В отличие от информации о биометрической функциональности, которая зависит только от биометрической модальности, параметры биометрического сравнения зависят как от биометрической модальности, так и от приложения. Параметры биометрического сравнения хранятся в шаблоне биометрической информации, который принадлежит приложению биометрического сравнения на идентификационной карте. Шаблон биометрической информации может быть связан с фактическими биометрическими данными. Параметры биометрического сравнения могут быть изменены во время биометрической регистрации. Если биометрический контрольный шаблон, хранящийся на ICC, доступен для использования несколькими приложениями, каждое приложение может иметь общий набор параметров биометрического сравнения в MF (см. *6*.3.4) или собственный набор параметров биометрического сравнения (если параметры различные). Пример приведен в приложении *D*.

В таблицах *3* и *4* представлены параметры биометрического сравнения, хранящиеся в шаблоне биометрической информации, для выполнения биометрического сравнения на идентификационной карте (тег '91' или 'B1' в DO'70', который находится в DO'A2').

Если шаблон биометрической информации содержит какие-либо параметры биометрического сравнения, он должен включать параметр минимального поддерживаемого качества данных биометрической верификации для выполнения сравнения (т. е. DO'85' в таблице *3*, если параметры указаны в DO'B1').

Таблица 2 — Объекты данных для элементов информации о функциональности биометрической модальности

Тег	Длина	Значение	Наличие
'80'	1—3	Максимальная длина данных биометрической пробы*	Опционально
'81'		Максимальная длина данных биометрического контрольного шаблона*	
'82'	1	Поддерживаемое число биометрических образцов: '00': информация отсутствует	
'83'		Возможность повторной биометрической регистрации: '00': повторная регистрация невозможна; '01': повторная регистрация возможна. Другие значения: RFU	
'85'	Var	Минимальное поддерживаемое качество данных биометрической верификации в соответствии с требованиями, определенными в *ГОСТ ISO/IEC 19794-1*, *ГОСТ Р 58295*, *ГОСТ Р 58298*, *ГОСТ Р 58668.8*, *ГОСТ Р 58668.11*, а также в *ГОСТ Р ИСО/МЭК 19794-2*, *ГОСТ Р ИСО/МЭК 19794-3*, *ГОСТ Р ИСО/МЭК 19794-5*, *ГОСТ Р ИСО/МЭК 19794-7*, *ГОСТ Р ИСО/МЭК 19794-8*, *ГОСТ Р ИСО/МЭК 19794-10*, *ГОСТ Р ИСО/МЭК 19794-11*, *ГОСТ Р ИСО/МЭК 19794-14*, *ГОСТ Р ИСО/МЭК 29794-1*, *ГОСТ Р ИСО/МЭК 29794-6*	
'87'		Минимальные требования к качеству биометрической пробы для выполнения сравнения (например, минимальное требуемое число контрольных точек отпечатков пальцев)	
'8F'		Проприетарные данные	
'90'		Тип биометрической верификации и дискриминационная способность (градация ВЛС) приведены в таблице *4*	Обязательно, если применима SP2 (см. *7*.2.3). Опционально в остальных случаях

* Каждая модальность может иметь собственное определение длины биометрической пробы и контрольного биометрического шаблона. Например, длина для модальности отпечатка пальца может указывать минимальное число контрольных точек, а для модальности лица — число байтов.

Примечание — Некоторые или все DO, указанные в настоящей таблице, могут стать обязательными, если того требует определенный профиль приложения.

Таблица 3 — Объекты данных для параметров биометрического сравнения

Тег	Длина	Значение	Наличие
'81'*	1—3	Минимальная и максимальная длина биометрической пробы***. Это значение должно быть совместимо со значением, определенным в теге '80' DO'B2' (см. *6*.3.3.2)	Опционально
'82'*	1	Упорядочивание последовательности, если применимо, биометрических признаков в биометрических данных	
'83'*		Индикатор обработки признака	
'84'*	Var	Информация об ориентации	
'85'**	Var	Минимальное поддерживаемое качество данных биометрической верификации в соответствии с требованиями, определенными в *ГОСТ ISO/IEC 19794-1*, *ГОСТ Р 58295*, *ГОСТ Р 58298*, *ГОСТ Р 58668.8*, *ГОСТ Р 58668.11*, а также в *ГОСТ Р ИСО/МЭК 19794-2*, *ГОСТ Р ИСО/МЭК 19794-3*, *ГОСТ Р ИСО/МЭК 19794-5*, *ГОСТ Р ИСО/МЭК 19794-7*, *ГОСТ Р ИСО/МЭК 19794-8*, *ГОСТ Р ИСО/МЭК 19794-10*, *ГОСТ Р ИСО/МЭК 19794-11*, *ГОСТ Р ИСО/МЭК 19794-14*, *ГОСТ Р ИСО/МЭК 29794-1*, *ГОСТ Р ИСО/МЭК 29794-6*. Это значение должно быть совместимо со значением, определенным в теге '85' DO'B2' (см. *6*.3.3.2)	Обязательно

Окончание таблицы 3

Тег	Длина	Значение	Наличие
'90'	1	Тип биометрической верификации и дискриминационная способность. Это значение должно быть совместимо со значением, определенным в теге '90' DO'B2' (см. *6*.3.3.2)	Обязательно, если применима SP2 (см. *7*.2.3). Опционально в остальных случаях
'91'	2	Оценка ICC максимального времени ответа (мс), которая будет предоставлена IFD '0001' — 'FFFF'	Опционально

* Значение данной переменной определено в *ГОСТ ISO/IEC 19794-1*, *ГОСТ Р 58295*, *ГОСТ Р 58298*, *ГОСТ Р 58668.8*, *ГОСТ Р 58668.11*, а также в *ГОСТ Р ИСО/МЭК 19794-2*, *ГОСТ Р ИСО/МЭК 19794-3*, *ГОСТ Р ИСО/МЭК 19794-5*, *ГОСТ Р ИСО/МЭК 19794-7*, *ГОСТ Р ИСО/МЭК 19794-8*, *ГОСТ Р ИСО/МЭК 19794-10*, *ГОСТ Р ИСО/МЭК 19794-11*, *ГОСТ Р ИСО/МЭК 19794-14*.

** Значение данной переменной определено в *ГОСТ ISO/IEC 19794-1*, *ГОСТ Р 58295*, *ГОСТ Р 58298*, *ГОСТ Р 58668.8*, *ГОСТ Р 58668.11*, а также в *ГОСТ Р ИСО/МЭК 19794-2*, *ГОСТ Р ИСО/МЭК 19794-3*, *ГОСТ Р ИСО/МЭК 19794-5*, *ГОСТ Р ИСО/МЭК 19794-7*, *ГОСТ Р ИСО/МЭК 19794-8*, *ГОСТ Р ИСО/МЭК 19794-10*, *ГОСТ Р ИСО/МЭК 19794-11*, *ГОСТ Р ИСО/МЭК 19794-14*, *ГОСТ Р ИСО/МЭК 29794-1*, *ГОСТ Р ИСО/МЭК 29794-6*.

*** Каждая модальность может иметь собственное определение длины биометрической пробы и контрольного биометрического шаблона. Например, длина для модальности отпечатка пальца может указывать минимальное число контрольных точек, а для модальности лица — число байтов.

Примечание — Некоторые или все DO, указанные в настоящей таблице, могут стать обязательными, если того требует определенный профиль приложения.

Таблица *4* — Тип биометрической верификации и дискриминационная способность (уровни ВЛС)

b8	b7	b6	b5	b4	b3	b2	b1	Значение
—	—	—	—	—	—	x	x	Тип биометрической верификации
—	—	—	—	—	—	0	0	Биометрическое сравнение на идентификационной карте
—	—	—	—	—	—	0	1	Биометрическое сравнение на идентификационной карте с распределением нагрузки
—	—	—	—	—	—	1	0	Система на идентификационной карте
—	—	—	—	—	—	1	1	RFU
—	—	—	x	x	x	—	—	Требуемое значение ВЛС*
—	—	—	0	0	0	—	—	Индикатор отсутствует
—	—	—	0	0	1	—	—	ВЛС уровня 1 (наибольшая)
—	—	—	0	1	0	—	—	ВЛС уровня 2
—	—	—	0	1	1	—	—	ВЛС уровня 3
—	—	—	1	0	0	—	—	ВЛС уровня 4
—	—	—	1	0	1	—	—	ВЛС уровня 5
—	—	—	1	1	0	—	—	ВЛС уровня 6 (наименьшая)
—	—	—	1	1	1	—	—	RFU
x	x	x	—	—	—	—	—	RFU

* Данный параметр позволяет создателю системы устанавливать различные уровни сравнения для различных приложений с конкретными продуктами, использующими биометрическое сравнение на идентификационной карте.

В таблице 5 приведена шкала градации ВЛС.

Таблица 5 — Градация ВЛС

Уровень ВЛС	*Значение* ВЛС
1	≤0,1
2	≤0,01
3	≤0,001
4	≤0,0001
5	≤0,00001
6	≤0,000001

Если значение ВЛС выше уровня 1, в поле «Уровень ВЛС» указывают значение «Индикатор отсутствует».

6.3.4 Использование биометрических данных несколькими приложениями

6.3.4.1 Общие положения

Когда на одной ICC хранится несколько приложений биометрического сравнения на идентификационной карте, политика управления данными, связанная с биометрическим сравнением, может быть разработана с учетом местоположения хранилища данных и настроек контроля доступа к нему.

Примечание — Информация, приведенная в 6.3.4.2—6.4.3.3, относится к приложению(ям) биометрического сравнения. Информация, приведенная в 6.3.4.4, также касается тех случаев, когда для биометрического сравнения используют одно общее приложение, которое применяет общий биометрический контрольный шаблон и общие параметры биометрического сравнения.

6.3.4.2 Несколько независимых приложений биометрического сравнения

В том случае, если каждое приложение биометрического сравнения на идентификационной карте использует собственный биометрический контрольный шаблон, то этот шаблон может храниться независимо в DF, связанном с конкретным приложением биометрического сравнения на идентификационной карте (т. е. DF приложения). Этот DF также хранит шаблон биометрической информации для предоставления параметров биометрического сравнения, как показано на рисунке 5. SP3 определяет требования к реализации безопасности.

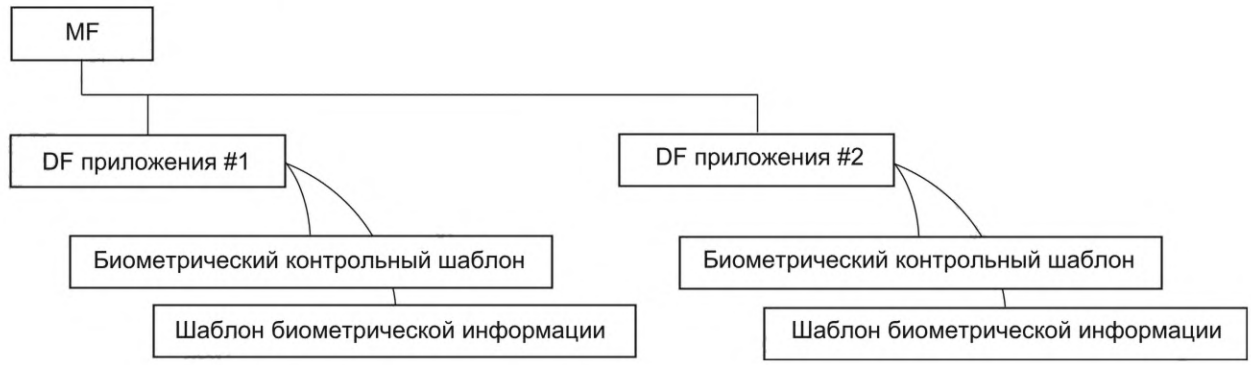

Рисунок 5 — Управление специфичными для приложений биометрическими контрольными шаблонами

6.3.4.3 Глобальный биометрический контрольный шаблон со специфичными для приложений параметрами биометрического сравнения

В том случае, когда несколько приложений для биометрического сравнения на идентификационной карте совместно используют один биометрический контрольный шаблон, то он может храниться в MF как глобальный биометрический контрольный шаблон, как показано на рисунке 6. Если каждое из приложений управляет своими параметрами биометрического сравнения независимо, каждый DF приложения хранит собственный шаблон биометрической информации для предоставления независимых параметров биометрического сравнения. Этот шаблон биометрической информации также может предоставлять информацию (например, ссылку, местоположение или квалификатор) относительно биометрического контрольного шаблона.

SP2 определяет требования к реализации безопасности.

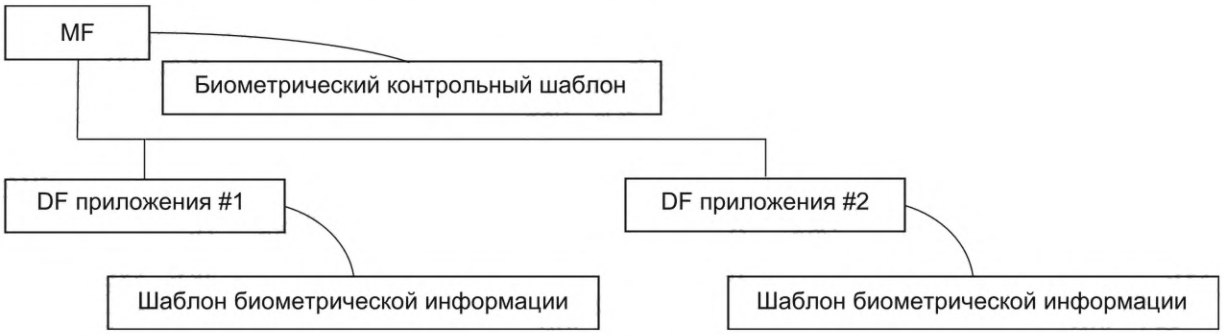

Рисунок 6 — Управление глобальным биометрическим контрольным шаблоном со специфичными для приложений параметрами биометрического сравнения

6.3.4.4 Глобальный биометрический контрольный шаблон с общими параметрами биометрического сравнения для нескольких приложений

В том случае, когда несколько приложений биометрического сравнения на идентификационной карте совместно используют общий биометрический контрольный шаблон (т. е. глобальный биометрический контрольный шаблон) и общий набор параметров биометрического сравнения (т. е. глобальные параметры), то биометрический контрольный шаблон и шаблон биометрической информации для предоставления параметров биометрического сравнения хранятся в MF. Для обеспечения доступа IFD к необходимым элементам данных для биометрического сравнения каждый DF может хранить собственный шаблон биометрической информации, который предоставляет информацию (например, ссылку, местоположение или квалификатор) относительно фактических элементов данных, хранящихся в MF, как показано на рисунке 7.

SP1 определяет требования к реализации безопасности.

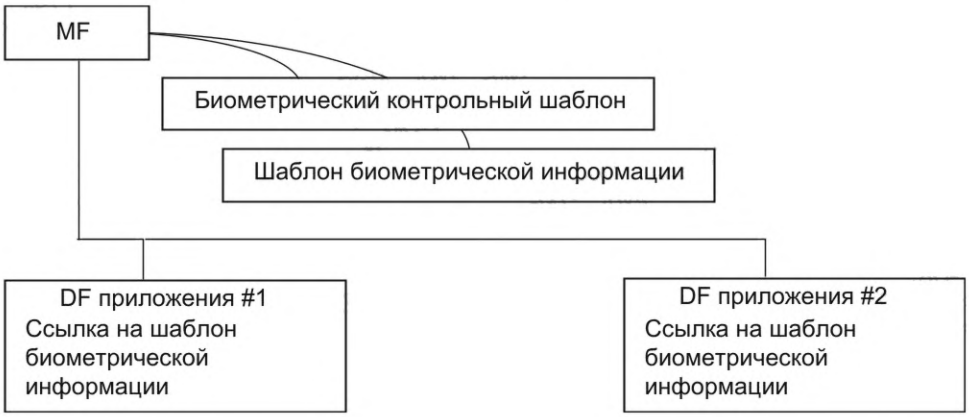

Рисунок 7 — Управление глобальным биометрическим контрольным шаблоном с общими параметрами биометрического сравнения

6.4 Процессы

6.4.1 Первичная и повторная биометрическая регистрация

Биометрическая регистрация (первичная и повторная) представляет собой процесс, посредством которого создают и сохраняют биометрический контрольный шаблон. Механизм биометрической регистрации должен соответствовать требованиям *ГОСТ 58671*. Механизм повторной биометрической регистрации может быть реализован согласно требованиям конкретной системы.

В зависимости от возможностей ICC обработка изображения/сигнала может быть распределена между IFD и ICC. Во всех случаях все биометрические данные передают на ICC с использованием доверенного защищенного канала или доверенной среды, гарантирующих конфиденциальность владельца ICC. Рекомендуется выполнять тестовую попытку биометрической верификации после (повторной) биометрической регистрации для проверки качества зарегистрированных биометрических данных.

Порядок записи зарегистрированных биометрических данных на ICC определен в *ГОСТ Р 58671*.

6.4.2 Биометрическая верификация

Механизм биометрической верификации должен быть реализован в соответствии с требованиями *ГОСТ Р 58671*.

В процессе биометрической верификации участвуют следующие параметры биометрического сравнения:

- минимальное качество данных биометрической верификации;
- тип биометрической верификации и дискриминационная способность (при наличии).

В результате биометрической верификации может быть установлен статус безопасности (биометрическая верификация завершена или не завершена). Процесс биометрической верификации состоит из процессов биометрического сравнения и принятия решения с использованием параметров биометрического сравнения. Перед началом процесса биометрической верификации параметры биометрического сравнения устанавливаются в соответствии с уровнем безопасности для конкретного приложения. Пример APDU биометрического сравнения на идентификационной карте для случая биометрической верификации по отпечаткам пальцев представлен в приложении *E*.

6.4.3 Процесс биометрического сравнения и принятие решения

6.4.3.1 Процесс биометрического сравнения

В случае биометрического сравнения на идентификационной карте с распределением нагрузки, по крайней мере, окончательный процесс биометрического сравнения проходит на ICC. Процесс биометрического сравнения на идентификационной карте без распределения нагрузки полностью осуществляется на ICC.

6.4.3.2 Принятие решения

Решение биометрической верификации представляет собой результат сравнения степени схожести представленных биометрических данных и заданного порога для достижения требуемого уровня безопасности. Если степень схожести равна или превышает заданный порог, биометрическая верификация завершена.

6.5 Завершение *приложения биометрического сравнения на идентификационной карте*

При завершении приложения биометрического сравнения на идентификационной карте (если такой процесс поддерживается) биометрический контрольный шаблон, относящийся только к данному приложению, должен стать недоступным. Возможный способ решения — это «обнуление» данных.

7 Политика безопасности для биометрического сравнения на идентификационной карте

7.1 Минимальные требования политики безопасности

7.1.1 Общие положения

В настоящем подразделе определен минимальный набор требований политики безопасности для приложений биометрического сравнения.

7.1.2 Минимальные требования

Во всех случаях применяют следующие минимальные требования политики безопасности:

- ICC не должна отправлять биометрический контрольный шаблон;
- механизм счетчика повторов должен быть реализован в соответствии с требованиями 7.1.3;
- при обмене сообщениями должна быть обеспечена целостность данных биометрического сравнения на идентификационной карте. В дополнение к механизму целостности, предоставляемому протоколом передачи, должны быть реализованы дополнительные механизмы (например, использование безопасного обмена сообщениями);
- все биометрические данные должны быть зашифрованы для передачи в ICC, если только не установлена доверенная среда для сохранения конфиденциальности;
- если в ICC реализован механизм блокировки биометрического сравнения на идентификационной карте, который действует по причинам, отличным от уменьшения счетчика повторов (например, обнаружение атаки), механизм разблокировки не должен восстанавливать счетчик повторов, так как такое восстановление предоставит злоумышленнику, который уже скомпрометировал механизм разблокировки, дополнительные попытки;
- правила безопасности, применяемые для повторной регистрации биометрического контрольного шаблона, должны быть, по крайней мере, эквивалентны тем, которые применены для *первичной* биометрической регистрации.

7.1.3 Управление счетчиком повторов

7.1.3.1 Общие положения

Счетчик повторов определяет доступность биометрического контрольного шаблона для использования в процессе биометрической верификации.

Применяют следующие правила:

- независимый счетчик повторов с определенным начальным значением может существовать для каждого биометрического контрольного шаблона;
- если результат биометрической верификации отрицательный, значение счетчика повторов должно быть уменьшено на единицу;
- если результат биометрической верификации положительный, счетчик повторов должен быть возвращен к его начальному значению;
- если счетчик повторов достигает максимального предела повторов, соответствующий биометрический контрольный шаблон, связанный с данным счетчиком повторов, блокируется.

В *ГОСТ Р ИСО/МЭК 7816-4* DO использования ключа и счетчика повторов определен в шаблоне применимости ключа DO'A3' в соответствующем DO шаблона управляющих ссылок.

Если возвращается допустимое количество повторных попыток, то оно может быть закодировано в байтах состояния SW1, SW2 = '63CX' (где X — оставшееся количество попыток) в ответ на команду биометрической верификации или на команду VERIFY, в которой поле данных отсутствует в соответствии с *ГОСТ Р ИСО/МЭК 7816-4*.

7.1.3.2 Механизм сброса

Операционная система ICC может иметь механизм сброса счетчика повторов биометрического сравнения на идентификационной карте. В тех случаях, когда блокировка механизма биометрического сравнения на идентификационной карте произошла из-за достижения максимального предела повторов, данный механизм должен сбросить счетчик повторов. В некоторых реализациях может дополнительно потребоваться новая биометрическая регистрация.

7.2 Политика безопасности для нескольких приложений биометрического сравнения на идентификационной карте

7.2.1 Таксономия приложений биометрического сравнения, используемых в ICC

Возможны три различные конфигурации *биометрического сравнения на ICC*, которые классифицируют следующим образом:

- для тех приложений, в которых биометрический контрольный шаблон используют как универсальный механизм верификации, отсутствует необходимость в нескольких наборах параметров биометрического сравнения, связанных с применением одного биометрического контрольного шаблона несколькими приложениями. Приложения, использующие механизм биометрического сравнения на идентификационной карте с таким биометрическим контрольным шаблоном, не должны независимо изменять параметры биометрического сравнения;
- в ICC с несколькими приложениями используют биометрическое сравнение на идентификационной карте с одним набором параметров биометрического сравнения (например, одинаковый уровень ВЛС).

Примечание — ICC с одним приложением является частным случаем, в котором применяется универсальный механизм биометрической верификации SP1 (см. 7.2.2);

- использование специфичных для приложений параметров биометрического сравнения. Возможны следующие случаи:

1) каждое приложение имеет собственный биометрический контрольный шаблон и связанную структуру, включая параметры биометрического сравнения,

2) все приложения используют один и тот же биометрический контрольный шаблон, но каждое приложение имеет собственные параметры биометрического сравнения, которые включают, например, различные уровни ВЛС. В этом случае любые изменения параметров биометрического сравнения одного приложения не должны влиять на параметры другого приложения.

Примечание — Термины «глобальный» и «специфичный» используют в соответствии с положениями об основных средствах защиты по *ГОСТ Р ИСО/МЭК 7816-4*.

Далее определены политики безопасности: SP1 (см. 7.2.2), SP2 (см. 7.2.3) и SP3 (см. 7.2.4). В таблице *6* приведено сравнение доменов данных между политиками безопасности.

Таблица 6 — Сравнение доменов данных между политиками безопасности

Политика безопасности	Биометрический контрольный шаблон	Параметры биометрического сравнения	Счетчик повторов
SP1	Общий глобальный	Общие глобальные	Общий глобальный
SP2	Общий глобальный	Отдельные для каждого приложения	Отдельный для каждого приложения
SP3	Отдельный для каждого приложения	Отдельные для каждого приложения	Отдельный для каждого приложения

7.2.2 Политика безопасности для универсального механизма биометрической верификации (SP1)

Для тех приложений, в которых биометрический контрольный шаблон используют как универсальный механизм биометрической верификации, необходимость в нескольких наборах параметров биометрического сравнения отсутствует (см. рисунок 8). В этом случае применяют следующую конфигурацию:

- несколько приложений совместно используют один и тот же биометрический контрольный шаблон и счетчик повторов;
- несколько приложений совместно используют один и тот же набор параметров биометрического сравнения.

Для этой конфигурации применяют следующую политику безопасности: ни одно из приложений не может независимо изменять параметры биометрического сравнения, если отсутствует соответствующее разрешение.

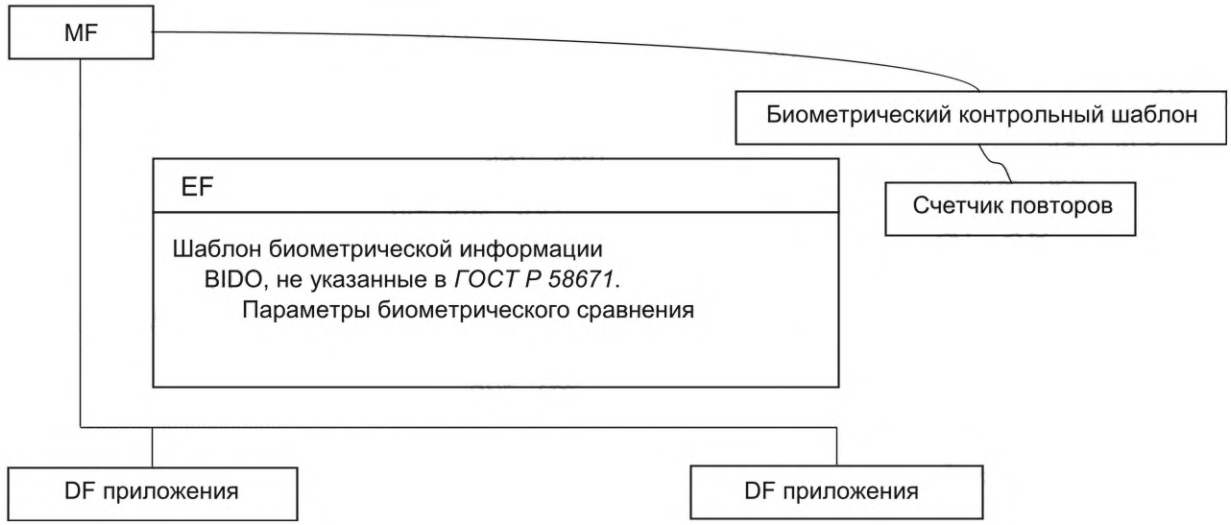

Рисунок 8 — Использование глобальных параметров биометрического сравнения с общим биометрическим контрольным шаблоном и счетчиком повторов

7.2.3 Политика безопасности для общего биометрического контрольного шаблона с независимыми механизмами биометрической верификации (SP2)

Для тех случаев, когда приложения запрашивают независимый контроль биометрического сравнения на идентификационной карте, но совместно используют один и тот же биометрический контрольный шаблон, применяют конфигурацию, представленную на рисунке 9:

- несколько приложений совместно используют один и тот же биометрический контрольный шаблон и счетчик повторов;
- каждое приложение использует собственный набор параметров биометрического сравнения.

Для этой конфигурации применяют следующую политику безопасности: каждое приложение может независимо изменять собственные параметры биометрического сравнения, не изменяя при этом параметры биометрического сравнения других приложений, которые совместно используют один и тот же биометрический контрольный шаблон.

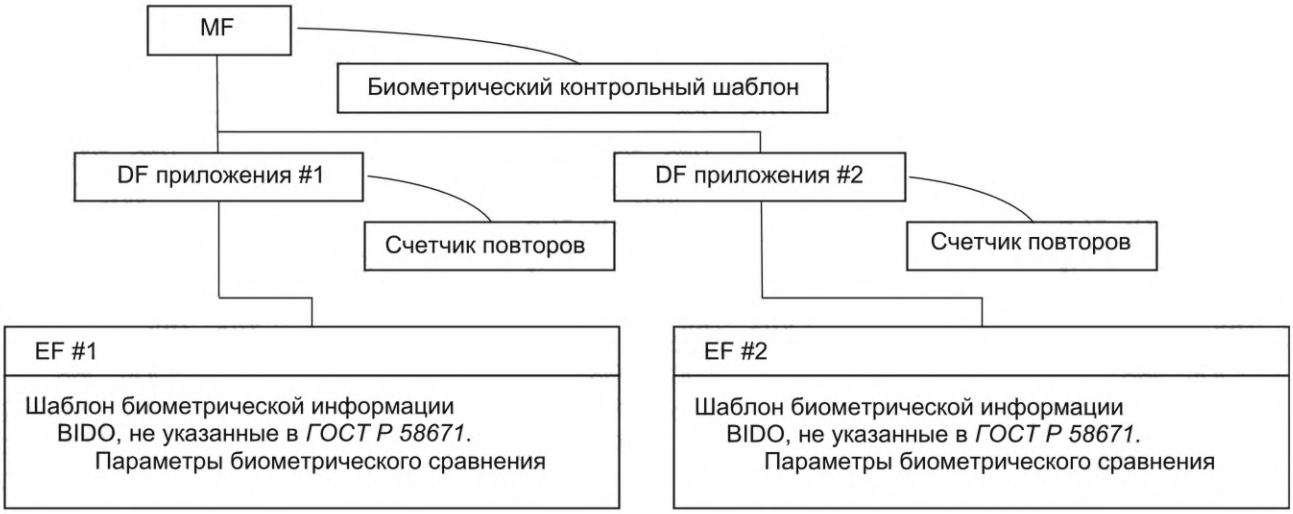

Рисунок 9 — Использование специфичных для приложений параметров биометрического сравнения с общим и биометрическим контрольным шаблоном и счетчиком повторов

7.2.4 Политика безопасности для независимых приложений *биометрического сравнения* (SP3)

В тех случаях, когда несколько приложений используют собственные параметры биометрического сравнения, различные биометрические контрольные шаблоны и счетчики повторов, каждое приложение может иметь собственную политику безопасности. Соответствующая конфигурация показана на рисунке 10. При реализации политики безопасности в соответствии с требованиями конкретного приложения следует руководствоваться требованиями, приведенными в 7.1.



Рисунок 10 — Использование специфичных для приложений параметров биометрического сравнения и различных биометрических контрольных шаблонов и счетчиков повторов

Приложение *А*
(справочное)

Примеры модели переходов статуса безопасности

А.1 Общие положения

В этом приложении приведены три примера реализации механизмов биометрического сравнения на идентификационной карте, относящихся к статусу безопасности ICC. Эти примеры проиллюстрированы с помощью диаграмм состояния *потоков*, где круги относятся к статусам безопасности, а стрелки обозначают процессы и их результаты; оба обозначения подразумевают переходы между состояниями.

Для статуса безопасности используют обозначение «SX», где X = 0 является начальным состоянием, и чем больше значение статуса, тем выше уровень безопасности.

Для понимания примеров используют пороги. Порог эквивалентен определенному уровню ВЛС. Когда выполняют биометрическое сравнение, результат сравнения *C* сравнивают с определенным порогом *T*. Если условие $C \geq T$ выполнено, доступ предоставляется, в противном случае доступ запрещен.

Если приложение на ICC использует более одного порогового значения, их обозначают T_1 T_2 при этом $T_2 > T_1$ и, следовательно, T_2 является более строгим требованием.

Во всех случаях в соответствии с рекомендациями настоящего стандарта процесс биометрического сравнения не может быть выполнен, если заранее не установлен защищенный канал связи между ICC и IFD, используемый при дальнейших операциях.

А.2 Одно одноуровневое приложение

Наиболее простым примером является использование одного приложения на ICC с одним уровнем биометрической верификации (одним порогом). На рисунке *А*.1 представлена схема общего рабочего процесса. В то время, как другие операции, которые не приводят к повышению статуса безопасности, могут быть осуществлены в начальном состоянии S0, биометрическая верификация выполняется только после достижения состояния S1 путем установления защищенного канала между ICC и IFD. Для достижения состояния S1 владелец ICC может выполнить команду `VERIFY`. Если доступ разрешен, достигается состояние S2 и можно выполнять операции, требующие S2.

Если биометрическую верификацию выполнить не удалось, счетчик повторов для биометрического сравнения уменьшается на единицу, и, если дальнейшие попытки не разрешены, механизм биометрического сравнения будет заблокирован.

В том случае, если возвращено сообщение об ошибке безопасности или запрошена несанкционированная операция, состояние будет изменено на начальное состояние S0, что требует установления нового защищенного канала между ICC и IFD перед выполнением дальнейших операций.

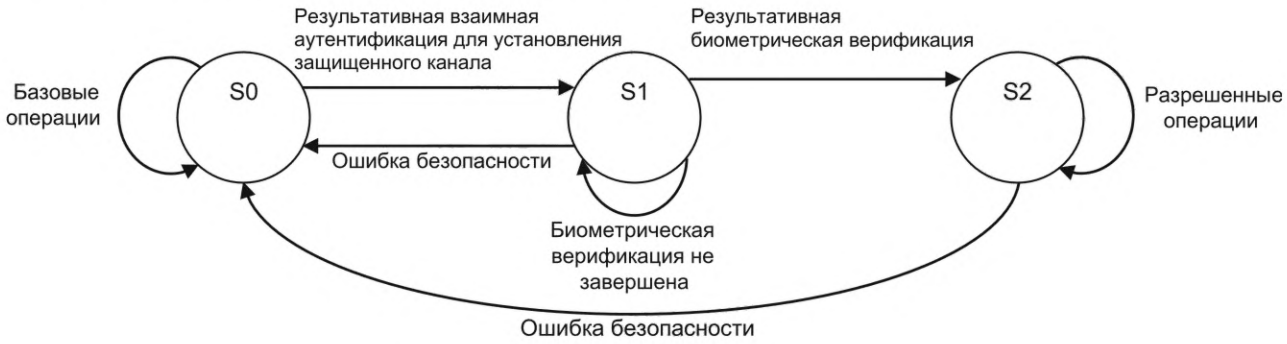

Рисунок *А*.1 — Диаграмма состояний для одного одноуровневого приложения

А.3 Одно разноуровневое приложение

В данной части проиллюстрирован более сложный пример. Если в одном приложении в ICC может быть использовано биометрическое сравнение для предоставления доступа к информации или некоторым операциям, вполне возможно, что для каждой операции будут установлены различные уровни безопасности. Тогда в приложении может быть применен другой уровень безопасности с помощью точности в процессе биометрического сравнения. Для таких случаев выбраны два различных уровня с помощью двух различных пороговых значений, T_1 и T_2, при этом $T_2 > T_1$, т. е. T_2 является более строгим требованием.

После установления защищенного канала между ICC и IFD будет достигнуто значение состояния S1, для которого может быть проведено биометрическое сравнение. Если операция выполнена, может произойти три

различных варианта развития событий. Если $C < T_1$, то доступ запрещен, соответствующий счетчик повторов уменьшается и сохраняется состояние S1. Если $T_1 \le C < T_2$, то будут разрешены только операции в состоянии S2. Только если $C \ge T_2$, разрешены операции в состоянии S3, *а также любые другие операции, требующие выполнения более низкого состояния*.

В том случае, если возвращено сообщение об ошибке безопасности или запрошена несанкционированная операция, будет достигнуто начальное состояние S0, и должен быть установлен новый защищенный канал между ICC и IFD для продолжения операций.

Схема приведена на рисунке А.2.

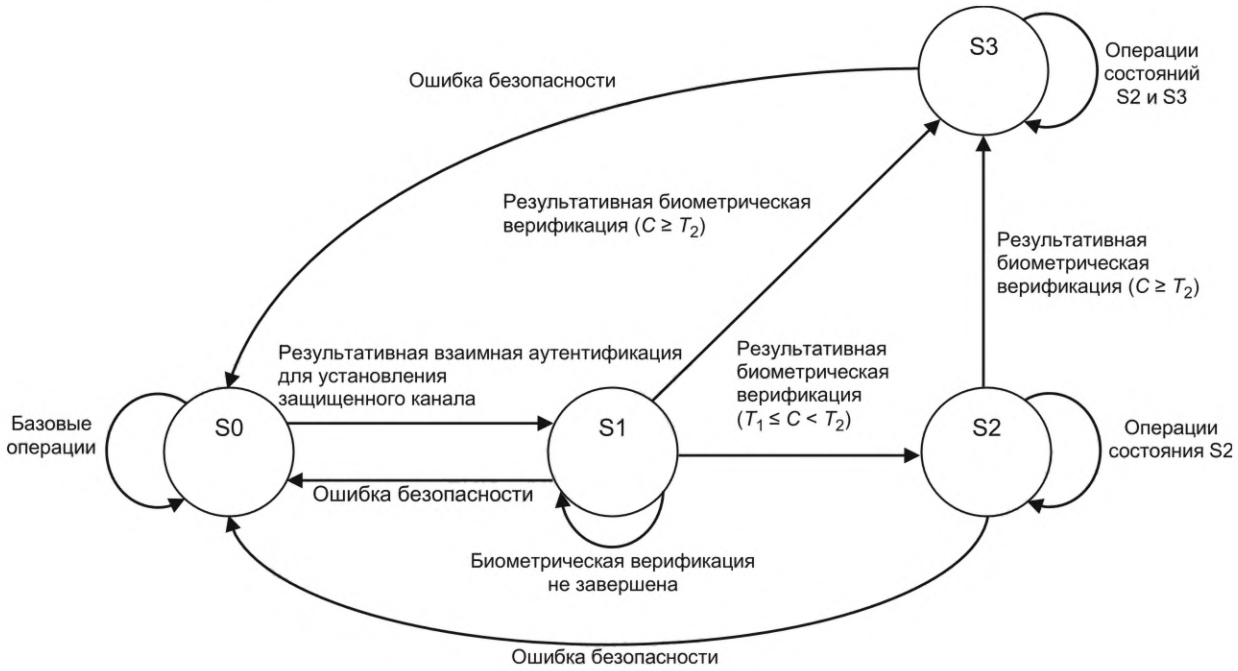

Рисунок А.2 — Диаграмма состояний для одного разноуровневого приложения

А.4 Несколько приложений

Наиболее сложным случаем является ICC с несколькими приложениями, где каждое приложение имеет свои пороговые значения и счетчики повторов для достижения собственных статусов безопасности с использованием одних и тех же данных биометрического контрольного шаблона.

Процедура аналогична той, которая описана для одного разноуровневого приложения, где единственным отличием являются различные пороги и счетчики повторов. Каждый порог и каждый счетчик повторов влияют только на соответствующее им приложение для того, чтобы избежать влияния одного приложения на функционал другого приложения. Статус безопасности одного приложения не влияет на другие приложения, потому что при выборе нового приложения статус безопасности возвращается к начальному значению. Таким образом, после выбора приложения, если использованы некоторые ограниченные операции, устанавливается новый защищенный канал между ICC и IFD, и после этого можно выполнить биометрическое сравнение с помощью команды `VERIFY`. При таком сравнении результатом будут следующие возможности:

- если верификацию выполнить не удалось ($C < T_1$)

1) уменьшение счетчика повторов на единицу, но только счетчика повторов выбранного приложения,

2) блокировка процесса биометрической верификации, если счетчик повторов истек;

- если верификация завершена, счетчик повторов для выбранного приложения будет сброшен и:

1) если $T_1 \le C < T_2$, то будет достигнуто состояние S2 и будут разрешены операции, для выполнения которых требуется состояние S2,

2) если $C \ge T_2$ то будет достигнуто состояние S3 и будут разрешены все операции (состояния S2 и S3).

Схема приведена на рисунке А.3.

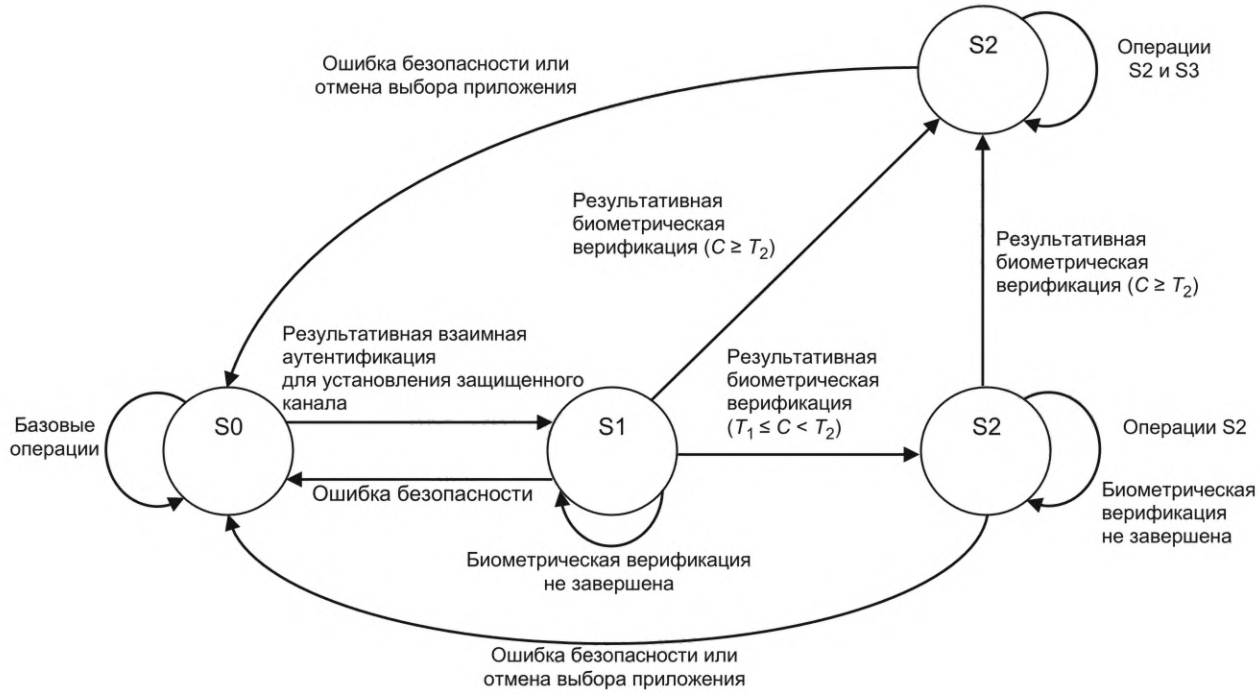

Рисунок *А*.3 — Диаграмма состояний для нескольких приложений

Приложение *В*
(справочное)

Рекомендации для механизмов обеспечения безопасности при биометрическом сравнении на идентификационной карте

В.1 Общие положения

Настоящее приложение предназначено для определения механизма обеспечения безопасности, который следует учитывать при биометрическом сравнении на идентификационной карте. Как указано в настоящем стандарте, настоятельно рекомендуется использовать механизмы обеспечения безопасности из-за проблем конфиденциальности биометрической информации.

Рекомендуется ссылаться на другие соответствующие стандарты обеспечения безопасности для всех технических деталей, которые необходимы для реализации данных механизмов обеспечения безопасности. Рекомендуется применять *ГОСТ Р 58671*, а также *ГОСТ Р ИСО/МЭК 7816-4*, в которых представлено описание команд и механизмов, связанных с ICC.

В.2 Взаимная аутентификация

Прежде всего следует учитывать при необходимости обеспечения безопасности, когда два объекта обмениваются данными, — это взаимное доверие данных объектов. Поэтому при взаимодействии должен быть использован механизм, гарантирующий доверие IFD к ICC, и еще один механизм, обеспечивающий доверие ICC к данному IFD. Эти механизмы называют внутренней и внешней аутентификацией. При использовании обоих механизмов процесс именуют взаимной аутентификацией.

Взаимная аутентификация, как правило, заканчивается генерацией ключа сессии для создания защищенного канала между ICC и IFD. Во избежание повторных атак для каждой сессии должен быть использован уникальный ключ. Некоторые алгоритмы, применяемые для взаимной аутентификации, направляют запрос генерации случайных или псевдослучайных чисел как ICC, так и IFD.

После установления защищенного канала связи между ICC и IFD могут быть реализованы нижеприведенные механизмы обеспечения безопасности.

В.3 Целостность сообщения

При обмене APDU источник компьютерной атаки может попытаться перехватить сообщения и изменить их с целью получения выгоды путем, например, повторной отправки предыдущего биометрического образца для получения доступа к информации об ICC и/или сервисам. Чтобы избежать такого рода атак, рекомендуется, чтобы и IFD, и ICC проверяли целостность полученного APDU.

В.4 Конфиденциальность

Проверку целостности рекомендуется проводить при любом обмене APDU, но иногда может быть использован более высокий уровень безопасности. Особенно значимыми являются те APDU, в которых биометрический контрольный шаблон или биометрический образец передается из IFD в ICC (или с ICC в IFD при биометрическом сравнении вне идентификационной карты). При этом данные не должны быть переданы в необработанном формате, а должны быть зашифрованы на высочайшем доступном уровне безопасности, тем самым повышая конфиденциальность в системе.

Например, если использован алгоритм шифрования с симметричным ключом, данные могут быть зашифрованы с помощью ключа сеанса, полученного путем взаимной аутентификации (при установлении защищенного канала между ICC и IFD).

Также рекомендуется проводить проверку целостности для возможности ее использования до или после шифрования передаваемых данных.

В.5 Предотвращение повторных атак с использованием кода аутентификации сообщения (MAC) с секретным ключом

Для предотвращения повторных атак рекомендуется внедрить в ICC защитный механизм. Один из возможных способов избежать повторной атаки заключается в использовании MAC биометрических данных в сочетании со случайным числом и секретным ключом. IFD может получить случайное число из ICC и рассчитать MAC биометрических данных, который будет связан со случайным числом (полученным из ICC) и секретным ключом. Секретный ключ хранится как в IFD, так и в ICC. Во время взаимодействия необходимо передать только случайное число и MAC. Когда ICC получает биометрические данные и MAC, MAC должен быть проверен на идентификационной карте перед выполнением процесса биометрического сравнения.

Если злоумышленник сможет получить биометрические данные, даже случайное число, полученное из ICC, и MAC предыдущего процесса сравнения, он тем не менее не сможет сгенерировать соответствующий MAC для следующей попытки биометрической верификации, не зная секретного ключа.

Однако при таком подходе при условии, что IFD является надежным и способно хранить секретный ключ, данный метод можно рассматривать как метод реализации защищенного канала между ICC и IFD.

Примечание — Данный подход является дополнительным по отношению к рабочей среде.

Приложение *С*
(справочное)

Пример шаблона биометрической информации, включающего элементы данных CBEFF-3

В настоящем приложении приведен пример шаблона биометрической информации, представленный в таблице *С*.1, включая необходимые элементы данных CBEFF-3 в BHT под тегом 'A1', а также BIDO, определенные в настоящем стандарте, под тегом 'A2'.

Таблица *С*.1 — Пример шаблона биометрической информации с BIDO, определенными в *ГОСТ Р 58294* и в настоящем стандарте

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="8">Значение</th><th>Наличие</th></tr>
<tr><td>'7F60'</td><td>Var</td><td colspan="8">Шаблон биометрической информации (см. ГОСТ Р 58671)</td><td rowspan="2">Наличие</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="7">Значение</td></tr>
<tr><td></td><td></td><td>'80'</td><td>1</td><td colspan="6">Ссылка на алгоритм для использования в команде VERIFY / EXT. AUTHENTICATE / MANAGE SE (см. ГОСТ Р ИСО/МЭК 7816-4) или в команде PBO (см. ГОСТ Р 58671)</td><td>Опционально</td></tr>
<tr><td></td><td></td><td>'83'</td><td></td><td colspan="6">Ссылка на квалификатор данных для использования в команде VERIFY / EXT. AUTHENTICATE / MANAGE SE (см. ГОСТ Р ИСО/МЭК 7816-4) или в команде PBO (см. ГОСТ Р 58671)</td><td></td></tr>
<tr><td></td><td></td><td>'A1'</td><td>Var</td><td colspan="6">BIDO, не указанные в ГОСТ Р 58671.
BIDO для CBEFF-3</td><td>Обязательно</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="3">Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'78'</td><td>Var</td><td colspan="3">Совместимый орган распределения тегов</td><td>Обязательно</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'06'</td><td>Var</td><td>OID по ГОСТ Р 58294</td><td>Обязательно</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="3">Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'70'</td><td>Var</td><td colspan="3"></td><td>Обязательно</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'A7'</td><td>8</td><td>CBEFF_BDB_format (созданные)</td><td>Обязательно, если отсутствуют первичные DO с тегами '87' и '88'</td></tr>
</table>

Продолжение таблицы С.1

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="6">Значение</th><th>Наличие</th></tr>
<tr><td rowspan="15">'7F60'</td><td rowspan="15">Var</td><td colspan="4" rowspan="2"></td><td>Тег</td><td>Длина</td><td>Значение</td><td rowspan="2">Наличие</td></tr>
<tr><td>'87'</td><td rowspan="2">2</td><td>C B E F F _ B D B _ format_owner</td><td rowspan="2">Обязательно, если отсутствует созданный DO'A7'</td></tr>
<tr><td colspan="4"></td><td>'88'</td><td>C B E F F _ B D B _ format_type</td></tr>
<tr><td></td><td>Тег</td><td>Длина</td><td colspan="5">Значение</td><td>Наличие</td></tr>
<tr><td></td><td>'A2'</td><td>Var</td><td colspan="5">BIDO, не указанные в ГОСТ Р 58671.
BIDO, указанные в настоящем стандарте</td><td>Обязательно</td></tr>
<tr><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="3">Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td>'78'</td><td>9</td><td colspan="3">Совместимый орган распределения тегов</td><td>Обязательно для настоящего стандарта</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'06'</td><td>7</td><td>'28 81 C1 53 01 8F 68'
OID настоящего стандарта</td><td>Обязательно для настоящего стандарта</td></tr>
<tr><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="3">Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td>'70'</td><td>Var</td><td colspan="3">BIDO, указанные в настоящем стандарте</td><td>Обязательно для настоящего стандарта</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'91' или 'B1'</td><td rowspan="2">Var</td><td>Параметры биометрического сравнения. DO, содержащиеся в DO'B1', приведены в таблице 3. Совместимый орган распределения тегов, указанный в DO'78' (т. е. в настоящем стандарте)</td><td rowspan="2">По крайней мере один DO</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'92' или 'B2'</td><td>Информация о биометрической функциональности. DO, содержащиеся в DO'B2', приведены в таблице 2. Совместимый орган распределения тегов, указанный в DO'78' (т. е. в настоящем стандарте)</td></tr>
</table>

Окончание таблицы С.1

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="4">Значение</th><th>Наличие</th></tr>
<tr><td rowspan="11">'7F60'</td><td rowspan="11">Var</td><td>Тег</td><td>Длина</td><td colspan="2">Значение</td><td></td></tr>
<tr><td>'5F2E'</td><td>Var</td><td colspan="2">Биометрические данные (первичные)</td><td>Если биометрические данные хранятся в DO'7F60', обязательно наличие DO'5F2E' или DO'7F2E'</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="2">Значение</td><td>Наличие</td></tr>
<tr><td>'7F2E'</td><td>Var</td><td colspan="2">Биометрические данные (созданные)</td><td>Если биометрические данные хранятся в DO'7F60', обязательно наличие DO'5F2E' или DO'7F2E'</td></tr>
<tr><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Наличие</td></tr>
<tr><td></td><td></td><td>'81'</td><td>Var</td><td>Биометрические данные в стандартном формате (первичные), как указано в ГОСТ ISO/IEC 19794-1, ГОСТ Р 58295, ГОСТ Р 58298, ГОСТ Р 58668.8, ГОСТ Р 58668.11, ГОСТ Р ИСО/МЭК 19794-3, ГОСТ Р ИСО/МЭК 19794-5, ГОСТ Р ИСО/МЭК 19794-7, ГОСТ Р ИСО/МЭК 19794-8, ГОСТ Р ИСО/МЭК 19794-10, ГОСТ Р ИСО/МЭК 19794-11, ГОСТ Р ИСО/МЭК 19794-14</td><td>Обязательно, если отсутствует DO'A1' под DO'7F2E'</td></tr>
<tr><td></td><td></td><td>'82'</td><td>Var</td><td>Биометрические данные в проприетарном формате (первичные)</td><td>Опционально. Возможно только в том случае, если отсутствует DO'A2' под DO'7F2E'</td></tr>
<tr><td></td><td></td><td>'A1'</td><td>Var</td><td>Биометрические данные в стандартном формате (созданные), как указано в ГОСТ Р 58668.2, ГОСТ Р 58668.3, ГОСТ Р 58668.4, ГОСТ Р 58668.8, ГОСТ Р 58668.11</td><td>Опционально, если отсутствует DO'81' под DO'7F2E'</td></tr>
<tr><td></td><td></td><td>'A2'</td><td>Var</td><td>Биометрические данные в проприетарном формате (созданные)</td><td>Опционально, если отсутствует DO'81' под DO'7F2E'</td></tr>
</table>

Приложение *D*
(справочное)

Пример реализации глобального биометрического контрольного шаблона

D.1 Общие положения

Когда принимается глобальный биометрический контрольный шаблон по *ГОСТ Р 58671*, он может быть немедленно зарегистрирован в MF и совместно использован несколькими приложениями биометрического сравнения на идентификационной карте. Для данного глобального биометрического шаблона MF хранит шаблон биометрической информации в EF, чтобы дать IFD подробную информацию об этом биометрическом контрольном шаблоне. Шаблон биометрической информации предоставляет информацию о биометрической функциональности глобального биометрического контрольного шаблона (см. таблицу *1*).

Согласно политике таких приложений параметры биометрического сравнения хранятся в разных местах. В настоящем приложении приведены примеры реализаций SP2 (см. *7*.2.3) для представления надлежащих методов связи приложения с удаленным элементом данных.

D.2 Общая структура глобального биометрического контрольного шаблона

Биометрический контрольный шаблон в рамках MF доступен глобально из DF приложений. Доступ к нему осуществляется путем указания квалификатора биометрического контрольного шаблона, который определяет ссылку на этот биометрический контрольный шаблон, представленный на рисунке *D*.1.

Два DF приложений хранятся непосредственно под MF, и каждый из DF размещает различные приложения биометрического сравнения на идентификационной карте. Когда IFD инициирует одно из приложений, выбирается прикладной DF и из его EF извлекается шаблон биометрической информации, приведенный в таблице *D*.1.

Шаблон биометрической информации предоставляет квалификатор биометрического контрольного шаблона, который указывает ссылку на глобальный биометрический контрольный шаблон, на котором базируется шаблон биометрической информации. Шаблон биометрической информации также предоставляет информацию о биометрической функциональности с общим шаблоном ссылок. Данный общий шаблон указывает местоположение фактической информации о биометрической функциональности глобального биометрического контрольного шаблона, хранящегося под MF. Благодаря данному местоположению, которое предоставляет DF приложения, становится возможным для IFD извлечь фактическую информацию о биометрической функциональности и подготовиться к процессу биометрической верификации.

Перед подготовкой процесса верификации IFD устанавливает, что шаблон биометрической информации является подходящим для оценки путем сопоставления значения квалификатора биометрического контрольного шаблона с таким в *CRT AT* безопасной среды, а также путем проверки значения байта квалификатора применимости в *CRT AT*, соответствующем основанной на биометрии аутентификации пользователя (*AT*) согласно *ГОСТ Р ИСО/МЭК 7816-4*. *SEID*, который идентифицирует безопасную среду по *ГОСТ Р ИСО/МЭК 7816-4*, предоставляется как один из атрибутов секретности из FCI, связанной с DF приложения.

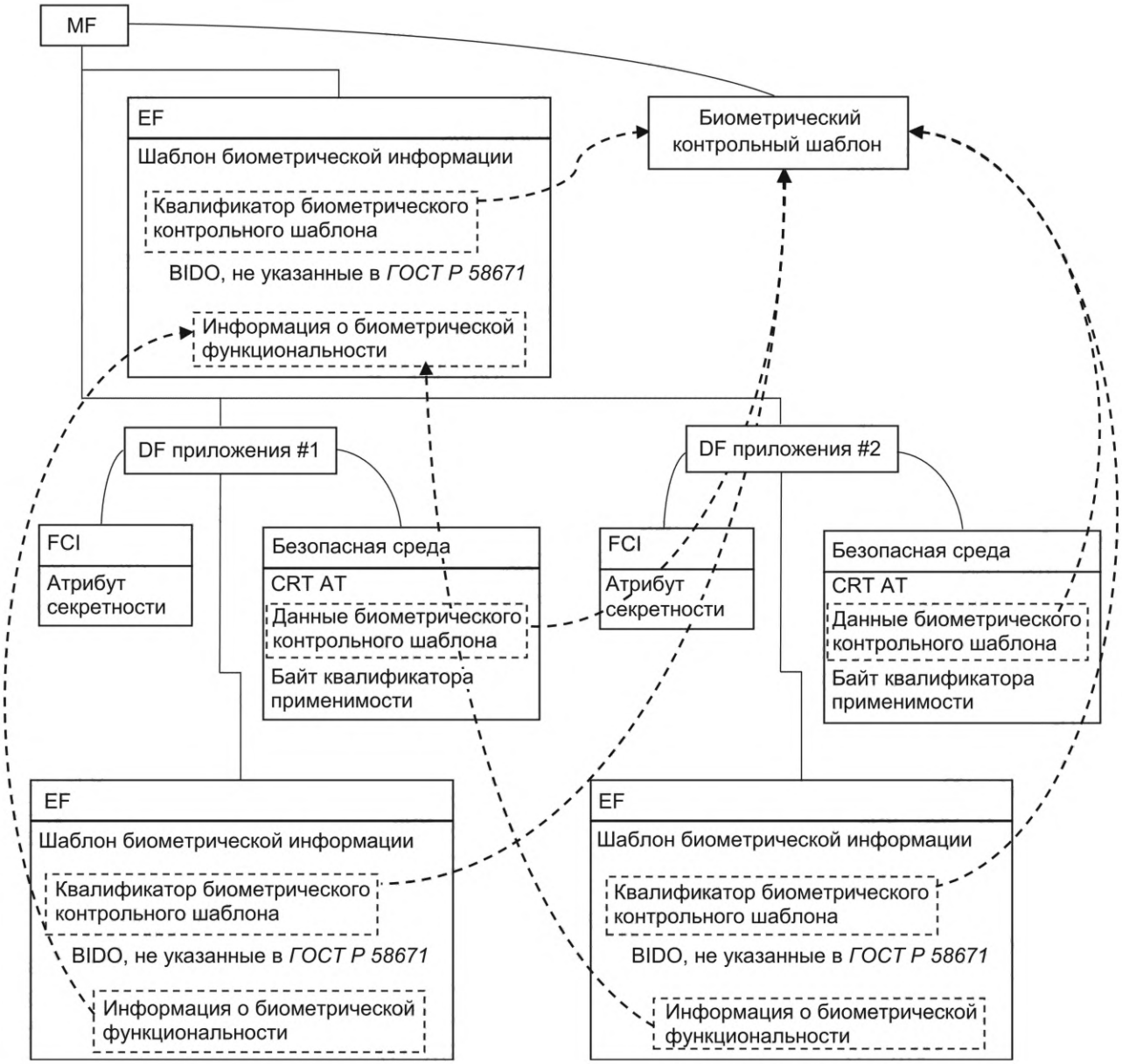

Рисунок D.1 — Пример общей структуры для глобального биометрического шаблона

Таблица *D*.1 — Шаблон биометрической информации для глобального биометрического контрольного шаблона

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="7">Значение</th></tr>
<tr><td>'7F60'</td><td>Var</td><td colspan="7">Шаблон биометрической информации</td></tr>
<tr><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="5">Значение</td></tr>
<tr><td></td><td></td><td>'83'</td><td>1</td><td colspan="5">Квалификатор биометрических данных</td></tr>
<tr><td></td><td></td><td>'A2'</td><td>Var</td><td colspan="5">BIDO, не указанные в ГОСТ Р 58671</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="3">Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'78'</td><td>9</td><td colspan="3">Совместимый орган распределения тегов</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'06'</td><td>7</td><td>OID настоящего стандарта
'28 81 C1 53 01 8F 68'</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="3">Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'70'</td><td>Var</td><td colspan="3">BIDO, указанные в настоящем стандарте</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'91' или 'B1'</td><td rowspan="3">Var</td><td>Параметры биометрического сравнения (применяемые в рамках DF приложения, см. 6.3.3.3)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'92' или 'B2'</td><td>Информация о биометрической функциональности (применяемая в рамках MF, см. 6.3.3.2)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'B2'</td><td>Информация о биометрической функциональности (применяемая в рамках DF приложения)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег | Длина | Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>'60' | Var | Общий шаблон ссылок</td></tr>
</table>

D.3 Глобальный биометрический контрольный шаблон, совместно используемый через ссылку файла DO

Каждое приложение имеет собственный шаблон биометрической информации DO'7F60', определенный в *ГОСТ Р 58671*, включая собственные параметры биометрического сравнения. Эти шаблоны биометрической информации также имеют шаблон биометрических данных DO'7F2E', определенный в *ГОСТ Р 58671*. Биометрический контрольный шаблон не входит в шаблоны биометрических данных, но ссылка на файл DO'51', определенная в *ГОСТ Р ИСО/МЭК 7816-4*, указывает фактический шаблон биометрических данных, который содержит квалификатор и данные биометрического контрольного шаблона.

Пример структуры шаблона биометрической информации приведен в таблице *D*.2.

В таблице D.2 для размещения приложений и хранения данных приложений применена файловая структура, определенная в *ГОСТ Р ИСО/МЭК 7816-4*. На рисунке *D*.2 показан пример файловой структуры, в которой один биометрический контрольный шаблон используется двумя приложениями. *Файловая структура следующая:*

- биометрический контрольный шаблон хранится во внутреннем EF для защиты в рамках MF. Данный биометрический контрольный шаблон используют два разных приложения через ссылку на файл DO'51', инкапсулированную в собственном шаблоне биометрической информации, хранящемся в EF каждого приложения;
- в MF находятся два DF, каждый из которых размещает приложение с функциональностью биометрической верификации;
- каждый рабочий EF в рамках каждого DF хранит зависящий от приложения шаблон биометрической информации. Каждое приложение может предоставлять собственные параметры сравнения биометрических данных;
- информация об управлении файлами (FCI) предоставляется каждому EF, хранящему зависящий от приложения шаблон биометрической информации. FCI, связанная с EF, может включать атрибуты секретности. Атрибуты секретности могут указывать условия секретности для выполнения каждой команды для данного EF, например `READ BINARY` и `VERIFY`;

Таблица *D*.2 — Пример шаблона биометрической информации для глобального биометрического контрольного шаблона, распространяемого через ссылку на файл DO

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="6">Значение</th><th>Примечание</th></tr>
<tr><td rowspan="20">'7F60'</td><td rowspan="20">Var</td><td colspan="6">Шаблон биометрической информации</td><td>—</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="4">Значение</td><td>Примечание</td></tr>
<tr><td>'A1'</td><td>Var</td><td colspan="4">BIDO, не указанные в ГОСТ Р 58671.
BIDO для CBEFF-3</td><td>Обязательно при наличии DO, указанных в ГОСТ Р 58294</td></tr>
<tr><td>Тег</td><td>Длина</td><td colspan="4">Значение</td><td>Примечание</td></tr>
<tr><td>'A2'</td><td>Var</td><td colspan="4">BIDO, не указанные в ГОСТ Р 58671.
BIDO, указанные в настоящем стандарте</td><td>—</td></tr>
<tr><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="2">Значение</td><td>Примечание</td></tr>
<tr><td></td><td></td><td>'78'</td><td>9</td><td colspan="2">Совместимый орган распределения тегов</td><td>—</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Примечание</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'06'</td><td>7</td><td>'28 81 C1 53 01 8F 68'</td><td>OID настоящего стандарта</td></tr>
<tr><td></td><td></td><td>'70'</td><td>Var</td><td colspan="2">BIDO, указанные в настоящем стандарте</td><td>—</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td>Значение</td><td>Примечание</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'91' или 'B1'</td><td>Var</td><td>Параметры биометрического сравнения</td><td>Если применимо (см. рисунок D.2)</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'92' или 'B2'</td><td>Var</td><td>Информация о биометрической функциональности</td><td>Если применимо (см. рисунок D.2)</td></tr>
<tr><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="4">Значение</td><td>Примечание</td></tr>
<tr><td></td><td></td><td>'7F2E'</td><td>Var</td><td colspan="4">Шаблон биометрических данных</td><td>—</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>Длина</td><td colspan="2">Значение</td><td>Примечание</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'51'</td><td>Var</td><td colspan="2">Ссылка на файл</td><td>Указание местоположения файла биометрического контрольного шаблона</td></tr>
</table>

- ссылка на файл DO'51' инкапсулируется в каждый шаблон биометрической информации, зависящий от приложения;
- ссылка на файл DO'51' указывает на фактический шаблон биометрических данных, который содержит квалификатор и данные биометрического контрольного шаблона.

MF, DF, внутренний и рабочий EF, FCI, атрибут секретности, условие секретности и ссылка на файл определены в *ГОСТ Р ИСО/МЭК 7816-4*.

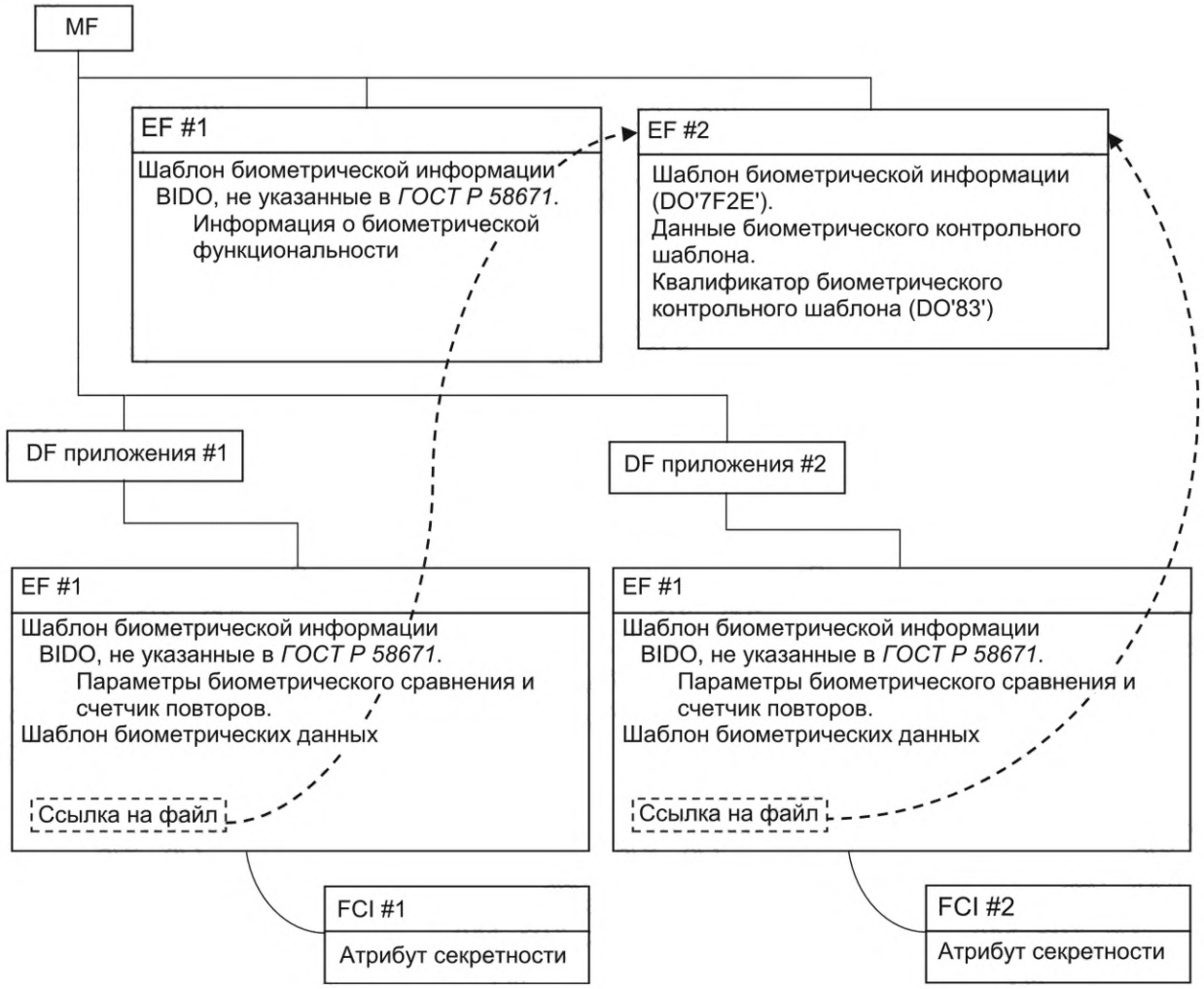

Рисунок *D*.2 — Пример общей структуры для глобального биометрического шаблона, распространяемого через DO ссылками на файл

Приложение *Е*
(справочное)

Типовой APDU для биометрического сравнения на идентификационной карте

Сравнение биометрических данных на идентификационной карте реализовано с помощью команды PBO, а также команды VERIFY, определенной в *ГОСТ Р ИСО/МЭК 7816-4*. Команду VERIFY используют для отправки данных контрольных точек отпечатков пальцев в ICC. Она имеет структуру, представленную в таблице *Е*.1.

Таблица *Е*.1 — Структура команды APDU для биометрического сравнения на идентификационной карте

Поле	Данные
CLA	'00'
INS	'20' или '21'*
P1	'00'
P2	'00'
Lc	Длина поля данных команды (не более 255)
Данные	Данные биометрической верификации*
Le	Отсутствуют
* Тег '20' используют, если поле данных содержит открытые данные с простой структурой, тогда как тег '21' указывает, что поле данных TLV закодировано в соответствии с BER. Примечание — Поле Le пустое, потому что в ответ на команду VERIFY в соответствии с *ГОСТ Р ИСО/МЭК 7816-4* данные не возвращены. В IFD возвращается только значение состояния.	

Поле данных содержит данные верификации. Возможности ICC могут быть косвенно указаны. Рекомендуется сформировать шаблон биометрической информации, который находится в открытом доступе для считывания с ICC с использованием команды GET DATA и тега '7F60' и предоставляет внешнему устройству информацию о возможностях ICC, например: о поддержке биометрического сравнения на идентификационной карте, о применяемом формате данных и типе формата и о том, будет ли ICC упорядочивать контрольные точки. Подробные сведения о шаблоне биометрической информации приведены в *ГОСТ Р 58671* и *ГОСТ Р 58294*.

Шаблон в поле данных должен быть TLV закодирован в соответствии с BER. Для кодирования используют следующие теги:

- '7F2E' — биометрический контрольный шаблон;
- '5F2E' — биометрические данные;
- '81' или 'A1' — биометрические данные в стандартном формате (первичные/созданные);
- '82' или 'A2' — биометрические данные в проприетарном формате (первичные/созданные).

Если на ICC отправляют данные стандартных контрольных точек, они кодируются в поле данных в соответствии с таблицей *Е*.2.

Таблица *Е*.2 — Поля данных для стандартных контрольных точек

Тег	Длина	Значение		
'7F2E'	Var	Шаблон биометрических данных		
		Тег	Длина	Значение
		'81'	Var	Биометрические данные в стандартном формате (первичные). Набор контрольных точек
Примечание — В таблице использован тег '7F2E', потому что поле «Значение» содержит объект созданных биометрических данных. Объект созданных биометрических данных начинается с тега '81', далее следуют значения актуальных биометрических данных. Другой возможный способ заключается в использовании тега '5F2E' для инкапсуляции биометрических данных в качестве первичных данных.				

На рисунке *Е*.1 представлен образец изображения с извлеченными данными контрольных точек.



Рисунок *Е*.1 — Образец изображения с извлеченными данными контрольных точек

Контрольные точки изображения отпечатка пальца переводят в метрическую систему и сжимают в формат идентификационной карты для использования в процессе биометрического сравнения на идентификационной карте. В результате получают следующие данные (в шестнадцатеричном представлении):

'25 5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF 81 48 B0 BF 48 96 48 48 5D 89
4A 9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50 91 42 54 85 6B 57 6B AA 58 86 B2 58 7D 70
59 36 82 5B 8C 57 5E 94 9C 5F 73 71 61 61 66 64 4C 9C 69 97 9B 6F A5 9D 70 33 B9 72 50 96
74 92 58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D 74 9A 3A 76'

Тип формата 6 владельца формата '0101' из *ГОСТ Р ИСО/МЭК 19794-2* используют для кодирования контрольных точек, за исключением любых расширенных данных. Контрольные точки расположены в точках бифуркации остова гребня и окончаниях остова гребня. Метод построен по аналогии с проверкой данных, используемой экспертом по отпечаткам пальцев, и на основе обычной практики большинства изготовителей алгоритмов отпечатков пальцев. Каждая контрольная точка представлена 3 байтами. Первая контрольная точка имеет значение '25' для координаты *X*, значение '5D' для координаты *Y*, типовую бифуркацию окончания гребня и ориентацию 205°, хранящиеся в '69'.

В общей сложности обнаружено 38 контрольных точек, в результате чего общий размер контрольных точек $3 \cdot 38 = 114$ байтов, в шестнадцатеричном формате — '72'.

Данные, добавленные в описанную выше структуру, получены при реализации команды, приведенной на рисунке *Е*.2.

CLA	INS	P1	P2	LC	Данные
'00'	'21'	'00'	'00'	'77'	–

Тег биометрического контрольного шаблона	Длина объекта биометрических данных	Тег стандартизованных биометрических данных	Длина данных контрольных точек	Данные контрольных точек
'7F2E'	'74'	'81'	'72'	–

‘25 5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF 81 48 B0
BF 48 96 48 48 5D 89 4A 9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50
91 42 54 85 6B 57 6B AA 58 86 B2 58 7D 70 59 36 82 5B 8C 57 5E 94 9C
5F 73 71 61 61 66 64 4C 9C 69 97 9B 6F A5 9D 70 33 B9 72 50 96 74 92
58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D 74 9A 3A 76´

Рисунок *E*.2 — Структура APDU для биометрического сравнения на идентификационной карте

Команда полностью:

'00 21 00 00 77 7F 2E 74 81 72 25 5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF
81 48 B0 BF 48 96 48 48 5D 89 4A 9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50 91 42 54 85
6B 57 6B AA 58 86 B2 58 7D 70 59 36 82 5B 8C 57 5E 94 9C 5F 73 71 61 61 66 64 4C 9C 69 97
9B 6F A5 9D 70 33 B9 72 50 96 74 92 58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D
74 9A 3A 76'

Есть и другие возможности для кодирования контрольных точек и построения команды. Могут быть использованы дополнительные признаки или проприетарные данные.

Профиль приложения должен дать указания для данных опций для облегчения реализации совместимости приложений, использующих технологии различных изготовителей.

Командные сообщения, приведенные в настоящем приложении, не шифруют биометрические данные. Эти сообщения могут быть использованы в безопасной среде или в безопасном механизме обмена сообщениями (например, команда ENVELOPE) для обеспечения конфиденциальности.

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 ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»[1)]
ГОСТ ISO/IEC 19794-1—2015	IDT	ISO/IEC 19794-1:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура»
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»[2)]
ГОСТ Р 58295—2018 (ИСО/МЭК 19794-6:2011)	MOD	ISO/IEC 19794-6:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
ГОСТ Р 58298—2018 (ИСО/МЭК 19794-4:2011)	MOD	ISO/IEC 19794-4:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»
ГОСТ Р 58668.2—2021 (ИСО/МЭК 39794-4:2019)	MOD	ISO/IEC 39794-4:2019 «Информационные технологии. Расширяемые форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»
ГОСТ Р 58668.3—2021 (ИСО/МЭК 39794-5:2019)	MOD	ISO/IEC 39794-5:2019 «Информационные технологии. Расширяемые форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
ГОСТ Р 58668.4—2021 (ИСО/МЭК 39794-6:2021)	MOD	ISO/IEC 39794-6:2021 «Информационные технологии. Расширяемые форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
ГОСТ Р 58668.8—2019 (ИСО/МЭК 19794-9:2011)	MOD	ISO/IEC 19794-9:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла»
ГОСТ Р 58668.11—2019 (ИСО/МЭК 19794-13:2018)	MOD	ISO/IEC 19794-13:2018 «Информационные технологии. Форматы обмена биометрическими данными. Часть 13. Данные голоса»
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»[3)]
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 19794-2—2013	IDT	ISO/IEC 19794-2:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца — контрольные точки»

[1)] ISO/IEC 2382-37:2012 заменен. Действует ISO/IEC 2382-37:2022.
[2)] ISO/IEC 19785-3:2015 заменен. Действует ISO/IEC 19785-3:2025.
[3)] ISO/IEC 7816-11:2017 заменен. Действует ISO/IEC 7816-11:2022.

Окончание таблицы ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО/МЭК 19794-3—2009	IDT	ISO/IEC 19794-3-2006 «Информационные технологии. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца»
ГОСТ Р ИСО/МЭК 19794-5—2013	IDT	ISO/IEC 19794-5:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
ГОСТ Р ИСО/МЭК 19794-7—2017	IDT	ISO/IEC 19794-7:2014 «Информационные технологии. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи»
ГОСТ Р ИСО/МЭК 19794-8—2015	IDT	ISO/IEC 19794-8:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 8. Данные изображения отпечатка пальца — остов»
ГОСТ Р ИСО/МЭК 19794-10—2010	IDT	ISO/IEC 19794-10:2007 «Информационные технологии. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки»
ГОСТ Р ИСО/МЭК 19794-11—2015	IDT	ISO/IEC 19794-11:2013 «Информационные технологии. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи»
ГОСТ Р ИСО/МЭК 19794-14—2017	IDT	ISO/IEC 19794-14:2013 «Информационные технологии. Форматы обмена биометрическими данными. Часть 14. Данные ДНК»
ГОСТ Р ИСО/МЭК 29794-1—2018	IDT	ISO/IEC 29794-1:2016 «Информационные технологии. Качество биометрического образца. Часть 1. Структура»
ГОСТ Р ИСО/МЭК 29794-6—2018	IDT	ISO/IEC 29794-6:2015 «Информационные технологии. Качество биометрического образца. Часть 6. Данные изображения радужной оболочки глаза»
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 24787-1:2024	
Разделы	Подразделы	Разделы	Подразделы
3	3.1	3	3.1
	3.2		3.2
	3.3		3.3
	3.4		3.4
	3.5		3.5
	—		3.6
	—		3.7
	—		3.8
	3.6		3.9
	—		3.10
	—		3.11
	3.7		3.12
	—		3.13
	—		3.14
	—		3.15
	—		3.16
4		4	
—		5	
—		6	
5	5.1	7	7.1
	5.2		7.2
	5.3		7.3
	5.4		7.4
	5.5		7.5
6	6.1	8	8.1
	6.2		8.2
	6.3		8.3
	6.4		8.4
	6.5		8.5
7	7.1	9	9.1
	7.2		9.2

Окончание таблицы ДБ.1

Структура настоящего стандарта		Структура международного стандарта ИСО/МЭК 24787-1:2024	
Разделы	Подразделы	Разделы	Подразделы
Приложения	A	Приложения	C
	B		D
	C		E
	D		B
	E		A
	ДА		—
	ДБ		—
—		Библиография	
Примечание — Сопоставление структуры стандартов приведено начиная с раздела 3, так как предыдущие разделы стандартов и их иные структурные элементы (за исключением предисловия) идентичны.			

УДК 336.77:002:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, идентификационные карты, биометрическое сравнение, биометрическое сравнение на идентификационной карте

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 06.02.2026. Подписано в печать 24.02.2026. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 3,86.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru