ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58291— 2018 (ИСО/МЭК 18584: 2015)

Информационные технологии

КАРТЫ ИДЕНТИФИКАЦИОННЫЕ

Требования к испытаниям на соответствие для приложений, осуществляющих биометрическое сравнение на идентификационной карте

(ISO/IEC 18584:2015, MOD)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») и Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4, при консультативной поддержке Акционерного общества «Ангстрем-Т» (АО «Ангстрем-Т») и Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2018 г. № 1041-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 18584:2015 «Информационные технологии. Карты идентификационные. Требования к испытаниям на соответствие для приложений, осуществляющих биометрическое сравнение на идентификационной карте» (ISO/IEC 18584:2015 «Information technology — Identification cards — Conformance test requirements for on-card biometric comparison applications», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом. Внесение указанных технических отклонений направлено на учет потребностей национальной экономики Российской Федерации.

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

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

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за установление подлинности каких-либо или всех таких патентных прав

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

© ISO, 2015 — Все права сохраняются
© Стандартинформ, оформление, 2018

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 Методология испытаний . . . 4
5.1 Тестовые утверждения . . . 4
5.2 Критерии испытаний . . . 4
6 Требования к испытаниям на соответствие данных, используемых для биометрического сравнения на идентификационной карте . . . 4
6.1 Обработка биометрического контрольного шаблона, хранящегося на идентификационной карте . . . 4
6.2 Данные конфигурации (для биометрической верификации) . . . 4
6.3 Общий интерфейс для нескольких приложений . . . 8
6.4 Управление счетчиком повторов . . . 8
7 Требования к испытаниям на соответствие стандартных процессов биометрического сравнения на идентификационной карте . . . 8
7.1 Стандартные процессы . . . 8
7.2 Процесс биометрического сравнения и вывод результата . . . 9
8 Требования к испытаниям на соответствие механизма выполнения распределения нагрузки с использованием WSR-протокола . . . 9
8.1 Биометрический контрольный шаблон для механизма распределения нагрузки . . . 9
8.2 Байты команды и ответа для распределения нагрузки . . . 9
8.3 Управление распределением нагрузки . . . 10
9 Требования к испытаниям на соответствие принципов обеспечения безопасности для биометрического сравнения на идентификационной карте . . . 11
9.1 Общие принципы обеспечения безопасности CSP для биометрического сравнения на идентификационной карте . . . 11
9.2 Принципы обеспечения безопасности SP1 для глобальных данных конфигурации сравнения . . . 12
9.3 Принципы обеспечения безопасности SP2 для локальных данных конфигурации сравнения . . . 12
Приложение А (обязательное) Регламент испытаний данных биометрического шаблона, использующихся для механизма распределения нагрузки . . . 14
Приложение В (справочное) Структура испытания . . . 15
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте . . . 17
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного международного стандарта . . . 19
Библиография . . . 20

Введение

Биометрическое сравнение на идентификационной карте обеспечивает более безопасную биометрическую аутентификацию, так как процесс сравнения выполняется на карте на интегральной схеме (ICC) и данные биометрического контрольного шаблона никогда не передаются из ICC. ГОСТ Р 58230 устанавливает требования к процессу биометрического сравнения на ICC. Приложение ICC, которое соответствует требованиям ГОСТ Р 58230, должно соответствовать требованиям, установленным в настоящем стандарте. Требования, установленные к ICC, выполняющим весь процесс биометрического сравнения на идентификационной карте, и ICC, использующим механизм распределения нагрузки, определены в ГОСТ Р 58230.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

КАРТЫ ИДЕНТИФИКАЦИОННЫЕ

Требования к испытаниям на соответствие для приложений, осуществляющих биометрическое сравнение на идентификационной карте

Information technology. Identification cards. Conformance test requirements for on-card biometric comparison applications

Дата введения — 2019—08—01

1 Область применения

Настоящий стандарт устанавливает требования к испытаниям на соответствие:

- для приложений с обобщенной структурой, осуществляющих биометрическое сравнение на идентификационной карте;
- для приложений, осуществляющих биометрическое сравнение на идентификационной карте с использованием механизма распределения нагрузки;
- для проверки выполнения принципов обеспечения безопасности в процессе биометрического сравнения на идентификационной карте, указанных в *ГОСТ Р 58230*.

Настоящий стандарт распространяется только на испытания пар команд и ответов APDU, используемых для ICC, способных выполнять биометрическое сравнение на идентификационной карте в соответствии с *ГОСТ Р 58230*.

Настоящий стандарт не распространяется на оценку эффективности алгоритмов биометрического сравнения на идентификационной карте с точки зрения вероятностей ошибок.

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

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

ГОСТ Р ИСО/МЭК 7816-11 Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами

ГОСТ Р ИСО/МЭК 14443-2 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 2. Радиочастотный энергетический и сигнальный интерфейс

ГОСТ Р ИСО/МЭК 19785-1 Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных

ГОСТ Р ИСО/МЭК 19785-2 Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии

Издание официальное

ГОСТ Р ИСО/МЭК 19794-2—2013 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 19794-4 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. 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 19794-6 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

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 19794-9 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла

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

ГОСТ Р 58230—2018 (ИСО/МЭК 24787:2010) Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте

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 ИСО/МЭК 7816-11*, а также следующие термины с соответствующими определениями:

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

Пример — Такие данные, как ориентация, масштабирование и т. п., являются вспомогательными данными.

3.2 **биометрическое заявление** (biometric claim): Заявление, что субъект сбора биометрических данных является собственно источником установленного биометрического контрольного шаблона.

3.3 **формат биометрических данных** (biometric data format): Структура представления биометрических данных.

3.4 **идентификатор биометрического продукта** (biometric product identifier): Уникальный идентификатор, присвоенный биометрическому продукту регистрационном органом в соответствии с *ГОСТ Р ИСО/МЭК 19785-1**.

3.5 **система биометрической верификации** (biometric verification system): Система, назначением которой является выполнение процесса подтверждения биометрического заявления.

3.6 **клиентское приложение** (client application): Программное обеспечение, установленное на биометрическом терминале и предназначенное для обработки запроса сравнения, в котором используется решение, полученное в процессе сравнения на идентификационной карте.

3.7 **установка** (installation): Запись требуемых параметров в энергонезависимую память ICC операционной системой (ОС) ICC, выполняющей процедуру установки после того, как приложение загружено в ICC.

3.8 **устройства сопряжения для карт на интегральной(ых) схеме(ах)** [integrated circuit(s) cards interface devices]: Требования и спецификации для USB-устройств, которые взаимодействуют с картами на интегральной(ых) схеме(ах) или действуют в качестве интерфейса для взаимодействия с картами на интегральной(ых) схеме(ах).

3.9 **биометрическое сравнение на идентификационной карте** (on-card comparison): Выполнение процесса биометрического сравнения и принятия решения на ICC, где хранятся данные биометрического контрольного шаблона с целью повышения безопасности и конфиденциальности.

3.10 **биометрическое сравнение вне идентификационной карты** (off-card comparison): Выполнение процесса биометрического сравнения вне идентификационной карты путем биометрической верификации с использованием биометрического контрольного шаблона, хранящегося на идентификационной карте.

3.11 **предварительные вычисления** (pre-comparison computation): Процедура расчета, выполняемая вне ICC, требующая (открытых) вспомогательных данных, хранящихся на идентификационной карте, для расчета метаданных, которые могут быть использованы для ускорения последующего процесса биометрического сравнения данных на идентификационной карте.

3.12 **распределение нагрузки** (work-sharing): Разделение вычислительной нагрузки процесса сравнения между идентификационной картой и биометрическим устройством сопряжения.

Примечание — Биометрическое сравнение на идентификационной карте с распределением нагрузки является одним из типов биометрического сравнения на идентификационной карте.

3.13 **система на идентификационной карте** (system-on-card): Система биометрической верификации на идентификационной карте, предназначенная для получения биометрических данных, их обработки и сравнения.

Примечание — Биометрическое сравнение в системе на идентификационной карте является одним из типов биометрического сравнения на идентификационной карте.

3.14 **обнуленные данные** (zeroize data): Сохраненные в электронном виде данные, которые были размагничены, стерты или перезаписаны.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

AID — идентификатор приложения (application identifier);

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

API — программный интерфейс приложения (application programming interface);

BIT — биометрический информационный шаблон (biometric information template);

---

* *Деятельность по присвоению уникальных идентификаторов биометрическим организациям, осуществляющим деятельность в Российской Федерации, и биометрическим продуктам, разрабатываемым и/или серийно выпускаемым, и/или реализуемым в Российской Федерации, а также ведение соответствующих реестров осуществляет Некоммерческое партнерство «Русское биометрическое общество», официально зарегистрированное Международной ассоциацией биометрии и идентификации [The International Biometrics & Identification Association (IBIA)] в качестве ведущей организации ЕСФОБД.*

CCID — устройства сопряжения карт на интегральной(ых) схеме(ах) [Integrated Circuit(s) Cards Interface Devices];

DIR — директория (directory);

FCP — контрольный параметр файла (file control parameter);

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

IFD — устройство сопряжения (interface device);

OID — идентификатор объекта (object Identifier);

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

SW1-SW2 — байты состояния (status bytes);

USB — универсальная последовательная шина (Universal Serial Bus);

WSR — запрос на распределение нагрузки (work-sharing request);

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

ОС — операционная система (operating system).

5 Методология испытаний

5.1 Тестовые утверждения

Тестовые утверждения предназначены для проверки соответствия заданного параметра требованиям спецификации. Если параметр не удовлетворяет критериям исходной спецификации, функция утверждения должна вернуть отрицательный результат (например, логическое значение «ложь»), указывающий, что «утверждение не выполнено», с конкретным сообщением об ошибке. В противном случае функция утверждения должна вернуть положительный результат (например, логическое значение «истина») и продолжить проводить испытания по следующему критерию. Все результаты испытаний должны быть консолидированы для формирования отчета о результатах испытания.

5.2 Критерии испытаний

Если испытуемое устройство указано как обязательное, данное устройство должно быть представлено в соответствии со спецификацией. В настоящем стандарте определены два уровня критериев испытаний содержимого/значения:

- уровень 1. Испытания содержимого/значения допускается проводить в соответствии с требованиями изготовителя;
- уровень 2. Испытания содержимого/значения допускается проводить в соответствии с требованиями/методами испытаний, указанными в настоящем стандарте.

6 Требования к испытаниям на соответствие данных, используемых для биометрического сравнения на идентификационной карте

6.1 Обработка биометрического контрольного шаблона, хранящегося на идентификационной карте

В случае испытаний обработки биометрического контрольного шаблона, хранящегося на идентификационной карте, определенной в 7.1.2, для испытаний формата биометрических данных должны быть применены требования к испытаниям на соответствие серии стандартов *ГОСТ Р ИСО/МЭК 19794*, за исключением случаев, когда для определенной рабочей среды отсутствует явное требование к проприетарному формату биометрических данных.

6.2 Данные конфигурации (для биометрической верификации)

6.2.1 Объекты данных для элементов данных конфигурации

Если данные конфигурации доступны и правило доступа, связанное с логическими структурами данных, позволяет извлечь данные конфигурации, должны быть применены требования к испытаниям, указанные в таблице 1.

Таблица 1 — Требования к испытаниям объектов данных для элементов данных конфигурации

Тег	Длина, байт	Значение	Описание	Обязательное требование	Уровень испытания	Результат испытания
'80'	От 1 до 3	Не определено	* Максимальная длина данных биометрического образца, предназначенного для биометрической верификации	Да	1	
'81'	От 1 до 3	Не определено	* Максимальная длина данных биометрического контрольного шаблона	Да	1	
'82'	1	От '00' до 'FF'	* Поддерживаемое число биометрических шаблонов ('00' — информация отсутствует)	Да	1	
'83'	1	От '00' до 'FF'	* Отметка, указывающая возможность повторной биометрической регистрации. Возможны только два значения: '00' — повторная регистрация невозможна и '01' — повторная регистрация возможна, любые другие значения зарезервированы для будущего использования и никогда не используются	Да	2	
'85'	Переменная	В соответствии с требованиями *ГОСТ Р ИСО/МЭК 29794-1*	Минимальное поддерживаемое качество биометрического образца в соответствии с требованиями, определенными в серии стандартов *ГОСТ Р ИСО/МЭК 19794, ГОСТ Р ИСО/МЭК 29794-1, ГОСТ Р ИСО/МЭК 29794-6, [1] и [2]*	Да	2	
'86'	1	Не определено	* Исходное значение счетчика повторов, указывающее максимальное поддерживаемое число разрешенных попыток биометрической верификации	Да	1	
'87'	Переменная	Не определено	Внутренние ограничения качества для выполнения сравнения. Значение зависит от конкретного приложения	Да	1	
'8F'	Переменная	Не определено	Проприетарные данные, зависящие от конкретного приложения	Нет	1	
'90'	Переменная	В соответствии с *таблицей 3 ГОСТ Р 58230—2018*	См. таблицу 3	Да	2	
'A4'	Переменная	В соответствии с требованиями регистрационного органа, определенными в *ГОСТ Р ИСО/МЭК 19785-2*	Зарезервировано для будущего использования; идентификатор алгоритма в соответствии с требованиями ИСО/МЭК СТК 1/ПК 37 «Биометрия»	Нет	1	

Примечание — «*» означает, что данный тег должен быть указан. Значение указывается изготовителем тестируемой ICC.

6.2.2 Параметры алгоритма биометрического сравнения

В таблице 2 представлены требования к испытаниям объектов данных, считываемых с идентификационной карты, закодированной в BIT.

Таблица 2 — Требования к испытаниям объектов данных для параметров алгоритмов биометрического сравнения

Тег	Длина, байт	Значение	Описание	Обязательное требование	Уровень испытания	Результат испытания
'81'	*	*	Минимальная и максимальная длина биометрических данных в соответствии с требованиями, определенными в серии стандартов *ГОСТ Р ИСО/МЭК 19794*. Содержание должно отвечать требованиям, определенным в серии стандартов *ГОСТ Р ИСО/МЭК 19794*	Да	2	
'82'	*	*	Упорядочивание последовательности, если применимо, биометрических признаков в биометрических данных в соответствии с требованиями, определенными в серии стандартов *ГОСТ Р ИСО/МЭК 19794*. Содержание должно отвечать требованиям, определенным в серии стандартов *ГОСТ Р ИСО/МЭК 19794*	Да	2	
'83'	*	*	Информация об обработке биометрических данных в соответствии с требованиями, определенными в серии стандартов *ГОСТ Р ИСО/МЭК 19794*. Содержание должно отвечать требованиям, определенным в серии стандартов *ГОСТ Р ИСО/МЭК 19794*	Да	2	
'84'	*	*	Информация о выравнивании в соответствии с требованиями, определенными в серии стандартов *ГОСТ Р ИСО/МЭК 19794*. Содержание должно отвечать требованиям, определенным в серии стандартов *ГОСТ Р ИСО/МЭК 19794*	Да	2	
'85'	**	**	Минимальное поддерживаемое качество данных биометрической верификации (см. таблицу 1). Содержание должно отвечать требованиям, определенным в серии стандартов *ГОСТ Р ИСО/МЭК 19794, ГОСТ Р ИСО/МЭК 29794-1, ГОСТ Р ИСО/МЭК 29794-6, [1] и [2]*	Да	2	
'90'	1	В соответствии с *таблицей 3 ГОСТ Р 58230—2018*	См. таблицу 3	Да	2	
'91'	2	От '0001' до 'FFFF'	Максимальное время ответа, мс. Карта, выполняющая трудоемкие операции, должна поддерживать соответствующее увеличение времени ожидания в соответствии с *ГОСТ Р ИСО/МЭК 7816-3*	Да	2	

Примечания

1 «*» означает, что значение данной переменной определено в серии стандартов *ГОСТ Р ИСО/МЭК 19794*.

2 «**» означает, что значение данной переменной определено в серии стандартов *ГОСТ Р ИСО/МЭК 19794, ГОСТ Р ИСО/МЭК 29794-1, ГОСТ Р ИСО/МЭК 29794-6, [1] и [2]*.

В таблице 3 представлены требования к испытаниям аутентификации и различающей способности, указанным в таблицах 1 и 2.

Таблица 3 — Тип аутентификации и различающая способность

b7	b6	b5	b4	b3	b2	b1	b0	Значение	Требование	Уровень испытания	Результат испытания
						x	x	Тип аутентификации	—		
						0	0	Биометрическое сравнение на идентификационной карте	* В соответствии с требованиями изготовителя	2	
						0	1	Биометрическое сравнение на идентификационной карте с распределением нагрузки	* В соответствии с требованиями изготовителя	2	
						1	0	Система на идентификационной карте	* В соответствии с требованиями изготовителя	2	
						1	1	RFU	Не используется		
			x	x	x			Требуемое значение ВЛС	—		
			0	0	0			Индикатор отсутствует	—		
			0	0	1			ВЛС уровня 1 (наибольшее)	** В соответствии с требованиями изготовителя	2	
			0	1	0			ВЛС уровня 2	** В соответствии с требованиями изготовителя	2	
			0	1	1			ВЛС уровня 3	** В соответствии с требованиями изготовителя	2	
			1	0	0			ВЛС уровня 4	** В соответствии с требованиями изготовителя	2	
			1	0	1			ВЛС уровня 5	** В соответствии с требованиями изготовителя	2	
			1	1	0			ВЛС уровня 6 (наименьшее)	** В соответствии с требованиями изготовителя	2	
			1	1	1			RFU	Не используется		
x	x	x						RFU	Не используется. Данные биты могут быть обнулены	1	

Примечания

1 «*» означает, что данные биты должны представлять операцию в соответствии с требованиями изготовителя. Например, для сравнения на идентификационной карте значения должны быть «b1» = 0 и «b0» = 1.

2 «**» означает, что данные биты должны иметь различающую способность в соответствии с требованиями изготовителя.

6.2.3 Идентификатор биометрического продукта

Идентификатор биометрического продукта должен быть целым числом в диапазоне от 1 до 65535 и должен быть зарегистрирован ригистрационным органом в соответствии с требованиями *ГОСТ Р ИСО/МЭК 19785-1*. Значение «0» не используется в качестве идентификатора.

6.3 Общий интерфейс для нескольких приложений

6.3.1 FCP

Испытания FCP должны быть проведены в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*.

6.3.2 Правила доступа

Испытания правил доступа должны быть проведены в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*.

6.4 Управление счетчиком повторов

Испытания процесса управления счетчиком повторов должны быть проведены в соответствии с таблицей 4.

Таблица 4 — Регламент проверки процесса управления счетчиком повторов

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
Счетчик повторов должен контролировать процесс биометрического сравнения держателя идентификационной карты, определяя, может ли процесс биометрической верификации продолжаться с использованием предоставленного биометрического контрольного шаблона	Да	2	
Начальное значение счетчика повторов должно быть связано с биометрическим контрольным шаблоном на идентификационной карте	Да	2	
Эта связь может быть закодирована с использованием атрибутов подклассов, присвоенных информационным объектам биометрических данных, в соответствии с требованиями *[3]*	Нет	2	
Если результат биометрической верификации отрицательный, значение счетчика повторов должно уменьшаться на единицу, а приложение должно возвратить статус ошибки, который содержит число оставшихся попыток	Да	2	
Допустимое число повторных попыток может быть закодировано в байтах состояния SW1-SW2= '63CX' (где X — оставшееся число попыток) в ответ на команду «VERIFY» («Выполнить верификацию»), в которой поле данных отсутствует в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*	Нет	1	
Положительный результат верификации биометрического контрольного шаблона должен возвращать соответствующий счетчик повторов к его начальному значению	Да	2	

7 Требования к испытаниям на соответствие стандартных процессов биометрического сравнения на идентификационной карте

7.1 Стандартные процессы

7.1.1 AID для биометрического сравнения на идентификационной карте

При реализации процесса биометрического сравнения как самостоятельного приложения AID должен быть сгенерирован в соответствии с требованиями *8.2.1.2* и *приложения А ГОСТ Р ИСО/МЭК 7816-4—2013*.

Примечание — AID извлекают из OID стандарта в соответствии с требованиями *8.2.1.2* и *приложения А ГОСТ Р ИСО/МЭК 7816-4—2013*.

7.1.2 Считывание данных биометрического контрольного шаблона

Данная операция никогда не будет поддерживаться независимо от использования конкретной команды APDU или считывания из файла.

7.1.3 Биометрическая регистрация

Данная операция должна поддерживаться. Биометрический терминал должен иметь возможность хранить биометрический контрольный шаблон в ICC с использованием механизма, указанного в *ГОСТ Р ИСО/МЭК 7816-11*. Для проверки правильности сохранения биометрического контрольного шаблона на ICC может быть использована тестовая процедура биометрической верификации.

7.1.4 Биометрическая верификация

Данная операция должна поддерживаться. Биометрический терминал должен иметь возможность передавать биометрические данные в ICC с использованием механизма, указанного в *ГОСТ Р ИСО/МЭК 7816-11*. Возвращенные байты не должны содержать результат биометрического сравнения.

7.1.5 Завершение приложения биометрического сравнения на идентификационной карте

Логическая структура данных на идентификационной карте, содержащая данные биометрического контрольного шаблона, относящиеся только к данному приложению, должна быть недоступна. Данные могут быть «обнулены» внутри карты.

7.2 Процесс биометрического сравнения и вывод результата

Процесс биометрического сравнения должен быть полностью осуществлен на идентификационной карте. Испытания проводят в соответствии со следующим регламентом:

a) для испытаний используют тестовые векторы положительных и отрицательных результатов биометрической верификации;

b) если результат биометрического сравнения данных положительный, значения SW1 и SW2 в ответе APDU на команду «VERIFY» («Выполнить верификацию») должны быть '90 00';

c) в противном случае SW1-SW2 должны содержать коды ошибки, определенные в серии стандартов *ГОСТ Р ИСО/МЭК 7816*.

8 Требования к испытаниям на соответствие механизма выполнения распределения нагрузки с использованием WSR-протокола

8.1 Биометрический контрольный шаблон для механизма распределения нагрузки

При реализации механизма распределения нагрузки биометрические данные, которые сохраняются во время биометрической регистрации, можно разделить на две части: защищенную и открытую. Защищенные данные, которые являются биометрическим контрольным шаблоном, не должны передаваться в систему биометрической верификации или IFD. Вспомогательные данные (открытые), которые содержат биометрические свойства, могут быть переданы с использованием протокола WSR для обработки биометрическим устройством сопряжения с целью уменьшения времени обработки. Защищенные данные и вспомогательные данные (открытые) должны быть закодированы внутри BIT в качестве обязательной части и проприетарной части в соответствии с требованиями *ГОСТ Р ИСО/МЭК 19794-2* и *ГОСТ Р ИСО/МЭК 7816-11*. В приложении А представлен регламент испытаний данных биометрического шаблона, использующихся для механизма распределения нагрузки.

8.2 Байты команды и ответа для распределения нагрузки

Для поддержки механизма распределения нагрузки с использованием протокола WSR ICC должна поддерживать команды и ответы APDU, определенные в *8.6 ГОСТ Р ИСО/МЭК 7816-4—2013*. Испытания поддержки ICC протокола WSR следует проводить в соответствии с регламентом, представленным в таблице 5.

Таблица 5 — Регламент проверки WSR-протокола

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
ICC должна поддерживать требования, определенные в *8.6 ГОСТ Р ИСО/МЭК 7816-4—2013*	Да	2	
ICC должна поддерживать команду «VERIFY» («Выполнить верификацию»), определенную в *5.2 ГОСТ Р ИСО/МЭК 7816-11—2013*	Да	2	
ICC должна поддерживать ответные байты '62/64 XX' для инициации механизма распределения нагрузки в соответствии с *5.1.3 ГОСТ Р ИСО/МЭК 7816-4—2013*	Да	2	

Окончание таблицы 5

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
IFD должно распознавать ответные байты '62/64 XX' для инициации механизма распределения нагрузки в соответствии с *5.1.3 ГОСТ Р ИСО/МЭК 7816-4—2013*	Да	2	
IFD должно поддерживать команду «GET DATA» («Получить данные») (00 CB 00 00 XX) для получения промежуточных данных/открытых данных шаблона с ICC для вычислений распределения нагрузки в соответствии с *7.4.2 ГОСТ Р ИСО/МЭК 7816-4—2013*	Да	2	
IFD должно поддерживать команду «PUT DATA» («Поместить данные») (00 DB 00 00 YY) для передачи вычисленных промежуточных данных в ICC в соответствии с *7.4.3 ГОСТ Р ИСО/МЭК 7816-4—2013*	Да	2	
После получения команды «PUT DATA» («Поместить данные») и промежуточных данных из IFD ICC должна иметь возможность продолжить выполнение процесса биометрического сравнения в соответствии с *7.4.3 ГОСТ Р ИСО/МЭК 7816-4—2013*	Да	2	
При необходимости дополнительных операций WSR ICC должна иметь возможность инициировать дополнительные процедуры WSR	Да	2	
После завершения процесса биометрического сравнения, если результат сравнения биометрических данных положительный, значения SW1 и SW2 в ответе APDU на команду «VERIFY» («Выполнить верификацию») должны быть '90 00'. В противном случае SW1-SW2 должны содержать коды ошибки, определенные в серии стандартов *ГОСТ Р ИСО/МЭК 7816*	Да	2	
Для проверки положительных и отрицательных результатов верификации используют тестовые векторы	Да	2	

8.3 Управление распределением нагрузки

Данный процесс следует использовать для испытаний ICC, которая поддерживает процедуру распределения нагрузки.

8.3.1 Уникальный идентификатор

В случае если ICC поддерживает управление распределением нагрузки, чтобы система биометрической верификации могла принимать запрос WSR в процессе биометрического сравнения, должен использоваться уникальный OID. Проверку управления распределением нагрузки следует проводить в соответствии с 8.3.2 и 8.3.3.

8.3.2 Исследование процедуры распределения нагрузки

Чтобы узнать о возможности реализации WSR внутри ICC с использованием уникального OID, IFD должен считать информацию из файла DIR или извлечь информацию с использованием стандартной команды «GET DATA» («Получить данные»). Для проверки поддержки механизма обнаружения должен быть использован следующий критерий. Карта должна возвращать OID в составных проприетарных данных (тег '73') внутри шаблона приложения (тег '61'), который должен считываться в файл DIR или восстанавливаться стандартной командой «GET DATA» («Получить данные»):

OID: '00' 'CB' '2F' '00' '02' '5C' '00' '00'

8.3.3 Операция процедуры распределения нагрузки

Выбор протокола WSR внутри ICC может быть обеспечен изготовителем. Для выбора протокола WSR, отвечающего требованиям *подраздела 8.1 ГОСТ Р 58230—2018*, IFD должно отправить в ICC случайную команду «ENVELOPE» («Оболочка»), содержащую OID протокола WSR. Регламент проверки операции процедуры распределения нагрузки представлен в таблице 6.

Таблица 6 — Регламент проверки операции процедуры распределения нагрузки

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
ICC должна поддерживать случайную команду «ENVELOPE» («Оболочка») в соответствии с *ГОСТ Р ИСО/МЭК 7816-4* (например, '00' 'C3' '00' '00' <Lc> '06' <Lc-2> <OID WSR протокола испытуемой ICC>)	Да	2	
Если OID, указанный в команде «ENVELOPE» («Оболочка»), совпадает с OID, зарегистрированным внутри карты, карта должна вернуть ответные байты '90' '00' о нормальной работе. После получения ответа о нормальной работе в ICC должен быть выбран указанный OID WSR-протокол. Испытания работы протокола WSR следует проводить в соответствии с 8.2	Да	2	
Если OID, указанный в команде «ENVELOPE» («Оболочка»), не совпадает с OID, зарегистрированным внутри карты, ICC должна возвращать байты ответа SW1-SW2 из ICC, содержащие коды ошибки, определенные в серии стандартов *ГОСТ Р ИСО/МЭК 7816*	Да	2	

9 Требования к испытаниям на соответствие принципов обеспечения безопасности для биометрического сравнения на идентификационной карте

9.1 Общие принципы обеспечения безопасности CSP для биометрического сравнения на идентификационной карте

Во всех случаях применяют общие принципы обеспечения безопасности, которые являются минимальными требованиями к обеспечению безопасности. Для испытания следует использовать регламент проверки, представленный в таблице 7.

Таблица 7 — Регламент проверки операции процедуры распределения нагрузки

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
Ни одно приложение не должно передавать биометрический контрольный шаблон с ICC (см. *7.2.2 ГОСТ Р 58230—2018)*	Да	2	
Для реализации механизма счетчика повторов должны быть применены принципы обеспечения безопасности, указанные в *7.1.5 ГОСТ Р 58230—2018*	Да	2	
Безопасный обмен сообщениями должен быть установлен априори для любой из операций, связанных с биометрическим контрольным шаблоном (биометрическая регистрация, повторная биометрическая регистрация и биометрическая верификация) (см. *ГОСТ Р ИСО/МЭК 7816-4*)	Да	2	
Все данные, передающиеся во время процесса биометрического сравнения на идентификационной карте, должны подтверждать свою целостность	Да	2	
Все биометрические данные, передаваемые между идентификационной картой и IFD, должны быть зашифрованы *[4]*	Да	2	
В процессе разблокировки процесса биометрического сравнения на идентификационной карте должен быть обнулен биометрический контрольный шаблон в ICC и направлен запрос для новой попытки биометрической регистрации	Нет	1	
Примечание — Данные требования определены в *ГОСТ Р 58230—2018.*			

9.2 Принципы обеспечения безопасности SP1 для глобальных данных конфигурации сравнения

В приложениях, использующих биометрический контрольный шаблон в качестве глобального механизма верификации, нет необходимости устанавливать двойную косвенность для определения конфигурации сравнения. В таблице 8 определен регламент проверки принципов обеспечения безопасности SP1.

Таблица 8 — Регламент проверки принципов обеспечения безопасности SP1 для глобальных данных конфигурации сравнения

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
Для идентификационных карт с несколькими приложениями, использующими один и тот же биометрический контрольный шаблон для биометрического сравнения на идентификационной карте, в случае если любое приложение, использующее биометрический контрольный шаблон, имеет высокий уровень безопасности, для всех приложений должен быть использован уникальный порог и единый счетчик повторов, связанный с биометрическим контрольным шаблоном (см. *7.2.8 ГОСТ Р 58230—2018)*	Да	2	
Все данные конфигурации связаны с биометрическим контрольным шаблоном. В частности: - порог биометрической верификации; - максимальное число попыток биометрической верификации; - счетчик повторов; - все параметры алгоритма сравнения	 Да Да Да Да	 2 2 2 2	
Ни одно из приложений, использующих механизм биометрического сравнения на идентификационной карте с указанным биометрическим контрольным шаблоном, не может автономно изменить данные конфигурации	Да	2	
Когда счетчик повторов достигнет нуля, механизм биометрического сравнения на идентификационной карте блокируется, и, следовательно, все приложения, использующие указанный биометрический контрольный шаблон для биометрической верификации, не смогут выполнять данные операции, защищенные механизмом биометрического сравнения на идентификационной карте	Да	2	
Положительный результат верификации биометрического контрольного шаблона сбрасывает соответствующий счетчик повторов до его начального значения независимо от того, какое из приложений осуществило успешную попытку биометрической верификации	Да	2	

9.3 Принципы обеспечения безопасности SP2 для локальных данных конфигурации сравнения

В таблице 9 определен регламент проверки принципов обеспечения безопасности SP2 для карт с приложениями, требующими независимого контроля процесса биометрического сравнения на идентификационной карте, но использующих один и тот же биометрический контрольный шаблон.

Таблица 9 — Регламент проверки принципов обеспечения безопасности SP2 для локальных данных конфигурации сравнения

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
Локальные данные конфигурации сравнения не допускаются, если приложение внутри карты квалифицируется как приложение с высоким уровнем безопасности	Да	2	

Окончание таблицы 9

Требования к испытаниям	Обязательное требование	Уровень испытания	Результат испытания
Все приложения, использующие механизм двойной косвенности, имеют собственное данные конфигурации сравнения, как минимум: - порог; - счетчик повторов	 Да Да	 2 2	
Не допускается конфигурировать приложения, обменивающиеся одними и теми же биометрическими данными, которые будут иметь разные пороги, но единый счетчик повторов	Да	2	
Использование биометрического контрольного шаблона одним приложением не должно влиять на безопасность и целостность остальных приложений, а именно: - каждый раз, когда приложение получает положительный результат верификации биометрического контрольного шаблона, только счетчик повторов данного приложения сбрасывается до его начального значения; - каждый раз, когда приложение получает отрицательный результат верификации биометрического контрольного шаблона, только счетчик повторов данного приложения будет уменьшаться на единицу; - если счетчик повторов одного из приложений достигнет нуля, только данное приложение отклоняет последующее выполнение команды «VERIFY» («Выполнить верификацию») для биометрического сравнения на идентификационной карте	 Да Да Да	 2 2 2	
Любое приложение может изменить свои данные конфигурации сравнения при необходимости, без изменения данных конфигурации сравнения других приложений, использующих тот же биометрический контрольный шаблон	Да	2	

Обобщенная архитектура испытательной установки и структура испытания приведены в приложении В.

Приложение А
(обязательное)

Регламент испытаний данных биометрического шаблона, использующихся для механизма распределения нагрузки

В таблице приведен регламент испытаний данных биометрического шаблона, использующихся для механизма распределения нагрузки.

Таблица А.1 — Биометрический шаблон, содержащий данные контрольных точек для механизма распределения нагрузки

Тег	Длина	Значение			Обязательное требование	Уровень испытания	Результат испытания
'7F2E'	Переменная	Данные биометрического шаблона				2	
		Тег	Длина	Значение		2	
		'90'	Переменная	Данные контрольных точек отпечатка пальца в соответствии с *8.1* или *8.2 ГОСТ Р ИСО/МЭК 19794-2—2013*, в зависимости от указанного владельца формата/типа формата	Да	2	
		'91'	Переменная	Данные гребневого счета в соответствии с *7.5.2.3 ГОСТ Р ИСО/МЭК 19794-2—2013*	Нет	1	
		'92'	Переменная	Данные ядра в соответствии с *7.5.3.9 ГОСТ Р ИСО/МЭК 19794-2—2013*	Нет	1	
		'93'	Переменная	Данные дельты в соответствии с *7.5.3.9 ГОСТ Р ИСО/МЭК 19794-2—2013*	Нет	1	
		'94'	Переменная	Данные качества ячейки в соответствии с *7.5.4.4 ГОСТ Р ИСО/МЭК 19794-2—2013*	Нет	1	
		'81/A1'	Переменная	Данные в стандартном формате. Если используется DO с тегом «81», данные следуют без инкапсуляции в соответствии с *8.1* или *8.2 ГОСТ Р ИСО/МЭК 19794-2—2013*	Да	2	
		'82/A2'	Переменная	Данные в проприетарном формате (промежуточные данные/открытые данные биометрического шаблона для механизма распределения нагрузки)	Да	1	

Приложение В
(справочное)

Структура испытания

В.1 Архитектура

На рисунке В.1 показана обобщенная архитектура испытательной установки. ICC, являющаяся тестируемым устройством, подключается к IFD через контактный или бесконтактный интерфейс в соответствии с *ГОСТ Р ИСО/МЭК 7816-3* и *ГОСТ Р ИСО/МЭК 14443-2* соответственно. ICC включает в себя ОС карты и приложение для биометрического сравнения на идентификационной карте. IFD с контактным или бесконтактным интерфейсом подключают к испытательному компьютеру с помощью любого стандартного протокола персонального компьютера, например USB, Xpress Card или последовательного порта. На испытательном компьютере должны быть установлены драйвера для работы с идентификационной картой и все необходимые API на уровне ОС, чтобы программное обеспечение для испытаний могло обрабатывать команду и ответ APDU. Платформа для испытаний должна состоять из компонентов, указанных на рисунке В.1, что является минимальным требованием для проведения испытаний.

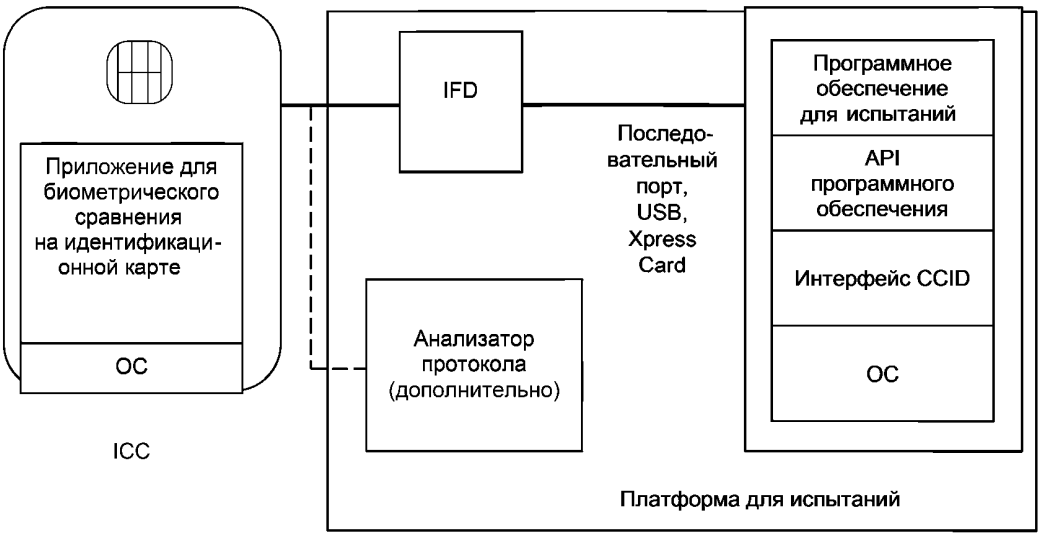

Рисунок В.1 — Обобщенная архитектура испытательной установки

В.2 Оборудование

Для настройки условий проведения испытаний должны присутствовать следующие аппаратные компоненты:

1) IFD в соответствии с *ГОСТ Р ИСО/МЭК 7816-3* (для контактной карты);

2) IFD в соответствии с *ГОСТ Р ИСО/МЭК 14443-2* (для бесконтактной карты);

3) персональный компьютер, который может быть подключен к вышеуказанным считывателям;

4) анализатор протокола APDU (дополнительно, для проверки связи между идентификационной картой и считывателем при необходимости);

5) образцы испытуемой идентификационной карты.

В.3 ОС

Любая ОС (независимо 32-разрядная или 64-разрядная) может быть использована для испытаний при условии, что для нее доступен драйвер устройства для соответствующего IFD. Необходимо принять во внимание, что для некоторых IFD не существует драйвера устройства для поддержки 64-разрядной ОС. Программное обеспечение для испытаний должно отвечать требованиям соответствующих стандартов, таким как спецификация CCID для разработки интерфейса приложения для подключения к IFD во время проведения испытаний. Более того, разработчик программного обеспечения для испытаний должен следить за порядком следования байтов (прямой или обратный), соответствующим архитектуре процессора, особенно если тестовый вектор генерируется на одной платформе, а программное обеспечение для испытаний выполняется на другой платформе с иной архитектурой процессора.

В.4 Программный интерфейс

Спецификация CCID, которая является спецификацией интерфейса для управления IFD через USB, рекомендуется для разработки программного обеспечения для испытаний отправки команды APDU и получения

ответа APDU. Для ОС Linux доступна версия спецификации CCID с открытым исходным кодом. Помимо спецификации CCID можно использовать проприетарный интерфейс. Независимо от использования спецификации CCID или проприетарного интерфейса разработчик должен гарантировать, что команда APDU, переданная функцией интерфейса, является той, которую фактически получает ICC. Если есть какие-либо сомнения относительно такой согласованности, разработчик должен использовать анализатор протоколов APDU для проверки или связаться с разработчиком IFD для разъяснения. Рекомендуется подтвердить соответствие спецификации CCID у разработчика IFD.

В.5 Язык программирования для испытаний

Функции API C/C++ доступны как в ОС Linux, так и в ОС Windows для вызова соответствующих функций спецификации CCID для управления IFD. Некоторые другие языки программирования могут предоставлять соответствующие функции API/интерфейсные функции для доступа к связанным функциям спецификации CCID. Разработчик может выбрать любой язык программирования для разработки программы для испытаний, но должен проверить синтаксис соответствующих функций для корректной передачи и получения команды и ответа APDU между персональным компьютером и идентификационной картой.

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 и межгосударственного стандартов	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»
ГОСТ ISO/IEC 19794-1	IDT	ISO/IEC 19794-1 «Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура»
ГОСТ Р ИСО/МЭК 7816-3	IDT	ISO/IEC 7816-3 «Идентификационные карты. Карты на интегральных схемах. Часть 3. Электронные сигналы и протоколы передачи»
ГОСТ Р ИСО/МЭК 7816-4—2013	IDT	ISO/IEC 7816-4:2005 «Идентификационные карты. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
ГОСТ Р ИСО/МЭК 7816-11	IDT	ISO/IEC 7816-11:2004 «Идентификационные карты. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами»
ГОСТ Р ИСО/МЭК 14443-2	IDT	ISO/IEC 14443-2 Идентификационные карты. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 2. Радиочастотный энергетический и сигнальный интерфейс»
ГОСТ Р ИСО/МЭК 19785-1	MOD	ISO/IEC 19785-1 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»
ГОСТ Р ИСО/МЭК 19785-2	IDT	ISO/IEC 19785-2 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии»
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»
ГОСТ Р ИСО/МЭК 19794-3	IDT	ISO/IEC 19794-3 «Информационные технологии. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца»
ГОСТ Р ИСО/МЭК 19794-4	IDT	ISO/IEC 19794-4 «Информационные технологии. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца»
ГОСТ Р ИСО/МЭК 19794-5	IDT	ISO/IEC 19794-5 «Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
ГОСТ Р ИСО/МЭК 19794-6	IDT	ISO/IEC 19794-6 «Информационные технологии. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
ГОСТ Р ИСО/МЭК 19794-7	IDT	ISO/IEC 19794-7 «Информационные технологии. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи»

Окончание таблицы ДА.1

Обозначение ссылочного национального и межгосударственного стандартов	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО/МЭК 19794-8	IDT	ISO/IEC 19794-8 «Информационные технологии. Форматы обмена биометрическими данными. Часть 8. Данные изображения отпечатка пальца — остов»
ГОСТ Р ИСО/МЭК 19794-9	IDT	ISO/IEC 19794-9 «Информационные технологии. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла»
ГОСТ Р ИСО/МЭК 19794-10	IDT	ISO/IEC 19794-10 «Информационные технологии. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки»
ГОСТ Р ИСО/МЭК 19794-11	IDT	ISO/IEC 19794-11 «Информационные технологии. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи»
ГОСТ Р ИСО/МЭК 19794-14	IDT	ISO/IEC 19794-14 «Информационные технологии. Форматы обмена биометрическими данными. Часть 14. Данные ДНК»
ГОСТ Р ИСО/МЭК 29794-1	IDT	ISO/IEC 29794-1:2015 «Информационные технологии. Биометрия. Качество биометрического образца. Часть 1. Структура»
ГОСТ Р ИСО/МЭК 29794-6	IDT	ISO/IEC 29794-6 «Информационные технологии. Биометрия. Качество биометрического образца. Часть 6. Данные изображения радужной оболочки глаза»
ГОСТ Р 58230—2018 (ИСО/МЭК 24787:2010)	MOD	ISO/IEC 24787:2010 «Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте»

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 международного стандарта

Таблица ДБ.1

Структура настоящего стандарта	Структура международного стандарта ИСО/МЭК 18584:2015
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственного стандартов международным стандартам, использованным в качестве ссылочных в применяемом международном стандарте	—
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного международного стандарта	—
Библиография	—
Примечание — Сопоставление структуры стандартов приведено начиная с приложения ДА, так как предыдущие разделы стандартов идентичны.	

Библиография

[1] *ISO/IEC 29794-4 Information technology — Biometric sample quality — Part 4: Finger image data (ИСО/МЭК 29794-4 Информационные технологии. Качество биометрического образца. Часть 4. Данные изображения отпечатка пальца)*

[2] *ISO/IEC TR 29794-5 Information technology — Biometric sample quality — Part 5: Face image data (ИСО/МЭК ТО 29794-5 Информационные технологии. Качество биометрического образца. Часть 5. Данные изображения лица)*

[3] *ISO/IEC 7816-15 Identification cards — Integrated circuit cards — Part 15: Cryptographic information application (ИСО/МЭК 7816-15 Идентификационные карты. Карты на интегральных схемах. Часть 15. Применение криптографической информации)*

[4] *ISO/IEC 24761 Information technology — Security techniques — Authentication context for biometrics (ИСО/МЭК 24761 Информационные технологии. Методы защиты. Контекст аутентификации для биометрии)*

УДК 336.77:002:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, идентификационная карта, требования к испытаниям, биометрическое сравнение, биометрическое сравнение на идентификационной карте, биометрия

БЗ 12—2018/7

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.И. Рычкова*
Компьютерная верстка *Д.В. Кардановской*

Сдано в набор 30.11.2018. Подписано в печать 28.12.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,60.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
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