ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58230— 2018 (ИСО/МЭК 24787: 2010)

Информационные технологии

ИДЕНТИФИКАЦИОННЫЕ КАРТЫ

Биометрическое сравнение на идентификационной карте

(ISO/IEC 24787:2010, MOD)

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным образовательным учреждением высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана) 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 АО «Ангстрем-Т» и Некоммерческого партнерства «Русское биометрическое общество»

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 сентября 2018 г. № 651-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 24787:2010 «Информационные технологии. Идентификационные карты. Биометрическое сравнение на идентификационной карте» (ISO/IEC 24787:2010 «Information technology — Identification cards — On-card biometric comparison», MOD). При этом в него не включены ссылочные международные стандарты примененного международного стандарта, которые нецелесообразно применять в российской стандартизации в связи с наличием национальных и межгосударственных стандартов, идентичных ссылочным международным стандартам. При этом дополнительные слова и ссылки, включенные в текст стандарта для учета потребностей национальной экономики Российской Федерации, выделены курсивом.

Техническая поправка к указанному международному стандарту Cor 1:2013, принятая после его официальной публикации, внесена в текст настоящего стандарта и выделена двойной вертикальной линией, расположенной на полях напротив соответствующего текста, а обозначение и год принятия технической поправки приведены в скобках после соответствующего текста.

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

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 (www.gost.ru)

Содержание

Введение

Биометрическое сравнение на идентификационной карте, определенное в *ГОСТ Р ИСО/МЭК 7816-11*, является единственным решением с использованием карт на интегральных схемах (integrated circuit cards, ICC) и биометрических технологий, обеспечивающим повышенную конфиденциальность и более безопасное биометрическое распознавание, так как процесс биометрического сравнения выполняется на ICC. В отличие от биометрического сравнения вне идентификационной карты (техническая поправка Cor 1:2013) биометрическое сравнение на идентификационной карте (техническая поправка Cor 1:2013) не требует передачи данных биометрического контрольного шаблона из ICC в устройство сопряжения. Поэтому даже в случае утери или кражи ICC данные биометрического контрольного шаблона, хранящиеся на ней, не смогут быть скопированы и останутся конфиденциальными.

ГОСТ Р ИСО/МЭК 7816-11 и нормативный документ* устанавливают требования к технологиям биометрического сравнения вне идентификационной карты (техническая поправка Cor 1:2013) и простого биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013). Самые надежные технологии биометрического сравнения, использующие биометрические образцы, полученные от реального источника, требуют высокой вычислительной мощности. В то же время, производительность процессора и другие ресурсы ICC улучшаются медленнее, так как требования низкого энергопотребления, малых размеров чипа, низкой себестоимости карт и т. д. являются препятствием для их более быстрого развития. Встраивание биометрических считывателей в ICC — по-прежнему технически сложная задача.

В результате необходимо разработать новый стандарт, устанавливающий требования к биометрическому сравнению на идентификационной карте (техническая поправка Cor 1:2013), за исключением биометрического сравнения вне идентификационной карты (техническая поправка Cor 1:2013) и биометрического сравнения в системе на идентификационной карте (техническая поправка Cor 1:2013).

Настоящий стандарт устанавливает требования и дает рекомендации:

- по описанию структуры процесса биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013);
- описанию структуры процесса биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013), что позволит уменьшить нагрузку на ICC с помощью предварительных вычислений;
- управлению значениями порогов и другим аспектам безопасности при биометрическом сравнении на идентификационной карте (техническая поправка Cor 1:2013).

* См. [1].

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ИДЕНТИФИКАЦИОННЫЕ КАРТЫ

Биометрическое сравнение на идентификационной карте

Information technology. Identification cards. On-card biometric comparison

Дата введения — 2019—01—01

1 Область применения

Настоящий стандарт устанавливает:

- требования к выполнению сравнения биометрических образцов и принятию решения на идентификационной карте;
- принципы обеспечения безопасности при биометрическом сравнении на идентификационной карте.

Настоящий стандарт также устанавливает команды и правила для проведения предварительных вычислений, выполняющихся вне идентификационной карты.

Настоящий стандарт не устанавливает требования:

- к выполнению биометрического сравнения вне идентификационной карты (техническая поправка Cor 1:2013);
- системе на идентификационной карте;
- хранению и процессу сравнения применительно к конкретным биометрическим модальностям.

2 Соответствие

Система на идентификационной карте, в которой осуществляется биометрическое сравнение (техническая поправка Cor 1:2013), соответствует настоящему стандарту, если она соответствует требованиям, указанным в 7.1.2—7.1.5, 7.2.1—7.2.8, 8.1 и 8.2.2—8.2.3.

Идентификационная карта, соответствующая требованиям настоящего стандарта, должна:

1) быть персонализирована двумя наборами данных:
- обработанные данные биометрического контрольного шаблона объекта в соответствии с 7.1.2,
- данные конфигурации для биометрического распознавания в соответствии с 7.1.3;

2) поддерживать общий интерфейс для ICC с несколькими приложениями в соответствии с 7.1.4;

3) поддерживать управление счетчиком попыток в соответствии с 7.1.5;

4) соответствовать требованиям, установленным в 7.2.1 и 7.2.8 для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013);

5) соответствовать требованиям, установленным в 8.1, 8.2.2. и 8.2.3 к распределению нагрузки.

Биометрическое распознавание может быть реализовано совместно с другими механизмами аутентификации, такими как ПИН-код. Данная реализация должна соответствовать требованиям *ГОСТ Р ИСО/МЭК 7816-4*.

Биометрические данные должны быть организованы и управляться с использованием файловой структуры или объектов данных в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4.* При этом если биометрические данные:

а) организованы с использованием файловой структуры, тогда система должна полностью соответствовать требованиям *ГОСТ Р ИСО/МЭК 7816-11*;

Издание официальное

b) организованы и управляются с использованием объектов данных, тогда идентификационная карта должна соответствовать требованиям *ГОСТ Р ИСО/МЭК 7816-4* к обработке объекта данных.

Кодирование объектов биометрических данных должно соответствовать требованиям *ГОСТ Р ИСО/МЭК 7816-11* и *нормативному документу**.

3 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37—2016 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ Р ИСО МЭК 7816-3—2013 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—2013 Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами

ГОСТ Р ИСО/МЭК 19785-1—2008 Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных

ГОСТ Р ИСО/МЭК 19785-2—2008 Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии

ГОСТ ISO/IEC 19794-1—2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура

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—2009 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-4—2014 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-5—2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ГОСТ Р ИСО/МЭК 19794-6—2014 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

ГОСТ Р ИСО/МЭК 19794-7—2009 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи

ГОСТ Р ИСО/МЭК 19794-8—2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения отпечатка пальца — остов

ГОСТ Р ИСО/МЭК 19794-9—2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла

ГОСТ Р ИСО/МЭК 19794-10—2010 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки

ГОСТ Р ИСО/МЭК 19794-11—2015 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи

ГОСТ Р ИСО/МЭК 19794-14—2017 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК

ГОСТ Р ИСО/МЭК 29794-1—2012 Информационные технологии. Биометрия. Качество биометрических образцов. Часть 1. Структура

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

* См. [1].

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.

4 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:

4.1 **вспомогательные данные** (auxiliary data): Данные, зависящие от особенностей биометрической модальности 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.

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

4.3 **установка** (installation): Запись требуемых параметров в энергонезависимую память карты на интегральной схеме (ICC) операционной системой ICC, выполняющей процедуру установки после того, как приложение загружено в ICC.

4.4 **биометрическое сравнение на идентификационной карте** (on-card biometric comparison) (техническая поправка Cor 1:2013): Выполнение процесса биометрического сравнения и принятия решения на карте на интегральной схеме, где хранятся данные биометрического контрольного шаблона, с целью повышения безопасности и конфиденциальности.

4.5 **биометрическое сравнение вне идентификационной карты** (off-card biometric comparison) (техническая поправка Cor 1:2013): Выполнение процесса биометрического сравнения вне идентификационной карты путем биометрической верификации с использованием биометрического контрольного шаблона, хранящегося на идентификационной карте.

4.6 **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.

4.7 **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 (техническая поправка Cor 1:2013) является одним из типов биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013).

4.8 **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 (техническая поправка Cor 1:2013) является одним из типов биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013).

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

5 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

AID — идентификатор приложения (application identifier);

ADF — назначенный файл приложения (application dedicated file);

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

AUT — аутентификация (authentication);

BER — базовые правила кодирования (basic encoding rules);

BIT — биометрический информационный шаблон (biometric information template);

CRT — шаблон управляющих ссылок (control reference template);

CPU — центральный процессор (central processing unit);

DF — назначенный файл (dedicated file);

DF.CIA — назначенный файл приложения для кодирования информации (dedicated file, cryptographic information application);

EF — элементарный файл (elementary file);

FCI — контрольная информация файла (file control information);

FCP — контрольный параметр файла (file control parameter);

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

MAC — код аутентификации сообщения (message authentication code);

MSE — среда безопасности (manage security environment);

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

SW1-SW2 — байты состояния (status bytes);

TLV — тег, длина, значение (tag, length, value);

WSCP — протокол вычислений распределения нагрузки (work-sharing computation protocol);

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

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

ОС — операционная система (OS, operational system).

6 Структура биометрического сравнения с использованием ICC

6.1 Общие положения

В следующих подразделах подробно описаны четыре метода распределения нагрузки при выполнении биометрического сравнения между идентификационной картой, отвечающей требованиям *ГОСТ Р ИСО/МЭК 7816-3, ГОСТ Р ИСО/МЭК 7816-4*, *ГОСТ Р ИСО/МЭК 7816-11* и системой биометрической верификации. Только 6.3 и 6.4 входят в область применения настоящего стандарта.

Для осуществления биометрической регистрации пользователь предоставляет биометрический образец для создания биометрического контрольного шаблона, после чего данные пользователя загружаются на идентификационную карту. Этот процесс не относится к биометрическому сравнению на идентификационной карте (техническая поправка Cor 1:2013), как указано в 6.5.

6.2 Биометрическое сравнение вне идентификационной карты (техническая поправка Cor 1:2013)

Биометрическое сравнение вне идентификационной карты (техническая поправка Cor 1:2013) означает, что процесс биометрической верификации проводится в системе биометрической верификации. Идентификационная карта 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 идентификационной карты для последующих транзакций. В случае отрицательного результата дальнейший доступ будет запрещен.

Шифрование обычно используют для взаимной проверки подлинности идентификационной карты и системы биометрической верификации. Для защиты процесса обмена данными между системой биометрической верификации и идентификационной картой защищенный канал должен быть создан до начала передачи любого шаблона или данных.

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.

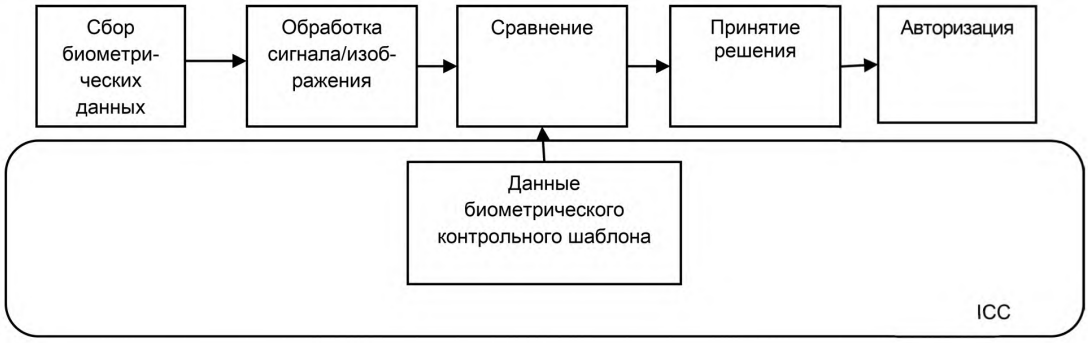


Рисунок 1 — Общая архитектура для биометрического распознавания с использованием сравнения вне идентификационной карты

6.3 Биометрическое сравнение на идентификационной карте (считыватель не встроен в карту) (техническая поправка Cor 1:2013)

Биометрическое сравнение на идентификационной карте (техническая поправка Cor 1:2013) означает, что верификация биометрического образца выполняется на идентификационной карте. Схема процесса представлена на рисунке 2. Процессор ICC должен иметь достаточную вычислительную мощность для выполнения сравнения. Процесс биометрической регистрации совпадает или аналогичен процессу биометрической регистрации при биометрическом сравнении вне идентификационной карты.

Для выполнения биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) система биометрической верификации регистрирует биометрический образец и извлекает биометрические данные. Созданные биометрические данные загружаются на идентификационную карту для выполнения биометрической верификации. При положительном результате биометрической верификации статус безопасности идентификационной карты обновляется, и соответствующий сигнал отправляется в серверную систему.

Для защиты процесса обмена данными между системой биометрической верификации и идентификационной картой рекомендуется использовать проверенный защищенный канал (с использованием безопасного обмена сообщениями в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816* и механизмами распределения функций сравнения при биометрической верификации, определенными в *нормативном документе**.

Пример — Рассмотрим идентификационную карту с возможностью создания цифровых подписей с использованием ключа, который никогда не передается с идентификационной карты. Запрос, отправленный на идентификационную карту с целью инициировать создание цифровой подписи, получает ответное сообщение об ошибке статуса безопасности. Это указывает пользователю о необходимости верификации. Пользователь предъявляет системе биометрической верификации требуемый биометрический образец для создания биометрических данных, которые передаются в ICC. ICC затем сравнивает вновь полученные биометрические данные с хранящимся биометрическим контрольным шаблоном, и в случае успешного сравнения ICC обновляет статус безопасности, что впоследствии позволяет ICC создавать цифровую подпись при получении соответствующих команд APDU.

* См. [2].

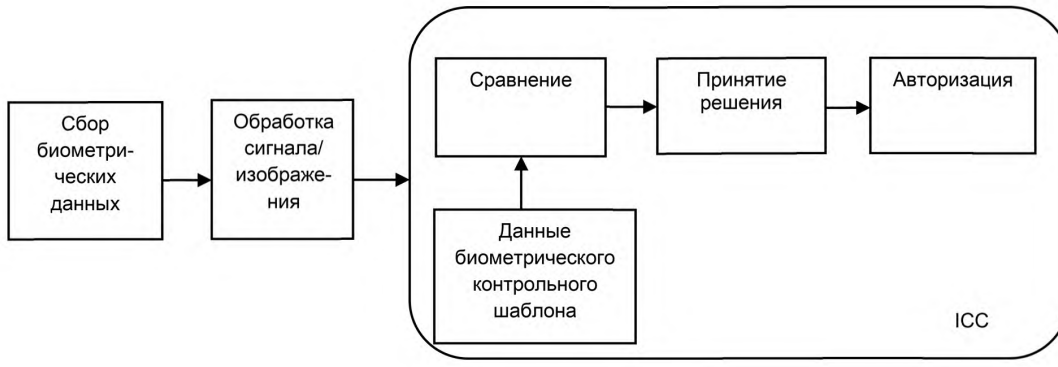


Рисунок 2 — Общая архитектура для биометрического распознавания с использованием сравнения на идентификационной карте

6.4 Биометрическое сравнение на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013)

Биометрическое сравнение на идентификационной карте с распределением нагрузки аналогично биометрическому сравнению на идентификационной карте за исключением процедуры сравнения. Схема процесса представлена на рисунке 3. Данный способ сравнения предназначен для использования с ICC, которые не обладают достаточными вычислительными возможностями для выполнения сравнения биометрических данных. В этом случае некоторые функции, которые требуют достаточно больших вычислительных мощностей, например математические преобразования, передаются системе биометрической верификации для выполнения расчетов. Результат вычислений возвращается в ICC, таким образом, окончательное решение о результате сравнения принимается на карте. В ходе предварительных вычислений происходит обмен данными между идентификационной картой и системой биометрической верификации. Для защиты связи между терминалом и идентификационной картой используется проверенный защищенный канал до тех пор, пока потребность в такой защите отпадает для определенной рабочей среды. Окончательное сравнение производится на идентификационной карте. Подробное описание схемы распределения нагрузки приведено в приложении А.

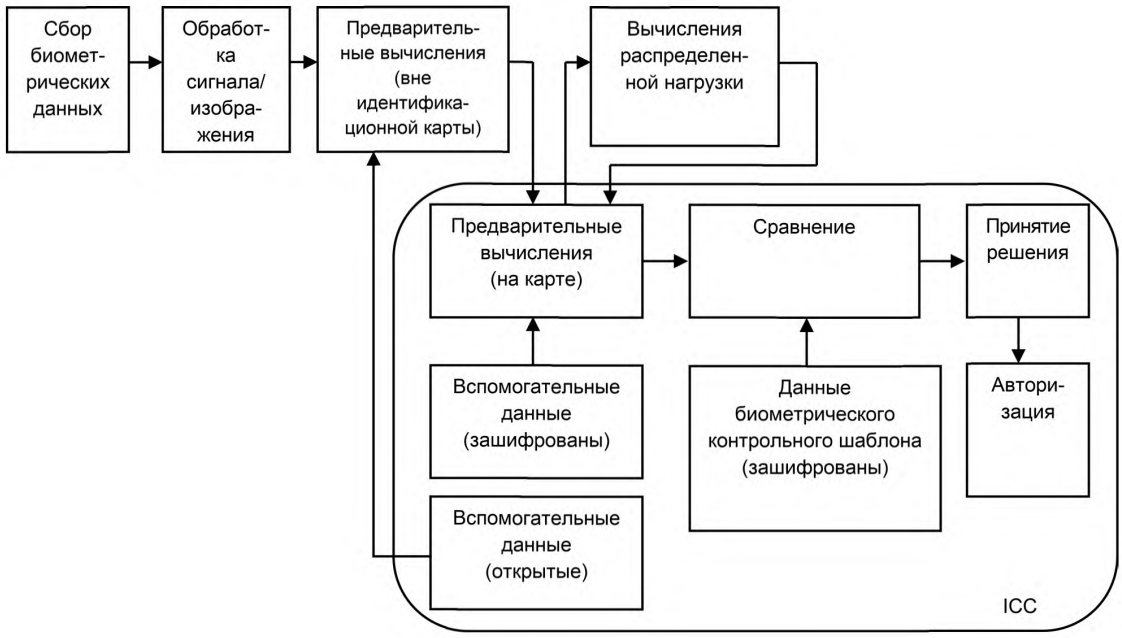


Рисунок 3 — Общая архитектура для биометрического распознавания с распределением нагрузки

Примечание — Биометрическое сравнение на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013) должно использоваться только в том случае, когда для используемой биометрической модальности выполнение процесса биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) не отвечает требованиям затрачиваемого времени транзакции для данного приложения.

6.5 Биометрическое сравнение в системе на идентификационной карте (техническая поправка Cor 1:2013)

Биометрическое сравнение в системе на идентификационной карте (техническая поправка Cor 1:2013) включает весь процесс верификации биометрического образца, выполняемый на идентификационной карте. Схема процесса представлена на рисунке 4. Для выполнения биометрического сравнения сканер, встроенный в идентификационную карту, регистрирует биометрический образец и извлекает биометрические данные. Полученные биометрические данные затем используются для биометрической верификации. Процесс биометрической верификации выполняется на идентификационной карте. Статус безопасности идентификационной карты обновляется один раз после окончания биометрической верификации. Биометрический образец или данные биометрического контрольного шаблона не передаются с идентификационной карты или на нее.

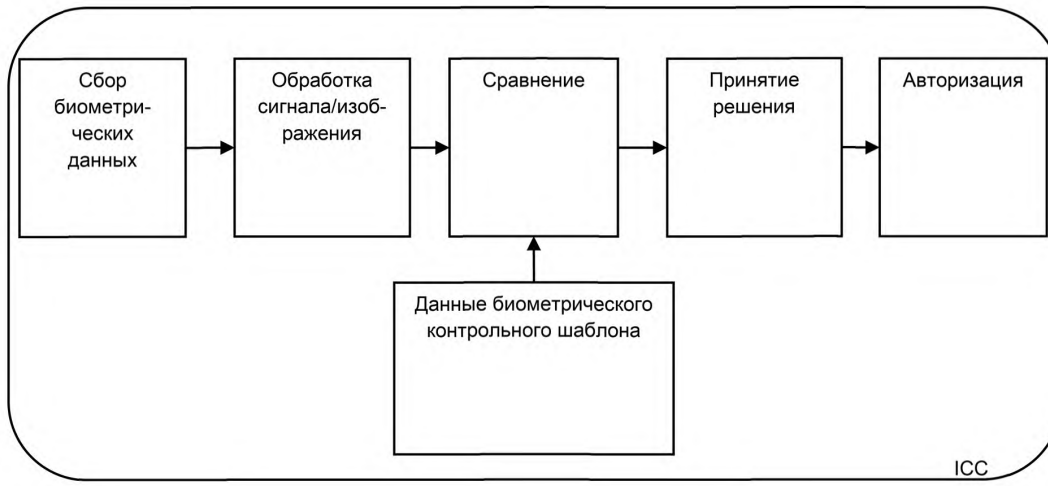


Рисунок 4 — Общая архитектура для биометрического распознавания с использованием сравнения на идентификационной карте

7 Общая структура приложений биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

7.1 Данные для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

7.1.1 Общие положения

В 7.1.2—7.1.5 установлены требования:

- к обработке данных биометрического контрольного шаблона;
- данным конфигурации для биометрической верификации;
- общему интерфейсу для нескольких приложений;
- управлению счетчиком повторов.

7.1.2 Обработка данных биометрического контрольного шаблона

С целью обеспечения совместимости данных биометрического контрольного шаблона для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) следует использовать биометрические данные в формате, определенном в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*. Пример приведен в приложении В.

В том случае если требования к совместимости данных биометрического контрольного шаблона отсутствуют для определенной рабочей среды, следует использовать биометрические данные в формате, определенном в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*.

Примечание — Рекомендуется использовать форматы обмена биометрическими данными, определенные в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*.

7.1.3 Данные конфигурации для биометрической верификации

7.1.3.1 Объекты данных для данных конфигурации

Данные конфигурации для биометрической верификации состоят из набора объектов данных, описанных в таблице 1. Для извлечения данных конфигурации используют правила доступа, связанные с логическими структурами данных, которые хранят эту информацию. Если данные конфигурации доступны, они хранятся в шаблоне биометрической информации (BIT) (см. *ГОСТ Р ИСО/МЭК 7816-11*). Эти данные конфигурации должны быть закодированы при наличии тега 'B1' BIT (см. *ГОСТ Р ИСО/МЭК 7816-11*), как показано в таблице 1.

Таблица 1 — Объекты данных для элементов данных конфигурации

Тег	Длина	Значение	Описание
'80'	От '01' до '03'		Максимальная длина данных биометрической верификации
'81'	От '01' до '03'		Максимальная длина данных биометрического контрольного шаблона
'82'	1	От '00' до 'FF'	Поддерживаемое число биометрических образцов ('00' — информация отсутствует)
'83'	1	'00': Повторная регистрация невозможна '01': Повторная регистрация возможна RFU: Другие значения	Отметка, указывающая возможность повторной биометрической регистрации
'85'	Переменная	В соответствии с требованиями *ГОСТ Р ИСО/МЭК 29794-1*	Минимальное поддерживаемое качество данных биометрической верификации в соответствии с требованиями, определенными в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794* и *ГОСТ Р ИСО/МЭК 29794*
'86'	1		Исходное значение счетчика повторов, указывающее максимальное поддерживаемое число разрешенных попыток биометрической верификации
'87'	Переменная		Внутренние ограничения качества для выполнения сравнения
'8F'	Переменная		Проприетарные данные
'90'	Переменная	См. таблицу 3 (техническая поправка Cor 1:2013)	Типы биометрического распознавания и, если применимо, представления идентификационной карты
'A4'	2	В соответствии с требованиями регистрирующего 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»
Примечание — Кодирование других параметров конфигурации, таких как: - требуемый статус безопасности для выполнения биометрической верификации; - требуемый статус безопасности для выполнения биометрической регистрации; - установка статуса безопасности после положительной верификации выходит за рамки настоящего стандарта.			

7.1.3.2 Параметры алгоритма биометрического сравнения

Перед выполнением биометрической верификации необходимо считать с идентификационной карты набор параметров биометрического сравнения. В таблицах 2 и 3 представлены параметры алгоритмов биометрического сравнения, хранящиеся в BIT, для выполнения биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) (тег '91'/'B1' в соответствии с *нормативным документом**), где первичные параметры обозначены тегом '91', а полученные параметры — тегом 'B1' и включают общую длину.

* См. [1].

Таблица 2 — Объекты данных для параметров алгоритма биометрического сравнения

Тег	Длина	Значение	Описание
'81'	*	*	Минимальная и максимальная длина биометрических данных в соответствии с требованиями, определенными в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*
'82'	*	*	Упорядочивание последовательности, если применимо, биометрических признаков в биометрических данных в соответствии с требованиями, определенными в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*
'83'	*	*	Индикатор обработки признака в соответствии с требованиями, определенными в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794* (техническая поправка Cor 1:2013)
'84'	*	*	Информация об ориентации в соответствии с требованиями, определенными в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*
'85'	**	**	Минимальное поддерживаемое качество данных биометрической верификации (см. таблицу 1)
'90'	1	См. таблицу 3 (техническая поправка Cor 1:2013)	Тип аутентификации и устойчивость алгоритма
'91'	2	От '0001' до 'FFFF'	Максимальное время ответа, мс[1)]

[1)] Карта, выполняющая трудоемкие операции, должна поддерживать соответствующее увеличение времени ожидания в соответствии с *ГОСТ Р ИСО/МЭК 7816-3*.

Примечания

1 * означает, что значение данной переменной определяется в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794*.

2 ** означает, что значение данной переменной определяется в комплексе стандартов *ГОСТ Р ИСО/МЭК 19794* и *ГОСТ Р ИСО/МЭК 29794*.

Биометрическое сравнение на идентификационной карте (техническая поправка Cor 1:2013) может потребовать выполнения правил доступа, включая использование любого защищенного канала для защиты процесса обмена командами и ответами APDU, необходимыми для завершения процесса. Поле данных APDU, передающего биометрические данные на идентификационную карту или из нее, должно быть закодировано в соответствии с требованиями настоящего стандарта. Правила доступа и безопасный обмен сообщениями, использующиеся для защиты APDU, должны соответствовать требованиям *ГОСТ Р ИСО/МЭК 7816-4*.

Таблица 3 — Тип аутентификации и дискриминирующая способность

b7	b6	b5	b4	b3	b2	b1	b0	Значение
—	—	—	—	—	—	x	x	Тип аутентификации
—	—	—	—	—	—	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[1)]
—	—	—	0	0	0	—	—	Индикатор отсутствует

Окончание таблицы 3

b7	b6	b5	b4	b3	b2	b1	b0	Значение
—	—	—	0	0	1	—	—	ВЛС уровня 1 (наибольшее)
—	—	—	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 (наименьшее)
—	—	—	1	1	1	—	—	RFU
x	x	x	—	—	—	—	—	RFU
[1)] Данный параметр позволяет создателю системы устанавливать различные уровни сравнения для различных приложений с конкретными продуктами, использующими биометрическое сравнение на идентификационной карте (техническая поправка Cor 1:2013).								

Разработчик должен указывать значение ВЛС в соответствии с установленной градацией. В таблице 4 приведен пример градации ВЛС.

Таблица 4 — Пример градации ВЛС

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

7.1.3.3 Идентификатор биометрического продукта

Идентификатор биометрического продукта должен быть целым числом в диапазоне от 1 до 65535 и должен быть зарегистрирован в регистрирующем органе в соответствии с требованиями *ГОСТ Р ИСО/МЭК 19785-1*.

7.1.4 Общий интерфейс для нескольких приложений

7.1.4.1 Общие положения

Допустимым требованием к разнородной системе биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) является использование одного и того же биометрического контрольного шаблона, например шаблона контрольных точек, для различных приложений с использованием различных данных конфигурации. Данное требование реализовано с помощью указателей правил доступа и элементов данных, определенных в *ГОСТ Р ИСО/МЭК 7816-3, ГОСТ Р ИСО/МЭК 7816-4, ГОСТ Р ИСО/МЭК 7816-11* и других биометрических стандартах, определяющих требования к обмену информацией между независимыми приложениями.

Система биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) может потребовать дополнительные параметры, например:

- указатель биометрического контрольного шаблона;
- параметры сравнения, например:
  - формат шаблона,
  - используемый алгоритм,
  - параметры пороговых значений.

Система может определить наибольший результат сравнения или вернуть положительный результат сравнения, как только будет достигнут принятый порог (техническая поправка Cor 1:2013).

Эта связь «один-к-одному» между параметрами и ключевыми числами определена в приложении С. Таким образом, можно связать параметры с ключевым числом.

7.1.4.2 Контрольный параметр файла

Контрольный параметр файла FCP, указанный в таблицах С.1—С.3 приложения С, в соответствии с *ГОСТ Р ИСО/МЭК 7816-4* должен быть обязательным для каждого назначенного файла приложения ADF, назначенного файла DF или элементарного файла EF в идентификационной карте. В зависимости от параметров команд FCP должен быть возвращен после успешного выполнения команды «SELECT» («ВЫБРАТЬ») APDU. FCP включает указатели правила доступа в соответствии с 7.1.4.3. В таблицах в приложении С приведена обобщенная структура TLV FCI для DF или EF.

7.1.4.3 Правила доступа

Правила доступа должны определять, какие условия безопасности SC должны быть выполнены для получения доступа к защищенным ресурсам карты для определенного режима доступа. Правило доступа «NEVER» («Никогда») должно быть связано со считыванием биометрического контрольного шаблона. Для идентификационных карт, совместимых с настоящим стандартом, правила доступа должны быть закодированы в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4* путем назначения условий безопасности для режимов доступа защиты логических структур данных идентификационной карты. В момент выполнения этих условий безопасности стороннее приложение получит статус безопасности, требуемый для получения доступа к защищенной структуре данных для данного режима доступа.

Примечание — Правило доступа «NEVER» («Никогда») определено в *таблицах 20 и 23 ГОСТ Р ИСО/МЭК 7816-4—2013*.

При кодировании правил доступа в идентификационной карте в соответствии с требованиями настоящего стандарта применяются правила, приведенные ниже.

Правила доступа могут быть связаны с любым ADF, DF и EF, а также с защищенными объектами данных.

Для приложения биометрического сравнения на идентификационной карте FCP, связанный с ADF, хранящим приложение, может кодировать правила доступа для выполнения биометрического сравнения на идентификационной карте.

Для любого другого приложения, размещенного на карте, правила доступа могут содержать ссылку на шаблон управляющих ссылок аутентификации (CRT AUT), хранящий шаблон биометрической информации объекта данных "7F60" согласно *ГОСТ Р ИСО/МЭК 7816-11*.

При необходимости передачи BIT процедура должна быть защищена с помощью безопасного обмена сообщениями в соответствии с *ГОСТ Р ИСО/МЭК 7816-11*.

Примечание — Правила доступа определены в *ГОСТ Р ИСО/МЭК 7816-4*.

7.1.4.4 Двойная косвенность

Двойная косвенность является необязательным функционалом, который идентификационная карта, соответствующая требованиям настоящего стандарта, может обеспечить только в том случае, когда она не поддерживает приложения с более высоким уровнем безопасности в соответствии с 7.2.8 и требованиями приложения D. Под двойной косвенностью понимается возможность переходить на биометрическое сравнение на идентификационной карте с использованием различных конфигураций, установленных соответствующими различными правилами доступа.

ГОСТ Р ИСО/МЭК 7816-4 предлагает различные возможности для спецификации правил доступа, которые могут применяться для реализации функционала двойной косвенности, обеспечивающей взаимодействие. Таким образом, правило доступа кодирует [в формате идентификационной карты или записи в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4* (техническая поправка Cor 1:2013)] связь, возникающую между режимами доступа для команд, связанных с биометрическим контрольным шаблоном и требуемыми условиями безопасности, которые должны быть выполнены. В соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4* эти условия безопасности могут передаваться среде безопасности приложения с шаблоном управляющих ссылок аутентификации. Этот механизм позволяет различным приложениям устанавливать различные правила доступа для процессов биометрической верификации с одинаковым биометрическим контрольным шаблоном.

На рисунке 5 приведен пример распределения конфигураций и биометрических контрольных шаблонов.

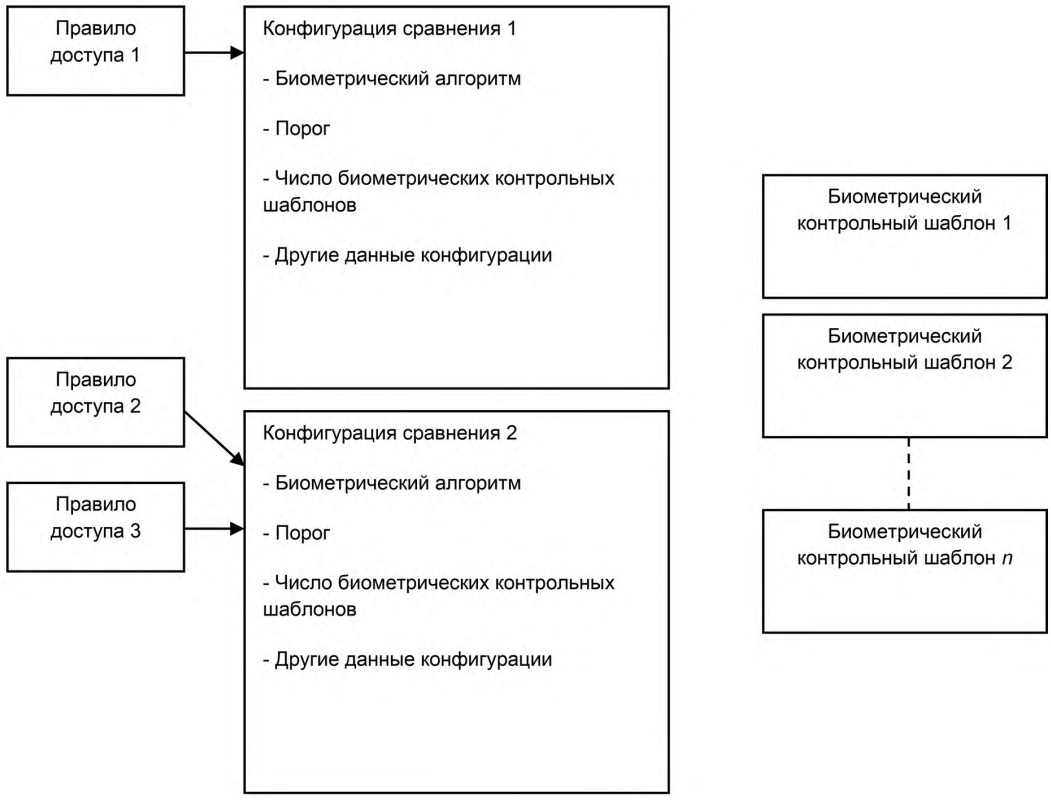


Рисунок 5 — Пример распределения конфигураций и биометрических контрольных шаблонов
(техническая поправка Cor 1:2013)

7.1.4.5 Использование среды безопасности

Номер ключа, используемый в MSE в режиме SET, определяет:

- шаблон ссылок;
- уровень безопасности.

В *ГОСТ Р ИСО/МЭК 7816-4* определены требования к квалификатору применимости для биометрического распознавания (‘04’, см. *таблицу 35 ГОСТ Р ИСО/МЭК 7816-4–2013*).

Последовательность выполнения биометрического сравнения приведена в *приложении В ГОСТ Р ИСО/МЭК 7816-11—2013* (см. рисунок 6, совпадающий с *рисунком В.6 ГОСТ Р ИСО/МЭК 7816-11—2013*).

Команда/Ответ	Значение
SELECT <ID файла> → ОК ←	Выбор расширенного файла FCI
READ BINARY → VIT || BIT ←	Извлечение шаблона информации о требованиях к верификации VIT и BIT
MANAGE SE <DO UQ || DO Ссылка на алгоритм || DO Ссылка на ключ> → ОК ←	Установление CRT AT с квалификатором применимости UQ, ссылки на алгоритм и ссылки на ключ
VERIFY <Данные биометрической верификации> → ОК ←	Верификация пользователя

Рисунок 6 — Команды для верификации без использования безопасного обмена сообщениями (пример)

Однако в *ГОСТ Р ИСО/МЭК 7816-11* не определено, каким образом биометрический контрольный шаблон и параметры сравнения хранятся внутри идентификационной карты, так как полностью не определен процесс биометрической регистрации.

В *таблице 33 ГОСТ Р ИСО/МЭК 7816-4—2013* перечислены следующие объекты данных:

- '80' ссылка на криптографический механизм;
- ссылки на файл и ключ:
  - '81' — ссылка на файл [то же кодирование, что и в *ГОСТ Р ИСО/МЭК 7816-4—2013 (5.3.1.2)*],
  - '82' — имя DF [см. *ГОСТ Р ИСО/МЭК 7816-4—2013 (5.3.1.1)*],
  - '83' — ссылка на секретный ключ (для прямого использования):
  - ссылка на открытый ключ,
  - квалификатор эталонных данных,
- '84' — ссылка на вычисление ключа сеанса:
  - ссылка на закрытый ключ,
  - 'A3' — шаблон применимости ключа (см. *ГОСТ Р ИСО/МЭК 7816-4*);
  - ссылка на исходные данные: не применимо.

7.1.5 Управление счетчиком повторов

Управление счетчиком повторов определяет политику управления механизмами счетчика повторов. Установлены следующие принципы управления:

a) счетчик повторов должен контролировать процесс биометрического сравнения держателя идентификационной карты, определяя, может ли процесс верификации продолжаться с использованием предоставленного биометрического контрольного шаблона;

b) начальное значение счетчика повторов должно быть связано с биометрическим контрольным шаблоном на идентификационной карте;

c) эта связь может быть закодирована с использованием атрибутов подклассов, присвоенных информационным объектам биометрических данных, в соответствии с требованиями *нормативного документа**;

d) если результат верификации отрицательный, значение счетчика повторов должно уменьшаться на единицу, а приложение — возвратить статус ошибки, который содержит количество оставшихся попыток;

* См. [3].

e) допустимое количество повторных попыток может быть закодировано в байтах состояния SW1-SW2 = “63CX” (где X — оставшееся количество попыток) в ответ на команду «VERIFY» («Выполнить верификацию»), в которой поле данных отсутствует в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*;

f) положительный результат верификации биометрического контрольного шаблона должен возвращать соответствующий счетчик повторов к его начальному значению.

7.2 Стандартный порядок биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

7.2.1 AID для биометрического сравнения на идентификационной карте

Идентификационная карта должна поддерживать AID. При выполнении биометрического сравнения на идентификационной карте как самостоятельного приложения это приложение должно быть идентифицировано с помощью AID в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*. Приложение биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) может быть выбрано при помощи AID ‘E8 28 81 C1 53 00’.

Примечание — AID извлекают из идентификатора объекта в соответствии с *8.2.1.2 и приложением А ГОСТ Р ИСО/МЭК 7816-4—2013*.

7.2.2 Считывание данных биометрического контрольного шаблона

В приложении биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) не производится считывание биометрического контрольного шаблона для использования в процессе сравнения. Вспомогательные данные (открытые), связанные с биометрическим контрольным шаблоном, могут быть считаны в соответствии с потребностями приложения.

7.2.3 Биометрическая регистрация

Биометрическая регистрация представляет собой процесс, посредством которого создается и сохраняется биометрический контрольный шаблон. В системах биометрического сравнения на идентификационных картах (техническая поправка Cor 1:2013) данный процесс включает в себя:

1) передачу одного или более биометрических шаблонов в ICC и их хранение в ней;

2) передачу и хранение других параметров, необходимых для выполнения процесса биометрического сравнения (например, порог сравнения, параметры обеспечения качества и т. д.).

В зависимости от возможностей ICC обработка сигнала может быть распределена между биометрическим устройством сопряжения и ICC. Во всех случаях все биометрические данные передаются на идентификационную карту с использованием проверенного защищенного канала или проверенной среды, гарантирующих конфиденциальность пользователей. Рекомендуется выполнять тестовую попытку биометрической верификации после биометрической регистрации для проверки качества процесса.

Руководство по записи биометрических данных на идентификационную карту содержится в *ГОСТ Р ИСО/МЭК 7816-11*.

Для обновления биометрических данных пользователя может потребоваться повторная биометрическая регистрация. В этом случае должны применять правила для процесса биометрической регистрации.

7.2.4 Биометрическая верификация

Процесс биометрической верификации представляет собой сравнение биометрических данных с биометрическим контрольным шаблоном. В системе биометрического сравнения на идентификационной карте процесс сравнения производится в ICC. Биометрический контрольный шаблон может включать в себя множество попыток биометрической регистрации, например несколько отпечатков одного человека или различные модальности, такие как радужная оболочка глаза и лицо.

Биометрическое сравнение требует условий доступа, определенных в структуре файла приложения. Данные условия должны быть по возможности выполнены путем взаимной или внешней аутентификации, как определено в структуре файла приложения. В соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4* для передачи на идентификационную карту биометрических данных для процесса биометрической верификации должен использоваться безопасный обмен сообщениями.

Команду «VERIFY» («Выполнить верификацию») в соответствии с *ГОСТ Р ИСО/МЭК 7816-4* применяют для инициирования процесса биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013). Если результат сравнения положительный, то статус безопасности карты может быть установлен в соответствии с условиями доступа. Во избежание атак можно использовать счетчик повторов, если только необходимость таких мер явно не установлена для определенной рабо-

чей среды. Если результат сравнения отрицательный, значение счетчика повторов должно быть уменьшено и может быть возвращено в статусе биометрической верификации. Если счетчик повторов достигнет нуля, дальнейшие попытки биометрической верификации должны быть заблокированы. Счетчик повторов может быть сброшен с помощью методов разблокирования, описанных в *ГОСТ Р ИСО/МЭК 7816-4*.

7.2.5 Завершение приложения биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

При завершении приложения биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) логическая структура данных, содержащая данные биометрического контрольного шаблона, относящиеся только к данному приложению, должна быть недоступна. Возможный способ решения — это «обнуление» данных.

7.2.6 Процесс биометрического сравнения и вывод результата

7.2.6.1 Процесс биометрического сравнения

Процесс биометрического сравнения полностью осуществляется на идентификационной карте.

7.2.6.2 Результат биометрического сравнения

Результат биометрического сравнения представляет собой результат сравнения представленных биометрических данных и заданного порога для достижения требуемого уровня безопасности. Если степень схожести превышает заданный порог, значение SW1-SW2 в ответе APDU на команду «VERIFY» («Выполнить верификацию») должно быть '90 00'. В противном случае SW1-SW2 должны содержать код ошибки, определенный в *ГОСТ Р ИСО/МЭК 7816-11*.

7.2.7 Требования безопасности и управление биометрическими контрольными шаблонами

Требования безопасности и политика управления биометрическими контрольными шаблонами устанавливают, что:

a) условия безопасного доступа к биометрическому контрольному шаблону не должны позволять считывать данные с использованием любой команды;

b) для обновления данных биометрического контрольного шаблона применяют правила, используемые при биометрической регистрации;

c) биометрическую верификацию проводят только при заданном статусе безопасности;

d) независимый счетчик повторов может существовать для каждой ссылки на хранимый биометрический контрольный шаблон;

e) счетчики повторов для различных приложений могут быть независимыми. Это означает, что, если один счетчик повторов достиг нулевого значения, счетчики повторов для других приложений, ссылающихся на те же биометрические данные, остаются неизменными.

Рекомендации для механизмов обеспечения безопасности при биометрическом сравнении на идентификационной карте приведены в приложении E.

Примеры реализации механизмов биометрического сравнения на идентификационной карте приведены в приложении F.

7.2.8 Управление пороговым значением

Управление пороговым значением определяет политику управления пороговыми значениями и соответствующих механизмов. Рекомендуется соблюдать следующие правила:

a) если идентификационная карта имеет несколько приложений биометрического сравнения на идентификационной карте, использующих один и тот же биометрический контрольный шаблон, тогда для этих приложений используются единые значение порога и счетчик повторов.

Примечание — Настоящий стандарт признает, что при внедрении технологии или по коммерческим причинам может существовать необходимость в различных пороговых значениях для одного и того же биометрического контрольного шаблона. В таком случае руководствуются принципами, приведенными в приложении D настоящего стандарта, в частности SP2;

b) данные конфигурации должны определять параметр для внутренних ограничений качества для выполнения процесса сравнения во время 1-й установки приложения биометрического распознавания на идентификационной карте;

c) правило доступа для двойной косвенности, особенно в контексте различных конфигураций, в частности порога сравнения, должно быть определено на этапе установки приложений;

d) для того чтобы определить подлинность при выполнении процесса верификации, должны быть приняты во внимание следующие параметры, как указано в 7.1.3.2:

i) параметры алгоритма биометрического сравнения,

ii) тип аутентификации и дискриминирующая способность;

e) уровни безопасности, которые могут быть достигнуты в результате положительной биометрической верификации, должны быть получены из данных конфигурации. Основное устройство должно выбрать уровень безопасности, который требуется приложению, перед началом биометрической верификации;

f) параметры пороговых значений, описанные в данном пункте, не подлежат изменению во время процесса биометрической верификации на идентификационной карте.

8 Распределение нагрузки

8.1 Механизм выполнения распределения нагрузки с использованием протокола WSR

При реализации биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) с распределением нагрузки процесс сравнения осуществляется на ICC. Предварительные вычисления могут полностью или частично выполнять в системе биометрической верификации, в зависимости от реализации конкретной системы биометрической верификации в ICC. Команда «ENVELOPE» («Оболочка»), как описано в 8.2.2 и 8.2.3, может быть использована для определения, доступен ли поддерживаемый протокол WSR. Как описано в 6.4, в ICC хранится две части биометрических данных. Защищенные данные, которые являются биометрическим контрольным шаблоном, не передаются системе биометрической верификации. Вспомогательные данные (открытые), которые содержат биометрические признаки, могут быть переданы с использованием протокола WSR для обработки биометрическим устройством сопряжения, с целью ускорения времени обработки. Данный механизм может быть реализован как для предварительных вычислений, так и для распределения нагрузки во время выполнения процесса верификации. Пример схемы распределения нагрузки описан в приложении G. *На рисунке G.1 приведена блок-схема биометрического сравнения на идентификационной карте с распределением нагрузки*. На рисунке G.2 показан механизм распределения нагрузки в соответствии с рисунком 3. Рисунок G.2 не может быть применен для других схем распределения нагрузки. Команды и ответы APDU, определенные в *8.6 ГОСТ Р ИСО/МЭК 7816-4—2013*, следует использовать для поддержки протокола WSR. Карта может отправить несколько запросов WSR в один отдел APDU локальной системы биометрической верификации. Перед обращением к функции WSR соответствующие данные для расчетов должны быть переданы в буфер APDU. На рисунке 7 числа, приведенные в скобках рядом со стрелками, указывают последовательность действий. Когда протокол WSR установлен (см. 8.2.2) или выбран (см. 8.2.3), действия происходят в следующей последовательности:

1) идентификационная карта получает команду для биометрического сравнения, требующую WSR, и запускает выполнение WSR на идентификационной карте;

2) операционная система (ОС) идентификационной карты должна вернуть ответные байты “62 *XX*” системе биометрической верификации, что указывает, что идентификационная карта подтверждает выполнение запроса WSR в соответствии с шагом 1). У идентификационной карты есть запрос из «*XX*» байтов, которые система биометрической верификации должна извлечь и на которые идентификационная карта ожидает получить ответ;

3) и 4) после того, как система биометрической верификации получает байты “62 *XX*”, система биометрической верификации должна отправить команду «GET DATA» («Получить данные») (00 CB 00 00 *XX*) на идентификационную карту для получения промежуточных данных с идентификационной карты. Для извлечения запроса из «*XX*» байтов, доступных на идентификационной карте, устройство сопряжения должно отправить команду «GET DATA» («Получить данные») с байтами P1-P2, установленными на ‘0000’, и полем Le, установленным на «*XX*». Если есть необходимость передать данные до их получения от внешнего устройства, идентификационная карта должна направить команду SW1-SW2 = 62 *XY* и возобновить выполнение шага 3) и 4);

5) после того как система биометрической верификации завершила выполнение обработки промежуточных данных, устройство должно передать обработанные данные на идентификационную карту. Чтобы продолжить процесс биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) система биометрической верификации должна использовать команду «PUT DATA» («Поместить данные») (00 DB 00 00 *YY* ...) для передачи обработанных данных на идентификационную карту. Устройство сопряжения должно отправить команду «PUT DATA» («Поместить данные») с байтами P1-P2, установленными на ‘0000’, и полем Lc, установленным на «*YY*». Если внешнее устройство

еще не передало все данные, то команды «PUT DATA» («Поместить данные») должны быть объединены в цепочку, и выполнение шага 5 должно быть возобновлено;

6) если у идентификационной карты все еще есть необходимость в WSR, ОС идентификационной карты возобновляет выполнение функции биометрического сравнения на шаге 2). Если такой необходимости нет, то идентификационная карта должна ответить с применением SW1-SW2, которые являются ответом на команду для биометрического сравнения, полученную на шаге 1).

В приложении Н определена диаграмма состояния протокола WSR.

XX — это число байтов промежуточных данных, переданных в систему биометрической верификации, а *YY* — это число возвращенных байтов обработанных данных, переданных на идентификационную карту.

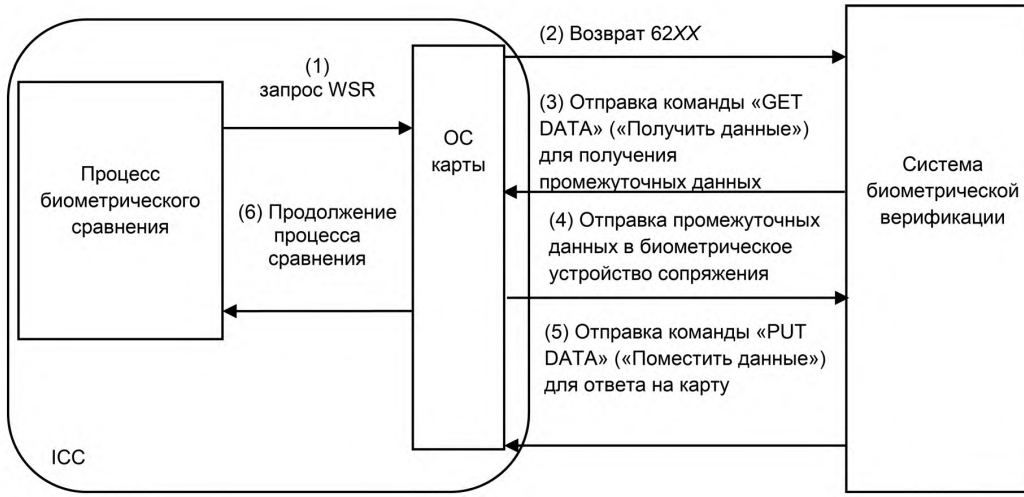


Рисунок 7 — Механизм WSR

8.2 Управление распределением нагрузки

8.2.1 Общие положения

Приложениям биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013) могут потребоваться процедуры управления, чтобы оповестить систему биометрической верификации о возможности реализации протокола WSR и однозначно ссылаться на данный протокол WSR. В этом случае должен использоваться уникальный идентификатор объекта, чтобы система биометрической верификации могла принять запрос WSR в процессе биометрического сравнения. Следовательно, спецификация должна быть достаточно точной, чтобы обеспечить реализацию протокола WSR, принадлежащего дереву идентификатора объекта, что означает, что спецификация имеет уникальный идентификатор объекта.

8.2.2 Процедура распределения нагрузки

Поддержка конкретного протокола WSR в сочетании с приложением, требующим биометрического распознавания на идентификационной карте, может быть указана путем инкапсуляции идентификатора объекта в составные проприетарные данные (тег ‘73’) внутри шаблона приложения (тег ‘61’), который должен считываться в файл DIR или восстанавливаться командой «GET DATA» («Получить данные»); на канале 0 она должна быть:

‘00’ ‘CB’ ‘2F’ ‘00’ ‘02’ ‘5C’ ‘00’ ‘00’.

Примечание — В *нормативном документе** этот вид кодирования информации применяют для различных целей.

* См. [3].

8.2.3 Порядок действия при распределении нагрузки

Приложение, требующее биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013), должно быть выбрано в текущий момент. Устройство сопряжения должно знать (в соответствии с 8.1), что протокол WSR доступен. Для того чтобы подобрать протокол WSR, отвечающий требованиям 8.1, устройство сопряжения может отправлять на идентификационную карту случайную команду «ENVELOPE» («Оболочка»), содержащую идентификатор объекта протокола WSR. На канале 0, она должна быть:

'00' 'C3' '00' '00' <Lc> '06' <Lc-2> <Идентификатор объекта WSR протокола>.

Положительный результат выполнения команды (ответ = '90 00') указывает, что:

- идентификационная карта поняла идентификатор объекта, следовательно, поддерживает указанный протокол WSR;
- идентификационная карта готова к выполнению данного протокола, например, что он будет запущен в нужном месте в рабочем процессе приложения и что соответствующая среда безопасности сформирована.

Все остальные значения SW1-SW2 указывают на то, что протокол WSR не поддерживается или временно не может быть использован. Рекомендуемое значение SW1-SW2 — '6A' '81'. Если команда «ENVELOPE» («Оболочка») успешно выполнена идентификационной картой, идентификатор объекта в поле данных команды «ENVELOPE» («Оболочка») APDU должен указывать на спецификацию, в которой определен протокол WSR.

Приложение А
(справочное)

Программный разделяемый интерфейс для биометрического сравнения

А.1 Общие положения

Идентификационные карты имеют встроенный механизм межсетевого экрана для защиты конфиденциальных данных каждого приложения в ICC, имеющей несколько приложений. Преимущество данного механизма в том, что он ограничивает доступ вредоносной программы к данным другого приложения. Однако этот механизм также создает проблему для доверенного приложения, которое хочет получить метод или данные из другого доверенного приложения. Наличие защищенного программного интерфейса или программного межсетевого экрана позволит приложениям использовать только выбранные метод или данные, тем самым защищая конфиденциальные данные от несанкционированного доступа. Для реализации биометрических приложений необходимо делиться результатами или биометрическими данными с другими приложениями на идентификационной карте.

А.2 Механизм разделяемого интерфейса

Ниже описан метод совместного использования функций или данных посредством разделяемого интерфейса. На рисунке А.1 представлена идентификационная карта с двумя приложениями. Биометрическое приложение, реализующее механизм совместного использования, создает два набора функций или данных: функции, не используемые совместно, с полным доступом для данного приложения и функции или данные для совместного использования другими приложениями с ограниченным доступом к ним. Функции для совместного использования получают от разделяемого интерфейса. Если еще одно универсальное приложение хочет использовать разделяемые функции или данные из биометрического приложения, оно также создает два набора функций или данных: функции, не используемые совместно, для своих собственных методов и функции для совместного использования методом другого приложения.

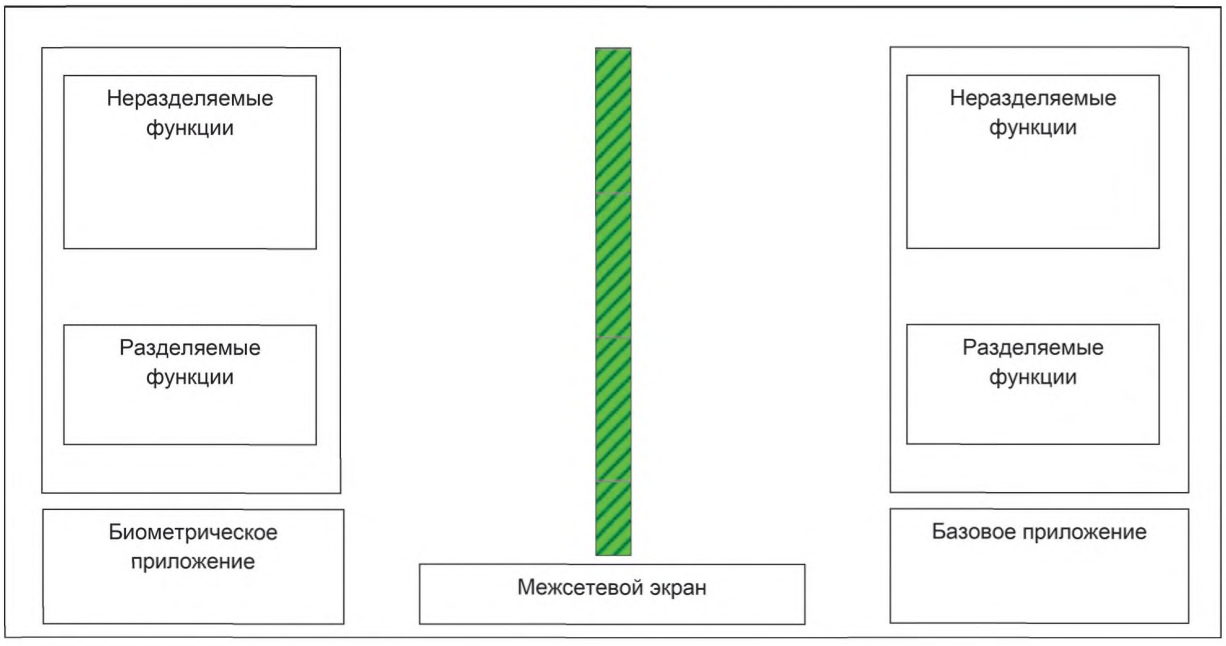


Рисунок А.1 — Приложения на идентификационной карте

Базовое приложение вызывает разделяемую функцию биометрического приложения. ОС проверяет и пересылает запрос биометрическому приложению. Биометрическое приложение получает запрос и определяет, будет ли оно делиться разделяемыми функциями с инициатором запроса. Если биометрическое приложение принимает положительное решение по запросу, то формируется ссылка на его разделяемые функции; в противном случае возвращается сообщение об ошибке. ОС направляет эту ссылку инициатору запроса (базовому приложению). Данный процесс показан на рисунке А.2, где числа, приведенные в скобках рядом со стрелками, указывают последовательность действий.

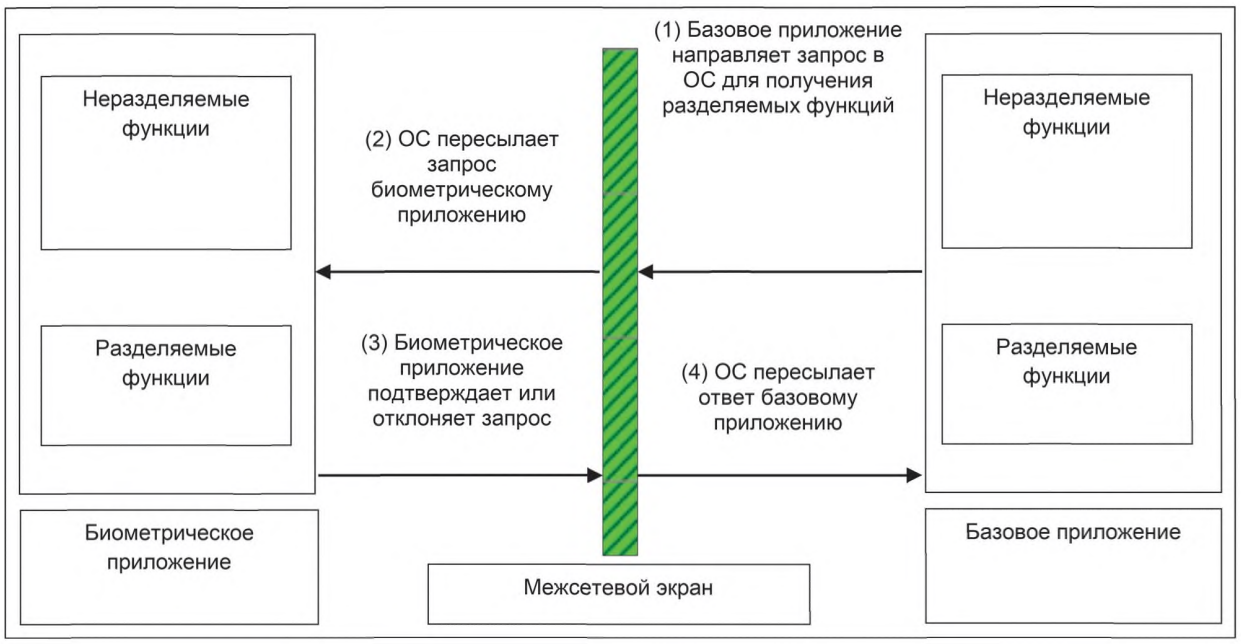


Рисунок А.2 — Доступ к разделяемым объектам

После того как базовое приложение получило эту ссылку, оно может использовать разделяемые функции или данные биометрического приложения. Базовое приложение может получить результат биометрического сравнения с помощью разделяемой функции для подтверждения транзакции или получения необходимой информации авторизованного пользователя для передачи. Разделяемая функция может быть доступна для использования базовому приложению на определенный период времени, что определяется ОС или биометрическим приложением для повышения уровня безопасности, как показано на рисунке А.3.

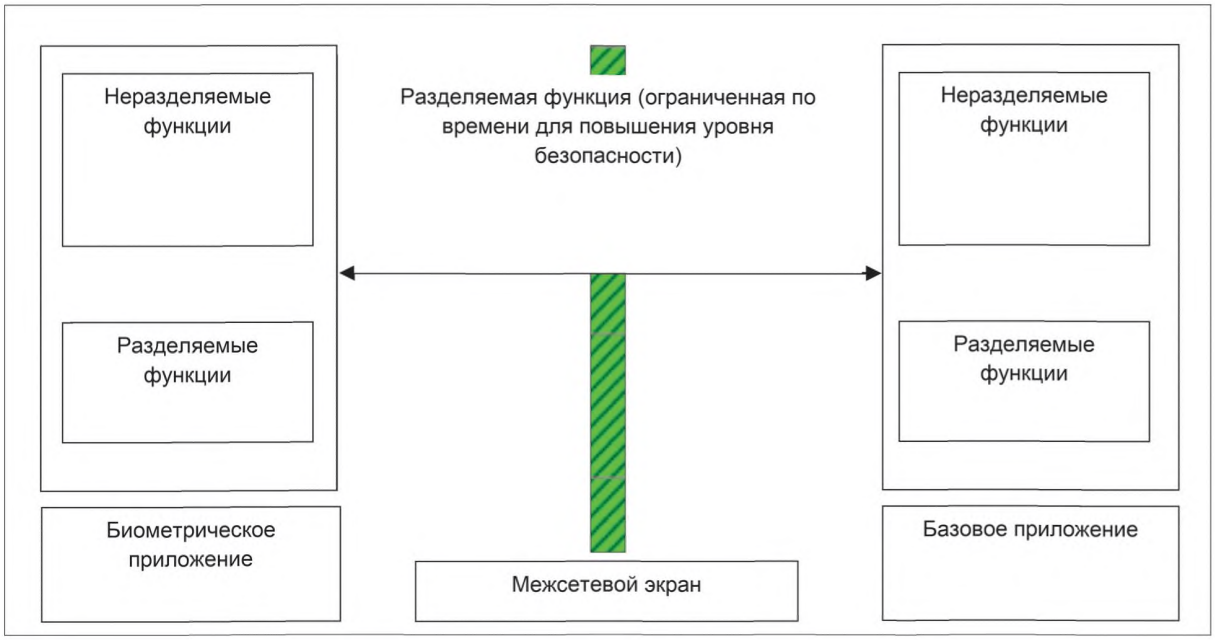


Рисунок А.3 — Успешная реализация совместного использования объекта

Например, после того, как биометрическое приложение завершило процесс биометрической верификации, вычисляется результат сравнения и сохраняется внутри программы. Базовое приложение может получить доступ к биометрическому приложению, чтобы получить результат сравнения с помощью доступа к разделяемым функциям через межсетевой экран. Межсетевой экран проверяет возможность доступа инициатора запроса (базового приложения), а затем позволяет ему извлечь результат сравнения из биометрического приложения (при успешной верификации). Межсетевой экран управляется ОС идентификационной карты.

Приложение В
(справочное)

Типовой APDU для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

В таблице В.1 представлена структура типового APDU в соответствии с требованиями действующих стандартов.

Команда APDU «VERIFY» («Выполнить верификацию») используется для отправки шаблона контрольных точек изображения отпечатка пальца на ICC. Она имеет следующую структуру.

Таблица В.1 — Структура команды APDU

CLA	INS	P1	P2	Lc	Данные
0x00	0x20 0x21[1)]	0x00	0x00	длина	Lc байты

[1)] Тег 0x20 используется, если поле данных содержит открытые данные с простой структурой, тогда как тег 0x21 указывает, что поле данных TLV-закодировано в соответствии с BER.

Примечания

1 Поле Le пустое, потому что в ответ на команду «VERIFY» («Выполнить верификацию») в соответствии с *ГОСТ Р ИСО/МЭК 7816-4* данные не возвращаются. Устройству сопряжения возвращается только значение состояния.

2 Использование биометрических технологий отображается внутри BIT.

Поле данных содержит данные верификации. Возможности ICC могут быть неявно известны. Рекомендуется сформировать BIT, который находится в открытом доступе для считывания с идентификационной карты с использованием команды «GET DATA» («Получить данные») (тег 0x7F60) и предоставляет внешнему устройству информацию о возможностях карты, например о поддержке биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013), об используемом формате данных и типе формата, о том, будет ли ICC упорядочивать контрольные точки или нет. Подробные сведения о BIT приведены в *ГОСТ Р ИСО/МЭК 7816-11*.

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

0x7F2E — биометрический контрольный шаблон;

0x5F2E — биометрические данные;

0x81/0xA1 — биометрические данные в стандартном формате (первичные/созданные);

0x82/0xA2 — биометрические данные в проприетарном формате (первичные/созданные).

Если на идентификационную карту отправляются данные стандартных контрольных точек, они кодируются в поле данных в соответствии с таблицей В.2.

Таблица В.2 — Поля данных для стандартных контрольных точек

Тег биометрического контрольного шаблона (техническая поправка Cor 1:2013)	Длина объекта данных	Тег стандартизированных биометрических данных	Длина данных контрольных точек	Данные контрольных точек
0x7F2E	L+2	0x81	L	—

Примечание — В таблице используется тег '7F2E', потому что поле «Значение» содержит объект созданных биометрических данных. Объект созданных биометрических данных начинается с тега '0x81', далее следуют значения актуальных биометрических данных. Другой возможный способ заключается в использовании тега '5F2E' для инкапсуляции биометрических данных в качестве первичных данных (техническая поправка Cor 1:2013).

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

Рисунок В.1 — Образец изображения с извлеченными данными контрольных точек

Контрольные точки изображения отпечатка пальца переводят в метрическую систему и сжимают в формат идентификационной карты (техническая поправка Cor 1:2013) для использования в процессе биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013). 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 6e 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 (техническая поправка Cor 1:2013).

Тип формата 6 владельца формата '0101' из *ГОСТ Р ИСО/МЭК 19794-2* использовался 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 производителей алгоритмов отпечатков пальцев. Каждая контрольная точка представлена 3 байтами. Первая контрольная точка имеет значение 0x25 для координаты *X* и значение 0x5D для координаты *Y*, типовую бифуркацию окончания гребня и ориентацию 205°, хранящиеся в 0x69 (техническая поправка Cor 1:2013).

В общей сложности обнаружено 38 контрольных точек, в результате чего общий размер контрольных точек 3x38 = 114 байтов, в шестнадцатеричном формате — 0x72 (техническая поправка Cor 1:2013).

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

CLA	INS	P1	P2	Lc	Данные
0x00	0x21	0x00	0x00	0x77 (техническая поправка Cor 1:2013)	–

Тег биометрического контрольного шаблона	Длина объекта данных	Тег стандартизированных биометрических данных	Длина данных контрольных точек	Данные контрольных точек
0x7F2E	0x74 (техническая поправка Cor 1:2013)	0x81	0x72 (техническая поправка Cor 1:2013)	–

0x25 0x5D 0x69 0x2D 0xA1 0x43 0x2F 0xAA 0x82 0x2F 0x6F 0x48 0x2F 0x43 0x49 0x35 0x96 0x45 0x37 0xAF 0x81 0x48 0xB0 0xBF 0x48 0x96 0x48 0x48 0x5D 0x89 0x4A 0x9C 0x43 0x4D 0x7C 0x6A 0x4D 0x63 0x6A 0x4D 0x19 0x45 0x4F 0x73 0x8B 0x50 0x91 0x42 0x54 0x85 0x6B 0x57 0x6B 0xAA 0x58 0x86 0xB2 0x58 0x7D 0x70 0x59 0x36 0x82 0x5B 0x8C 0x57 0x5E 0x94 0x9C 0x5F 0x73 0x71 0x61 0x61 0x66 0x64 0x4C 0x9C 0x69 0x97 0x9B 0x6F 0xA5 0x9D 0x70 0x33 0xB9 0x72 0x50 0x96 0x74 0x92 0x58 0x7D 0x27 0x59 0x7E 0x9D 0x59 0x80 0x66 0x93 0x83 0x4A 0x56 0x86 0x8E 0x56 0x90 0x3D 0x74 0x9A 0x3A 0x76 (техническая поправка Cor 1:2013)

Рисунок В.2 — Структура APDU для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

Команда полностью:

0x00 0x21 0x00 0x00 0x77 0x7F 0x2E 0x74 0x81 0x72 0x25 0x5D 0x69 0x2D 0xA1 0x43 0x2F 0x6F 0x48 0x2F 0x43 0x49 0x35 0x96 0x45 0x37 0xAF 0x81 0x48 0xB0 0xBF 0x48 0x96 0x48 0x48 0x5D 0x89 0x4A 0x9C 0x43 0x4D 0x7C 0x6A 0x4D 0x63 0x6A 0x4D 0x19 0x45 0x4F 0x73 0x8B 0x50 0x91 0x42 0x54 0x85 0x6B 0x57 0x6B 0xAA 0x58 0x86 0xB2 0x58 0x7D 0x70 0x59 0x36 0x82 0x5B 0x8C 0x57 0x5E 0x94 0x9C 0x5F 0x73 0x71 0x61 0x61 0x66 0x64 0x4C 0x9C 0x69 0x97 0x9B 0x6F 0xA5 0x9D 0x70 0x33 0xB9 0x72 0x50 0x96 0x74 0x92 0x58 0x7D 0x27 0x59 0x7E 0x9D 0x59 0x80 0x66 0x93 0x83 0x4A 0x56 0x86 0x8E 0x56 0x90 0x3D 0x74 0x9A 0x3A 0x76 (техническая поправка Cor 1:2013)

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 производителей.

Приложение С
(обязательное)

Обобщенная структура TLV контрольного параметра файла

Таблицы С.1—С.3, определенные в *5.4.3 ГОСТ Р ИСО/МЭК 7816-4—2013* для кодирования правил доступа, состоят из информационных объектов режима доступа и одного или нескольких информационных объектов статуса безопасности.

Таблица С.1 — Обобщенная структура TLV контрольного параметра файла для DF

Тег	Длина	Значение		
62	x	Тег	Длина	Значение
		82	1	'38' Дескриптор файла
		83	2	ID файла
		84	От '01' до '10'	Имя DF (AID)
		8A	1	5

Таблица С.2 — Обобщенная структура TLV контрольного параметра файла для форматированного EF

Тег	Длина	Значение		
62	X	Тег	Длина	Значение
		82	5	Дескриптор файла (1 байт) 41 00 Максимальная длина записи (1 байт) Максимальное значение счетчика записей (1 байт)
		83	2	ID файла
		85	2	Максимальный размер
		88	1	Короткий EFID
		8A	1	5 (активное состояние)
		A1	Переменная	Объекты данных со ссылками на правила доступа

Таблица С.3 — Обобщенная TLV структура контрольных параметров файла для открытых EF

Тег	Длина	Значение		
62	X	Тег	Длина	Значение
		80	02	Объем памяти открытого EF
		82	01	Дескриптор файла, открытого EF
		83	2	ID файла
		88	1	SFI
		8A	1	5
		A1	x	Объекты данных со ссылкой/ссылками на правило доступа

Приложение D
(обязательное)

Принципы обеспечения безопасности для биометрического сравнения на идентификационной карте

D.1 Введение

Настоящее приложение определяет минимальные требования к обеспечению безопасности для приложений на ICC, использующих биометрическое сравнение на идентификационной карте. Далее рассмотрены различные схемы реализации, и, хотя некоторые принципы могут быть общими для всех схем, существуют принципы, специфичные для конкретной схемы реализации.

Во введении представлен обзор различных схем, а также таблица для сопоставления этих схем с принципами обеспечения безопасности, которые подробно описаны в следующих пунктах. Данные схемы могут быть определены в соответствии со следующей классификацией:

a) использующие данные конфигурации сравнения в качестве глобального элемента. Это относится к следующим ситуациям:

1) идентификационная карта с единственным приложением, использующим биометрическое сравнение на идентификационной карте,

2) идентификационная карта с несколькими приложениями, использующими биометрическое сравнение на идентификационной карте с единой конфигурацией сравнения (т. е. один и тот же порог, один и тот же счетчик повторов и т. д.). В этом случае если одно приложение препятствует выполнению биометрического сравнения на идентификационной карте, то это отразится на всех приложениях, использующих тот же механизм биометрической верификации. С другой стороны, если приложение получило положительный результат биометрической верификации, то счетчик повторов будет сброшен для всех приложений (техническая поправка Cor 1:2013);

b) использующие данные конфигурации сравнения в качестве локального элемента. Это относится к следующим ситуациям:

1) каждое приложение имеет собственную структуру биометрического контрольного шаблона, в том числе данные биометрического контрольного шаблона, данные конфигурации, такие как пороги и максимальное значение счетчика повторов, счетчик повторов и т. д.,

2) все приложения только обмениваются общими данными биометрического контрольного шаблона, но каждое приложение имеет собственные данные конфигурации (данные конфигурации сравнения), которые включают в себя различные пороги, счетчик повторов и т. д. (техническая поправка Cor 1:2013).

В таблице D.1 вышеуказанные схемы сопоставлены с принципами обеспечения безопасности, определенными в настоящем приложении.

Таблица D.1 — Сопоставление схем биометрического сравнения на идентификационной карте и принципов обеспечения безопасности

	SP1: глобальные данные конфигурации сравнения	SP2: локальные данные конфигурации сравнения
a.1	*X*	—
a.2	*X*	—
b.1	(техническая поправка Cor 1:2013)	*X* (техническая поправка Cor 1:2013)
b.2	—	*X*

Далее определены общие принципы обеспечения безопасности, принципы SP1 и принципы SP2.

D.2 Общие принципы обеспечения безопасности CSP для биометрического сравнения на идентификационной карте

Следующие минимальные правила обеспечения безопасности применяют во всех случаях:

- ни одному приложению не допускается передавать биометрический контрольный шаблон с ICC (см. 7.2.2);
- для реализации механизма счетчика повторов должны применять принципы обеспечения безопасности, указанные в 7.1.5;
- все приложения должны использовать механизмы обеспечения безопасности для создания биометрических контрольных шаблонов (биометрическая регистрация), обновления биометрических контрольных шаблонов (повторная биометрическая регистрация) или сравнения с биометрическим контрольным шаблоном (биометрическая верификация), в частности:

- безопасный обмен сообщениями устанавливается априори для любой из вышеуказанных операций (см. *ГОСТ Р ИСО/МЭК 7816-4*);

- все данные, передающиеся во время процесса биометрического сравнения на идентификационной карте, должны подтверждать свою целостность;

- все биометрические данные должны быть зашифрованы для передачи на ICC для обеспечения конфиденциальности (см. *нормативный документ**);

- ОС идентификационной карты может иметь механизм разблокировки процесса биометрического сравнения на идентификационной карте. В таком случае в процессе разблокировки должен быть обнулен биометрический контрольный шаблон в ICC и направлен запрос для новой попытки биометрической регистрации.

D.3 Принципы обеспечения безопасности SP1 для глобальных данных конфигурации сравнения

В приложениях, использующих биометрический контрольный шаблон в качестве глобального механизма биометрической верификации, нет необходимости устанавливать двойную косвенность для определения конфигурации сравнения. Кроме того, применяют следующие правила:

- для идентификационных карт с несколькими приложениями, использующими биометрическое сравнение на идентификационной карте с одним и тем же биометрическим контрольным шаблоном, если любое приложение, использующее биометрический контрольный шаблон, имеет высокий уровень безопасности, для всех приложений должен использоваться уникальный порог и единый счетчик повторов, связанный с биометрическим контрольным шаблоном [см. 7.2.8 а)];

- все данные конфигурации связаны с биометрическим контрольным шаблоном. В частности:

- порог биометрической верификации;

- максимальное количество попыток биометрической верификации;

- счетчик повторов;

- все параметры алгоритма сравнения;

- ни одно из приложений, использующих механизм биометрического сравнения на идентификационной карте с описанным биометрическим контрольным шаблоном, не может автономно изменить данные конфигурации;

- когда счетчик повторов достигнет нуля, механизм биометрического сравнения на идентификационной карте блокируется, и, следовательно, все приложения, использующие описанный биометрический контрольный шаблон для биометрической верификации, не смогут выполнять эти операции, защищенные механизмом биометрического сравнения на идентификационной карте;

- положительный результат верификации биометрического контрольного шаблона сбрасывает связанный счетчик повторов до его начального значения независимо от того, какое из приложений осуществило успешную попытку биометрической верификации.

D.4 Принципы обеспечения безопасности SP2 для локальных данных конфигурации сравнения

В приложениях, требующих независимого контроля процесса биометрического сравнения на идентификационной карте, но обменивающихся данными биометрического контрольного шаблона, применяют следующие правила:

- все приложения, использующие механизм двойной косвенности, имеют собственные данные конфигурации сравнения, как минимум:

- порог,

- счетчик повторов;

- не допускается конфигурировать приложения, обменивающиеся одними и теми же биометрическими данными, которые будут иметь разные пороги, но единый счетчик повторов;

- 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 для данного приложения сбрасывается до начального значения;

- каждый раз, когда приложение получает отрицательный результат верификации биометрического контрольного шаблона, только счетчик повторов для 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;

- любое приложение может изменить свои данные конфигурации сравнения при необходимости, без изменения данных конфигурации сравнения других приложений, использующих тот же биометрический контрольный шаблон.

---

* См. [2].

Приложение Е
(справочное)

Рекомендации для механизмов обеспечения безопасности при биометрическом сравнении на идентификационной карте (техническая поправка Cor 1:2013)

Е.1 Общие положения

Настоящее приложение предназначено для определения механизма обеспечения безопасности, который следует учитывать при биометрическом сравнении на идентификационной карте (техническая поправка Cor 1:2013). 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 обратиться к комплексу стандартов *ГОСТ Р ИСО/МЭК 7816*, описывающих команды и механизмы, связанные с идентификационными картами на интегральной схеме (например, части 4, 11), и к соответствующим стандартам, разработанным ИСО/МЭК JTC 1/SC 27.

Е.2 Взаимная аутентификация

Первый момент, который необходимо учитывать при попытке обеспечения безопасности, когда два объекта обмениваются данными — это взаимное доверие данных объектов. Поэтому при взаимодействии должен использоваться механизм, обеспечивающий доверие терминала к идентификационной карте, и еще один механизм, обеспечивающий доверие идентификационной карты к данному терминалу. Эти механизмы называются внутренней и внешней аутентификацией. При использовании обоих механизмов процесс именуют взаимной аутентификацией.

Взаимная аутентификация обычно заканчивается генерацией ключа сессии для создания защищенного канала. С целью избежать повторных атак для каждой сессии должен быть использован уникальный ключ. Некоторые алгоритмы, используемые для взаимной аутентификации, направляют запрос генерации случайных или псевдослучайных чисел как идентификационной карте, так и терминалу.

После установления защищенного канала связи между идентификационной картой и терминалом могут быть реализованы с большим успехом следующие механизмы обеспечения безопасности.

Е.3 Целостность сообщения

При обмене APDU хакеры могут попытаться перехватить сообщения и изменить их с целью получения выгоды путем, например, повторной отправки предыдущего биометрического образца для получения доступа к информации об идентификационной карте и/или сервисам. Чтобы избежать такого рода атак, рекомендуется, чтобы и терминал, и идентификационная карта проверяли целостность полученного APDU.

Один из способов проверки целостности — это добавление подписи APDU как для заголовка, так и для данных с помощью алгоритма шифрования с симметричным ключом и добавления подписи, полученной при обмене данными. Использование сеансового ключа, сгенерированного в ходе взаимной аутентификации, позволяет предотвратить атаки, упомянутые выше.

Е.4 Конфиденциальность

Проверку целостности рекомендуется проводить при любом обмене APDU, но иногда может использоваться более высокий уровень безопасности. Особенно важными являются те APDU, в которых биометрический шаблон или биометрический образец передаются из считывателя на идентификационную карту [или с идентификационной карты на считыватель при биометрическом сравнении вне идентификационной карты (техническая поправка Cor 1:2013)]. При этом данные не должны передаваться в формате RAW, но 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). Также рекомендуется проводить проверку целостности для возможности ее использования до или после шифрования передаваемых данных.

Е.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. Терминал может получить случайное число из идентификационной карты и рассчитать MAC биометрических данных, который связывает со случайным числом (полученным из идентификационной карты) и секретным ключом. Секретный ключ хранится как в приложении, так и в идентификацион-

ной карте. Во время взаимодействия необходимо передать только случайное число и MAC. Когда идентификационная карта 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 идентификационной карты 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 терминал является надежным и способен хранить секретный ключ, данный метод можно рассматривать как метод реализации «защищенного канала».

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

Приложение F
(справочное)

Примеры реализации механизмов биометрического сравнения на идентификационной карте

F.1 Введение

В этом приложении приведены три примера реализации механизмов биометрического сравнения на идентификационной карте, относящихся к статусу безопасности карты. Эти примеры будут 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 SS. Статусы безопасности будут отмечены числами, где 0 является начальным состоянием, и чем больше значение статуса, тем выше уровень безопасности.

Для простоты понимания примеров будут использоваться пороги. Когда процесс биометрического сравнения завершен, результат сравнения cs сравнивается с некоторым пороговым значением th. Если cs > th, доступ предоставляется, в противном случае доступ запрещен. Если приложение на идентификационной карте использует более одного порогового значения, они обозначаются th1 и th2, при этом th2 > th1 и, следовательно, th2 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, используемый при дальнейших операциях.

F.2 Одно одноуровневое приложение

Самым простым примером является использование одного приложения на идентификационной карте с одним уровнем биометрической верификации (одним порогом). На рисунке F.1 представлена блок-схема состояний безопасности. В то время как другие операции могут быть выполнены при начальном SS, биометрическая верификация выполняется только после достижения более высокого SS путем установления защищенного канала. Для данного SS пользователь может выполнить команду «VERIFY» («Выполнить верификацию»). Если доступ разрешен, более высокий SS достигнут и операции, требующие данного значения SS или ниже, могут быть выполнены.

Если биометрическую верификацию выполнить не удалось, возвращается сообщение об ошибке безопасности и соответственно начальное значение SS достигнуто, что требует установления нового защищенного канала перед выполнением дальнейшей попытки верификации. Кроме того, счетчик повторов для биометрического сравнения уменьшается на единицу, и, если дальнейшие попытки не разрешены, механизм биометрического сравнения будет заблокирован.

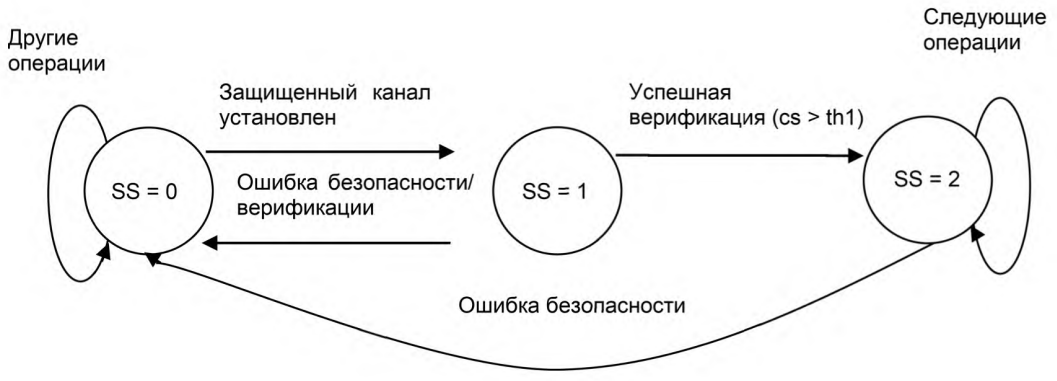


Рисунок F.1 — Блок-схема для одного одноуровневого приложения

F.3 Одно разноуровневое приложение

В данной части проиллюстрирован более сложный пример. Если одно приложение на идентификационной карте хочет использовать биометрическое сравнение для предоставления доступа к информации или некоторым операциям, может быть возможным, что для каждой операции будут установлены различные уровни безопасности. Тогда приложение может установить другой уровень безопасности с помощью точности в процессе биометрическо-

го сравнения. Для таких случаев выбраны два различных уровня с помощью двух различных пороговых значений th1 и th2, где th2 > th1, т. е. th2 является более строгим требованием.

После установления защищенного канала будет достигнуто значение SS = 1. Для этого SS может быть выполнено биометрическое сравнение. Если операция выполнена, может произойти три различных варианта. Если cs ≤ th1, то доступ запрещен, соответствующий счетчик повтора уменьшается и достигается начальное SS. Если cs больше, чем th1, но меньше или равен th2, то будут разрешены только операции 1-го уровня, как и любые другие операции, требующие более низкого SS. Только если cs более th2, разрешены операции 2-го уровня, а также любые другие операции, требующие более низкого SS.

В любом случае если возвращается сообщение об ошибке безопасности, то достигается начальный SS и должен быть установлен новый защищенный канал для продолжения прерванных операций.

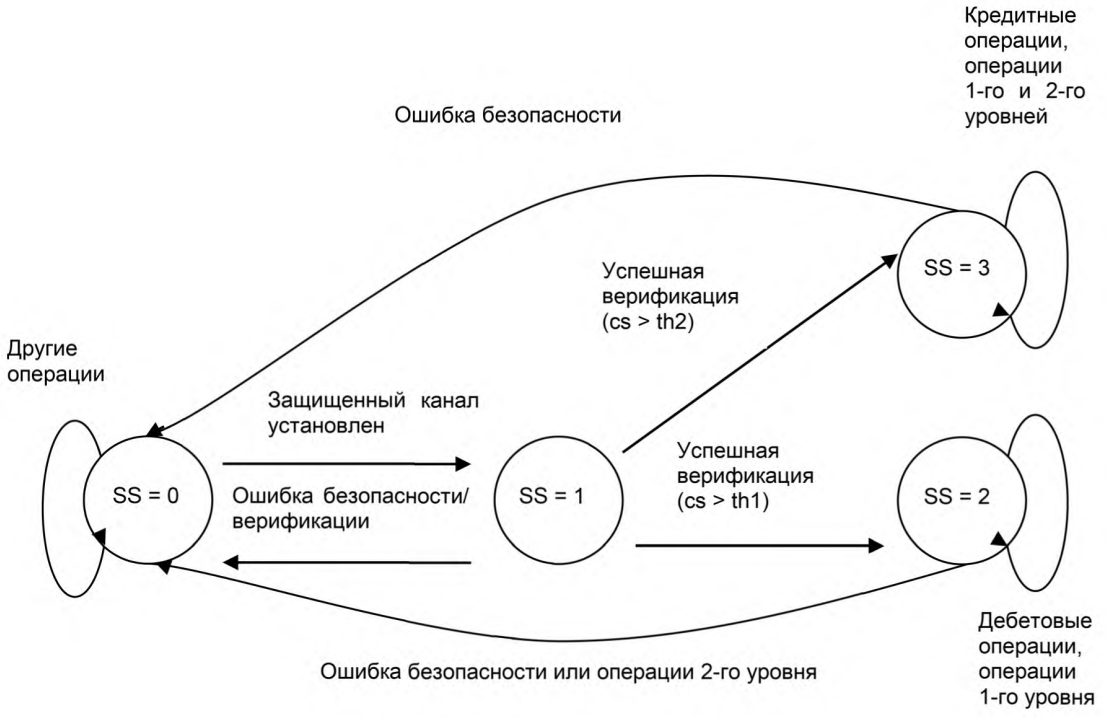


Рисунок F.2 — Блок-схема для одного разноуровневого приложения

F.4 Несколько приложений

Самым сложным случаем является ICC с несколькими приложениями, где каждое приложение имеет свои пороговые значения и счетчики повторов для достижения своих SS для обеспечения различных уровней безопасности, используя одни и те же данные 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 соответствующие им приложения, для того чтобы избежать влияния одного приложения на функционал другого приложения. SS одного приложения не влияет на другие приложения, потому что при выборе нового приложения SS возвращается к начальному значению. Таким образом, после выбора приложения если используются некоторые ограниченные операции, то устанавливается новый защищенный канал, и после этого можно выполнить биометрическое сравнение с помощью команды «VERIFY» («Выполнить верификацию»). Результат такого сравнения будет, как уже говорилось, обеспечивать следующие возможности:

- если верификацию выполнить не удалось (cs < th1):
  a) уменьшение счетчика повторов, но только счетчика повторов выбранного приложения;
  b) блокировка процесса биометрической верификации, если счетчик повторов достигает 0;
- если верификация прошла успешно, счетчик повторов для выбранного приложения будет сброшен:
  a) если th2 < cs < th1, то будет достигнут SS 1-го уровня и будут разрешены операции, требующие такого SS;
  b) если cs > th2, то будет достигнут SS 2-го уровня и соответственно будут разрешены все операции (1-го и 2-го уровней).

Блок-схема приведена на рисунке F.3.

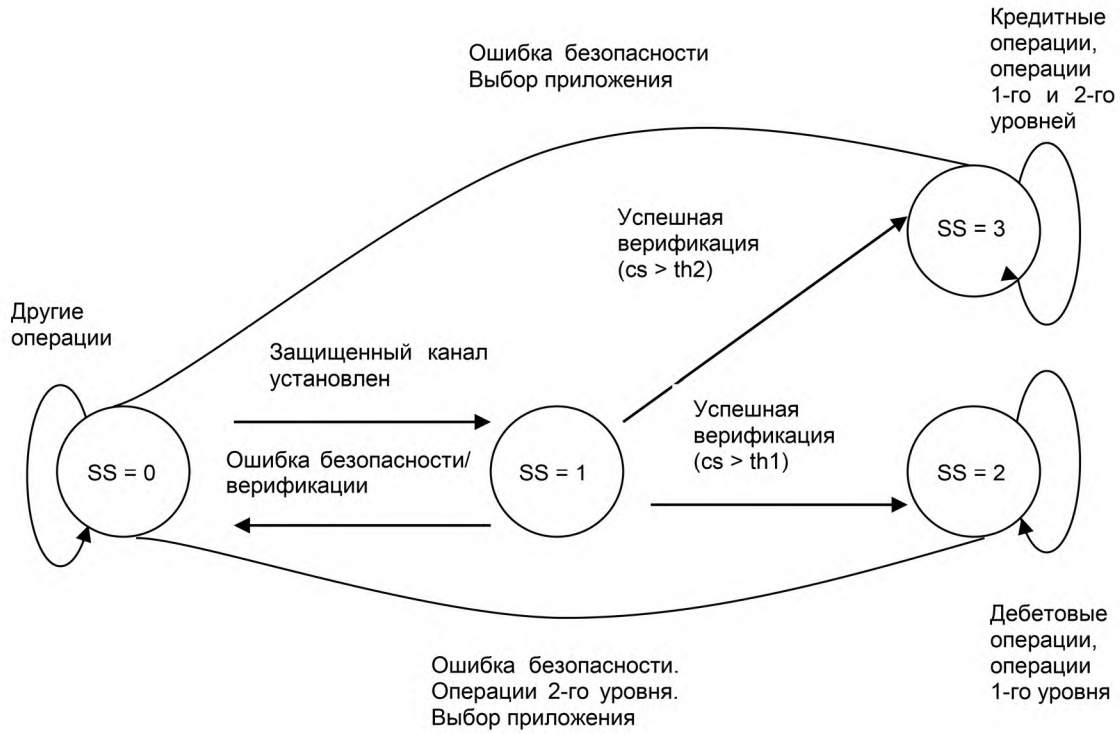


Рисунок F.3 — Блок-схема для нескольких приложений

Приложение G
(справочное)

Архитектура биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013)

G.1 Общие положения

Распределение нагрузки представляет собой особый способ реализации биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013), позволяющий распределить рабочую нагрузку процесса биометрического сравнения между ICC и устройством сопряжения. Описанный механизм позволяет идентификационной карте использовать локальные биометрические системы верификации, которые, как правило, представляют собой персональный компьютер (ПК) или встроенный процессор с высокой вычислительной мощностью, для помощи в вычислении трудоемких функций. Карта и локальная система биометрической верификации работают вместе для ускорения процесса биометрического сравнения с учетом обеспечения безопасности и конфиденциальности зарегистрированной биометрической информации. При распределении нагрузки биометрическое сравнение должно выполняться на ICC.

G.2 Схема распределения нагрузки для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

На рисунке G.1 показана структурная схема биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013). Большинство элементов, используемых для биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013), точно такие же, как для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013), за исключением следующих двух частей:

- биометрические данные, которые хранятся на идентификационной карте во время биометрической регистрации, делятся на защищенные и открытые. Защищенными данными является биометрический контрольный шаблон, что имеет решающее значение для уникальности, а открытые данные не критичны, так как они не могут быть использованы для восстановления защищенных данных. Защищенные данные, представляющие собой биометрический контрольный шаблон, хранятся в формате ИСО. Открытые данные, содержащие биометрические признаки, служат для ускорения процесса сравнения на идентификационной карте и передаются в локальную систему биометрической верификации;
- для ускорения процесса биометрического сравнения требуются некоторые расчеты, производимые в системе биометрической верификации.

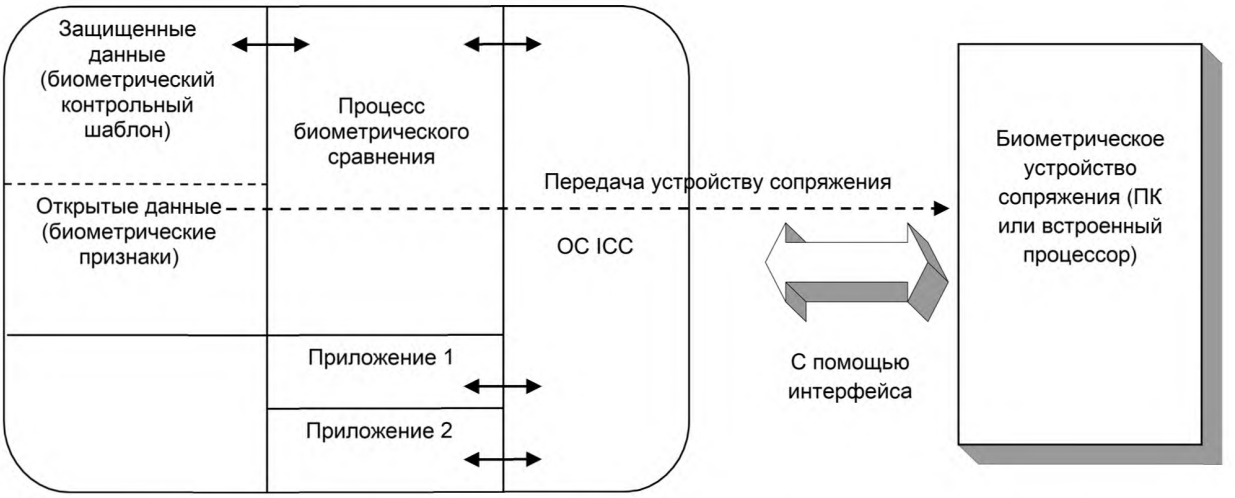


Рисунок G.1 — Блок-схема биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013)

Пунктирная стрелка на рисунке G.1 указывает, что открытые данные могут быть переданы в систему биометрической верификации. Открытые данные могут быть переданы по запросу локальной системы биометрической верификации. Эти данные могут быть предварительно сжаты и зашифрованы перед хранением для защиты шаблона и сохранения памяти соответственно.

G.3 Типы стратегии распределения нагрузки для биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013)

G.3.1 Общие положения

Для биометрического сравнения на идентификационной карте могут быть использованы два типа стратегии распределения нагрузки (техническая поправка Cor 1:2013). Один подразумевает использование предварительных вычислений, а второй — распределение нагрузки во время выполнения процесса сравнения. На рисунке 3 в 6.4 схематически изображена архитектура биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013).

G.3.2 Предварительные вычисления

Некоторые биометрические данные, такие как отпечатки пальцев, требуют выполнения выравнивания шаблона перед выполнением сравнения. Такой процесс называется предварительными вычислениями, так как вычисления должны быть произведены до начала процесса сравнения. Для выполнения предварительных вычислений требуется некоторая информация из зарегистрированного отпечатка пальца. Открытые данные могут быть использованы для выполнения такой операции.

Пример — Процесс распознавания изображений отпечатков пальцев с помощью вейвлетов может использовать открытые данные для хранения выбранных вейвлетов. Эти сжатые данные могут передаваться в локальную систему биометрической верификации для выполнения преобразований выравнивания шаблона.

G.3.3 Распределение нагрузки во время выполнения

В ходе процесса выполнения предварительных вычислений определенные вычисления требуют большой вычислительной мощности. Идентификационные карты низкого ценового сегмента могут не иметь достаточной вычислительной мощности для выполнения такой операции за короткий период времени. Следовательно, в целях ускорения процесса сравнения с идентификационной карты могут быть переданы некоторые промежуточные данные в локальную систему биометрической верификации для выполнения вычислений.

G.4 Протокол вычислений распределения нагрузки

Протокол вычислений распределения нагрузки WSCP определяет последовательность выполнения биометрического сравнения на идентификационной карте с распределением нагрузки (техническая поправка Cor 1:2013). Перед активацией WSCP рекомендуется проводить взаимную аутентификацию локальной системы биометрической верификации и идентификационной карты, чтобы убедиться, что и процесс сравнения, и локальная биометрическая система верификации являются доверенными и авторизованы выполнять процесс биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013).

Общая схема на рисунке G.2 показывает, что WSCP делится на две части. Первая часть является сектором выполнения предварительных вычислений. Предварительные вычисления включают в себя четыре этапа. Первый этап подразумевает отправку локальной системой биометрической верификации команды на идентификационную карту для активирования процедуры биометрического сравнения. После того как идентификационная карта получает команду, она пересылает открытые данные шаблона обратно в систему биометрической верификации. Система биометрической верификации получает открытые данные шаблона, затем использует открытый шаблон для выполнения необходимой операции, такой как поворот, и создает шаблон. Данный шаблон передается на идентификационную карту для начала выполнения биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013). Этапы (1)—(4) (см. рисунок G.2) являются стандартными транзакциями данных между системой биометрической верификации и идентификационной картой. Следовательно, команд и ответов APDU, определенных в *ГОСТ Р ИСО/МЭК 7816-4*, достаточно для передачи открытых данных для выполнения предварительных вычислений.

На этапе (5) идентификационная карта начинает вычисления процесса сравнения после завершения выполнения предварительных вычислений. В процессе сравнения, если идентификационной карте необходимо рассчитать ресурсоемкие функции, может использоваться протокол WSR для запроса распределения нагрузки с системой биометрической верификации. Если идентификационная карта не нуждается в выполнении таких функций, процесс может пропустить этапы (6)—(8) и перейти к этапу (9). Этапы (6), (7) и (8) являются процедурами выполнения WSR с локальной системой биометрической верификации, но если эти функции не применяются, то процесс может перейти непосредственно к этапу (9). Идентификационная карта на этапе (6) отправляет запрос распределения нагрузки и промежуточные данные в локальную систему биометрической верификации. Локальная система биометрической верификации, получив запрос и промежуточные данные на этапе (7), должна выполнить запрошенную функцию для обработки промежуточных данных. После завершения обработки биометрической системой верификации она должна отправить результат на идентификационную карту на этапе (8), и идентификационная карта должна продолжить процесс выполнения сравнения. Когда идентификационная карта завершает вычисление результата сравнения на этапе (9), она должна направить уведомление локальной системе биометрической верификации о завершении биометрического сравнения. На этапе (10) локальная система биометрической верификации может продолжить последовательность операций, используя результат биометрического сравнения на идентификационной карте (техническая поправка Cor 1:2013).

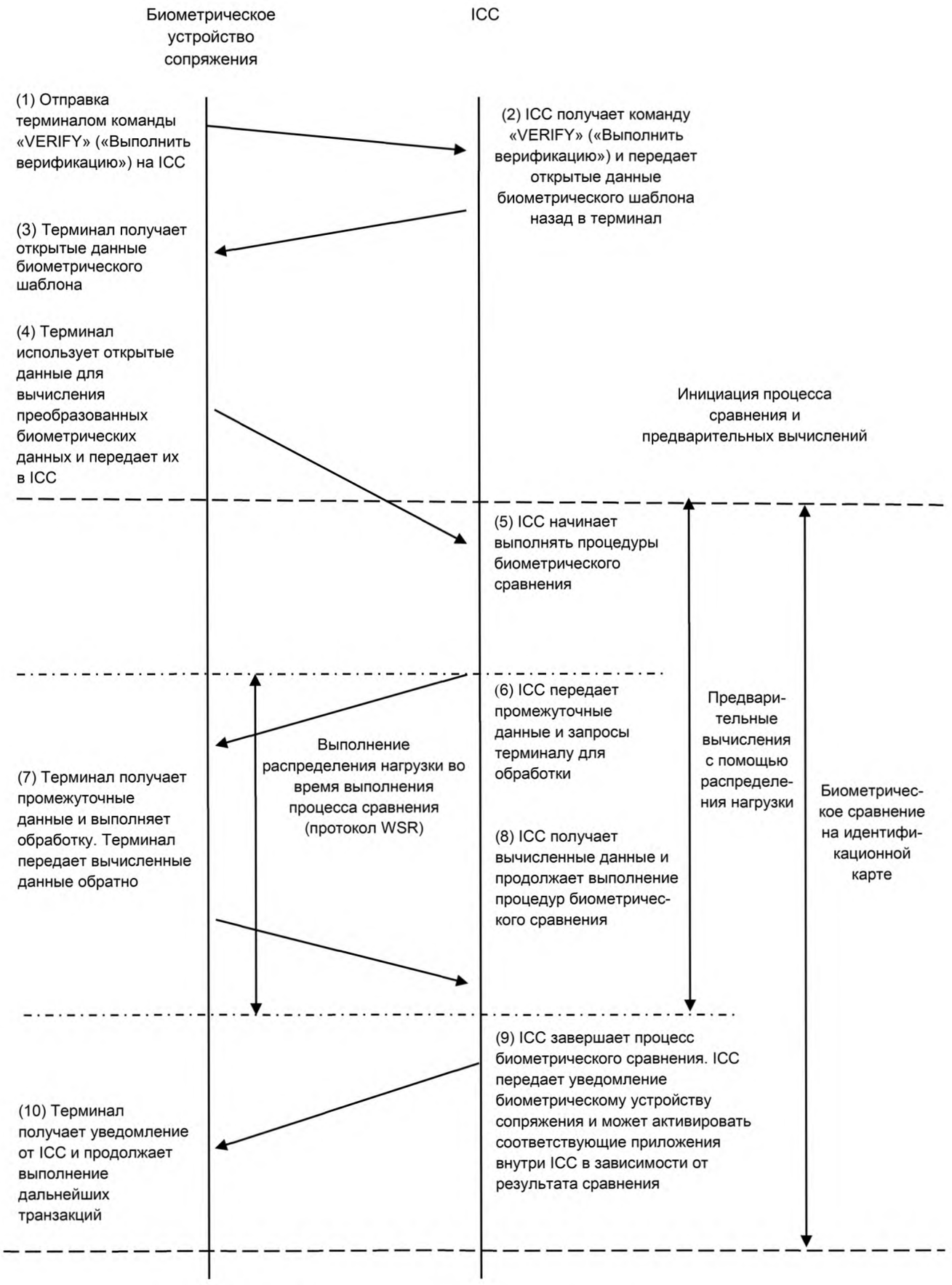
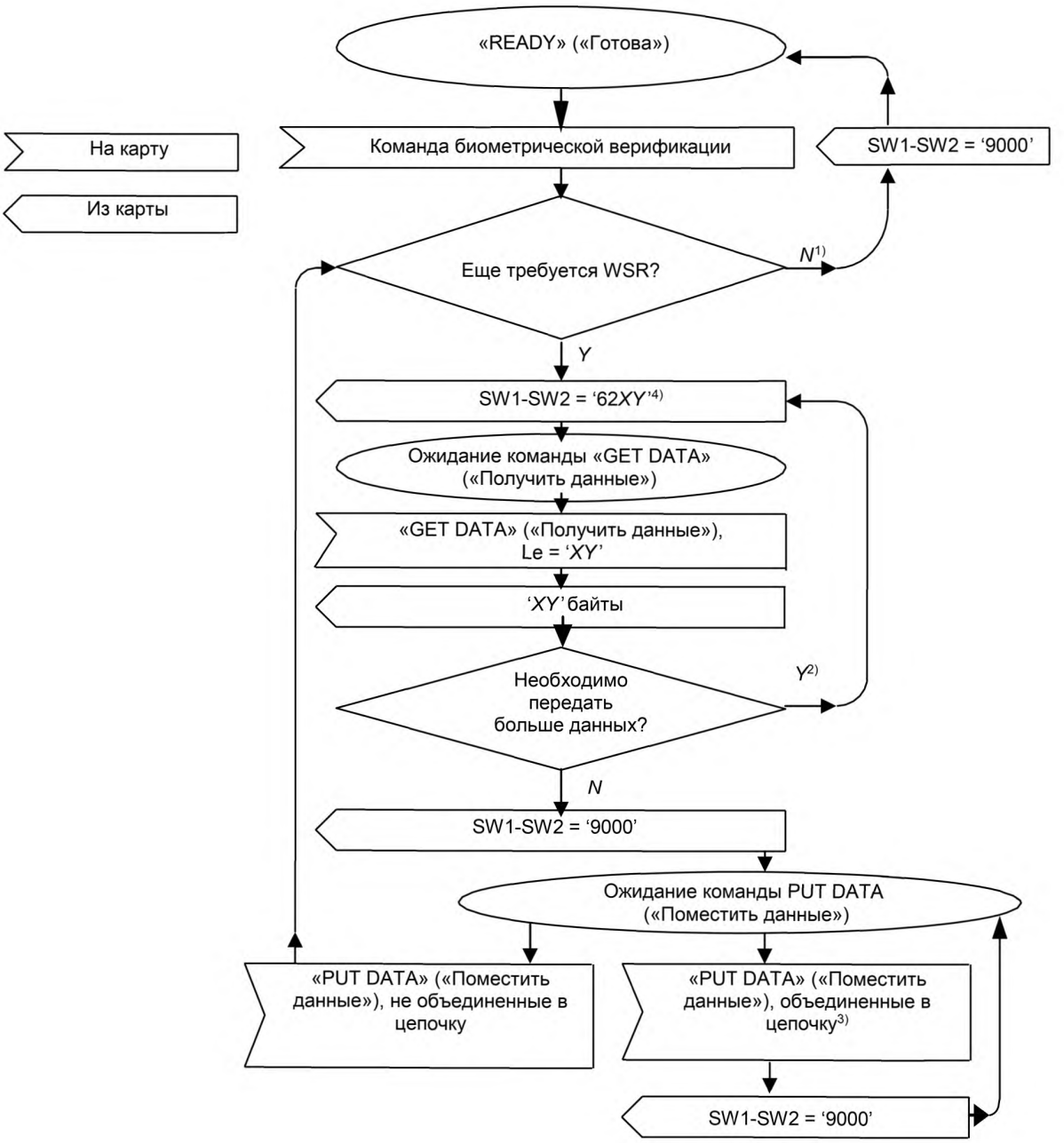


Рисунок G.2 — Общая схема протокола вычислений распределения нагрузки

Приложение Н
(справочное)

Диаграмма состояния идентификационной карты, при необходимости выполняющей WSR



Примечание — Если синтаксис, описанный в настоящем приложении, не соблюдается, например, потому, что одна команда отклонена или если внешнее устройство не сможет отправить команду «GET DATA» («Получить данные»), предполагается, что идентификационная карта вернется к состоянию «READY» («Готова»).

[1] Команде не требуется WSR или сеанс WSR завершен.

[2] Данный механизм определен в *ГОСТ Р ИСО/МЭК 7816-4*, если одной команды «GET DATA» («Получить данные») недостаточно.

[3] Данный механизм определен в *ГОСТ Р ИСО/МЭК 7816-4*, если одной команды «PUT DATA» («Поместить данные») недостаточно.

[4] Отправка соответствующей команды «GET DATA» («Получить данные») является обязательной в соответствии с требованиями настоящего стандарта и рекомендованной в соответствии с требованиями *ГОСТ Р ИСО/МЭК 7816-4*.

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 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»
ГОСТ Р ИСО МЭК 7816-3—2013	IDT	ISO/IEC 7816-3:2006 «Карты идентификационные. Карты на интегральных схемах. Часть 3. Карты с контактами. Электрический интерфейс и протоколы передачи»
ГОСТ Р ИСО/МЭК 7816-4—2013	IDT	ISO/IEC 7816-4:2005 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
ГОСТ Р ИСО/МЭК 7816-11—2013	IDT	ISO/IEC 7816-11:2004 «Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами»
ГОСТ Р ИСО/МЭК 19785-1—2008	IDT	ISO/IEC 19785-1:2006 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»
ГОСТ Р ИСО/МЭК 19785-2—2008	IDT	ISO/IEC 19785-2:2006 «Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 2. Процедуры действий регистрационного органа в области биометрии»
ГОСТ ISO/IEC 19794-1—2015	IDT	ISO/IEC 19794-1:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 1. Структура»
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—2009	IDT	ISO/IEC 19794-3-2006 «Информационные технологии. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца»
ГОСТ Р ИСО/МЭК 19794-4—2014	IDT	ISO/IEC 19794-4:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 4. 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 19794-6—2014	IDT	ISO/IEC 19794-6:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза»
ГОСТ Р ИСО/МЭК 19794-7—2009	IDT	ISO/IEC 19794-7:2007 «Информационные технологии. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи»

Окончание таблицы ДА.1

Обозначение ссылочного национального и межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
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 19794-9—2015	IDT	ISO/IEC 19794-9:2011 «Информационные технологии. Форматы обмена биометрическими данными. Часть 9. Данные изображения сосудистого русла»
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—2012	IDT	ISO/IEC 29794-1:2009 «Информационные технологии. Качество биометрического образца. Часть 1. Структура»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ИСО/МЭК 19785-3:2015* Информационные технологии. Единая структура форматов обмена биометрическими данными. Часть 3. Спецификации формата ведущей организации (ISO/IEC 19785-3:2015 Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications)

[2] ИСО/МЭК 24761:2009 Информационные технологии. Методы защиты информации. Аутентификационный статус для биометрии (ISO/IEC 24761:2009 Information technology — Security techniques — Authentification context for biometrics)

[3] ИСО/МЭК 7816-15:2016 Карты идентификационные. Карты на интегральных схемах. Часть 15. Применение криптографической информации (ISO/IEC 7816-15:2016 Identification cards — Integrated circuit cards — Part 15: Cryptographic information application)

* На момент публикации настоящего стандарта соответствующий гармонизированный национальный стандарт находится в разработке.

УДК 336.77:002:006.354 ОКС 35.240.15 П85

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

БЗ 1—2018/56

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.09.2018. Подписано в печать 15.10.2018. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,60.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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