ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 7816-11— 2013

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 11

Верификация личности биометрическими методами

ISO/IEC 7816-11:2004
Identification cards — Integrated circuit cards —
Part 11: Personal verification through biometric methods
(IDT)

Издание официальное

Москва
Стандартинформ
2014

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ) и Техническим комитетом по стандартизации ТК 22 «Информационные технологии» на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1632-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 7816-11:2004 «Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами» (ISO/IEC 7816-11:2004 «Identification cards — Integrated circuit cards — Part 11: Personal verification through biometric methods»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в ГОСТ 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в годовом (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячно издаваемом 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 национального органа Российской Федерации по стандартизации в сети Интернет (gost.ru)

Содержание

Введение

Настоящий стандарт — один из серии стандартов, описывающих параметры карт на интегральных схемах с контактами и их применение для обмена информацией.

Настоящий стандарт применим также к картам без контактов.

Международный стандарт ИСО/МЭК 7816-11 подготовлен подкомитетом № 17 «Карты и идентификация личности» совместного технического комитета № 1 ИСО/МЭК «Информационные технологии» (ISO/IEC JTC 1/SC 17).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 11

Верификация личности биометрическими методами

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

Дата введения — 2015—01—01

1 Область применения

Настоящий стандарт устанавливает межотраслевые команды, связанные с системой защиты и используемые для верификации личности биометрическими методами в картах на интегральной(ых) схеме(ах). В нем также определена структура данных и методы доступа к данным для использования карты в качестве носителя биометрических эталонных данных и/или в качестве устройства, позволяющего выполнить верификацию личности биометрическими методами (т.е. «он-карт» сопоставление). Идентификация личности с помощью биометрических методов выходит за рамки настоящего стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты.

Для датированных ссылок следует использовать только указанное издание, для недатированных ссылок следует использовать последнее издание указанного документа, включая все поправки:

ИСО/МЭК 7816-4:2005[1)] Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена (ИСО/МЭК 7816-4:2005 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange)

ИСО/МЭК 19785[2)] Информационные технологии. Структура форматов обмена общей биометрической информацией (ISO/IEC CD 19785, Information technology — Common Biometric Exchange Formats Framework (CBEFF))

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **биометрические данные** (biometric data): Данные, кодирующие признак или признаки, используемые при биометрической верификации.

3.2 **биометрическая информация** (biometric information): Информация, необходимая для внешних устройств для создания данных верификации.

3.3 **биометрические эталонные данные** (biometric reference data): Данные, хранящиеся в карте для сопоставления с данными биометрической верификации.

[1)] В ИСО/МЭК 7816-11:2004 допущена опечатка года издания стандарта ИСО/МЭК 7816-4:2003. ИСО/МЭК 7816-4:2005 заменен на ИСО/МЭК 7816-4:2013.

[2)] На момент издания международного стандарта ИСО/МЭК 7816-11:2004 международный стандарт ИСО/МЭК 19785 находился на стадии проекта комитета CD. В настоящее время действуют ИСО/МЭК 19785-1:2006, ИСО/МЭК 19785-2:2006, ИСО/МЭК 19785-3:2007, ИСО/МЭК 19785-4:2010.

Издание официальное

3.4 **биометрическая верификация** (biometric verification): Процесс верификации при взаимно однозначном сопоставлении данных биометрический верификации с биометрическими эталонными данными.

3.5 **данные биометрической верификации** (biometric verification data): Данные, собираемые в процессе верификации для сопоставления с биометрическими эталонными данными.

3.6 **шаблон** (template): По ИСО/МЭК 7816-4.

Примечание — Термин «шаблон» означает поле значения в составном информационном объекте. Не следует путать с обработанным образцом биометрических данных.

4 Сокращения

AID — Идентификатор приложения (Application Identifier);
AT — Шаблон аутентификации (Authentication Template);
BER — Базовые правила кодирования (Basic Encoding Rules);
BIT — Шаблон биометрической информации (Biometric Information Template);
BD — Биометрические данные (Biometric Data);
BDP — BD в проприетарном формате (BD in proprietary format);
BDS — BD в стандартном формате (BD in standardized format);
BDT — Шаблон биометрических данных (Biometric Data Template);
CCT — Шаблон криптографической контрольной суммы (Cryptographic Checksum Template);
CRT — Шаблон управляющих ссылок (Control Reference Template);
CT — Шаблон конфиденциальности (Confidentiality Template);
DE — Элемент данных (Data Element);
DF — Назначенный файл (Dedicated File);
DO — Информационный объект (Data Object);
DST — Шаблон цифровой подписи (Digital Signature Template);
EFID — Элементарный файл идентификатора (Elementary File ID);
FCI — Контрольная информация файла (File Control Information);
ID — Идентификатор (Identifier);
RD — Эталонные данные (Reference Data);
SE — Безопасная среда (Security Environment);
SM — Безопасный обмен сообщениями (Secure Messaging);
TLV — Тег-длина-значение (Tag-Length-Value);
UQ — Квалификатор применимости (Usage Qualifier);
VIDO — Информационный объект «информация о требованиях к верификации» (Verification requirement Information Data Object);
VIT — Шаблон «информация о требованиях к верификации» (Verification requirement Information Template).

5 Команды для процессов, связанных с биометрической верификацией

Команды для извлечения данных, верификации и аутентификации, определенные по ИСО/МЭК 7816-4, используют при биометрической верификации. Для биометрических данных (например, черты лица, форма ушей, отпечаток пальца, спектр речевых сигналов, образец голоса, клавиатурный почерк) может потребоваться защита от воспроизведения или предъявления данных верификации, полученных от исходных биометрических данных (например, отпечаток пальца, фото анфас). Для предотвращения такого типа нарушения защиты необходимо послать карте данные верификации с криптографической контрольной суммой или цифровую подпись с применением безопасного обмена сообщениями, как определено в ИСО/МЭК 7816-4. Аналогичным образом безопасный обмен сообщениями может быть использован для того, чтобы гарантировать аутентификацию биометрических данных, извлеченных из карты.

5.1 Команды для извлечения биометрической информации

Для извлечения биометрической информации необходимо использовать команды, определенные в ИСО/МЭК 7816-4 в разделе, описывающем обращение к данным.

5.2 Команды, используемые в процессе статической биометрической верификации

Командой, используемой в процессе статической верификации (см. приложение А), является команда VERIFY, определенная в ИСО/МЭК 7816-4. Передаваемой информацией является:

- идентификатор биометрических эталонных данных (т.е. квалификатор эталонных данных);
- данные биометрической верификации.

Данные биометрической верификации могут быть закодированы как информационные объекты BER-TLV (см. таблицу 2). Байт CLA может указывать, что поле данных команды закодировано в BER-TLV (см. ИСО/МЭК 7816-4).

Для комбинированных биометрических схем может использоваться сцепление команд по ИСО/МЭК 7816-8.

5.3 Команды, используемые в процессе динамической биометрической верификации

Чтобы создать задачу, для которой требуется ответ пользователя (см. приложение А), необходимо использовать команду GET CHALLENGE.

Тип задачи в процессе биометрической верификации, например фраза для спектрограммы голоса или фраза для верификации клавиатурного почерка, зависит от биометрического алгоритма, который может быть установлен в P1 команды GET CHALLENGE (см. ИСО/МЭК 7816-4). Или же соответствующий алгоритм может быть выбран при использовании команды MANAGE SECURITY ENVIRONMENT (например, опция SET с CRT AT и DO «квалификатор применимости» и DO «идентификатор алгоритма» в поле данных).

После успешного выполнения команды GET CHALLENGE в карту посылают команду EXTERNAL AUTHENTICATE. Поле данных команды передает соответствующие данные биометрической верификации. Для кодирования данных биометрической верификации применяют те же принципы, что и для команды VERIFY, см 5.1.

6 Элементы данных

6.1 Биометрическая информация

Шаблон биометрической информации (BIT) предоставляет наглядную информацию по соответствующим биометрическим данным. Он предусмотрен картой в ответ на извлечение команды, предшествующей процессу верификации. В таблице 1 определены DO «биометрическая информация».

Таблица 1 — DO «биометрическая информация»

Тег	L	Значение			Наличие
'7F60'	Переменная	Шаблон биометрической информации (BIT)			
		Тег	L	Значение	
		'80'	1	Ссылка на алгоритм для использования в командах VERIFY/EXT.[1] AUTHENTICATE/MANAGE SE[2]	Дополнительно
		'83'	1	Квалификатор эталонных данных для использования в команде VERIFY/EXT.AUTH.[3]/MANAGE SE	Дополнительно
		'A0'	Переменная	DO «биометрическая информация», определенные в настоящем стандарте	Дополнительно
				Орган распределения тегов (см. ИСО/МЭК 7816-6)	Один из этих DO является обязательным, если 'A1' присутствует
		'06'	Переменная	- Идентификатор объекта (OID)	
		'41'	Переменная	- Уполномоченный национальный орган (см. ИСО/МЭК 7816-4)	
		'42'	Переменная	- Эмитент (см. ИСО/МЭК 7816-4)	

Окончание таблицы 1

Тег	L	Значение					Наличие
		'4F'	Переменная	- Идентификатор приложения (AID), идентифицирующий приложение и его провайдера (см. ИСО/МЭК 7816-4) Орган распределения тегов по умолчанию — ИСО/МЭК СТК 1/ПК 37			Один из этих DO является обязательным, если 'A1' присутствует
		'A1'	Переменная	DO «биометрическая информация», заданные органом распределения тегов (указание обязательно, см. выше) См. также пример в приложении С			Обязательно, если 'A0' не присутствует
				Тег	L	Значение	
				'8x'/ 'Ax' '9x'/ 'Bx'	Переменная Переменная	DO, указанные органом распределения тегов ... (простые/составные) ... (простые/составные)	Зависит от DO

[1] EXT. — сокращение от EXTERNAL.
[2] SE — сокращение от Security Environment.
[3] AUTH. — сокращение от AUTHENTICATE.

Примечание — В случае если карта не выполняет процесс верификации, шаблон биометрической информации может также содержать в себе биометрические эталонные данные (см. таблицу 3) и, возможно, произвольные данные (тег '53' или '73'), например для данных, которые должны передаваться системе услуг, если верификация положительна (см. приложение С).

Если несколько BIT присутствуют в рамках одного приложения, то они должны быть сгруппированы, как показано в таблице 2.

Таблица 2 — Шаблон группы BIT

Тег	L	Значение			Наличие
'7F61'	Переменная	Шаблон группы BIT			
		Тег	L	Значение	
		'02'	Переменная	Число BIT в группе	Обязательно
		'7F60'	Переменная	BIT 1	Условно
				...	
		'7F60'	Переменная	BIT 2	Условно

Шаблон группы BIT может быть извлечен, например, с помощью:
- команды GET DATA;
- считывания из файла в соответствующих DF, EFID, найденных в FCI, или
- считывания шаблона SE (см. ИСО/МЭК 7816-4), в котором хранится шаблон группы BIT.

6.2 Биометрические данные

Биометрические данные (данные биометрической верификации, биометрические эталонные данные) могут:
- представлять собой сцепление элементов данных;
- быть в рамках DO «биометрические данные» по ИСО/МЭК 7816-6 или
- представлять собой сцепление DO в рамках шаблона биометрических данных, см. таблицу 3.

Таблица 3 — DO «биометрические данные»

<table>
<tr><th>Тег</th><th>L</th><th colspan="3">Значение</th><th>Наличие</th></tr>
<tr><td>'5F2E'</td><td>Перемен-ная</td><td colspan="3">Биометрические данные</td><td></td></tr>
<tr><td>'7F2E'</td><td>Перемен-ная</td><td colspan="3">Шаблон биометрических данных</td><td></td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td>Значение</td><td></td></tr>
<tr><td></td><td></td><td>'5F2E'</td><td>Перемен-ная</td><td>Биометрические данные</td><td rowspan="3">Присутствует как минимум один из данных DO, если используется шаблон</td></tr>
<tr><td></td><td></td><td>'81'/ 'A1'</td><td>Перемен-ная</td><td>Биометрические данные со стандартным форматом (простые/составные)</td></tr>
<tr><td></td><td></td><td>'82'/ 'A2'</td><td>Перемен-ная</td><td>Биометрические данные с проприетарным форматом (простые/составные)</td></tr>
</table>

Как показано в таблице 3, биометрические данные могут быть разделены на части со стандартным форматом и на части с проприетарным форматом, при этом часть с проприетарным форматом может использоваться, например, для повышения качества работы. Использование биометрических данных со стандартным и проприетарным форматами показано на рисунке 1.

Структура и кодирование биометрических данных зависят от биометрического типа (например, черты лица, отпечаток пальца) и выходят за рамки настоящего стандарта.

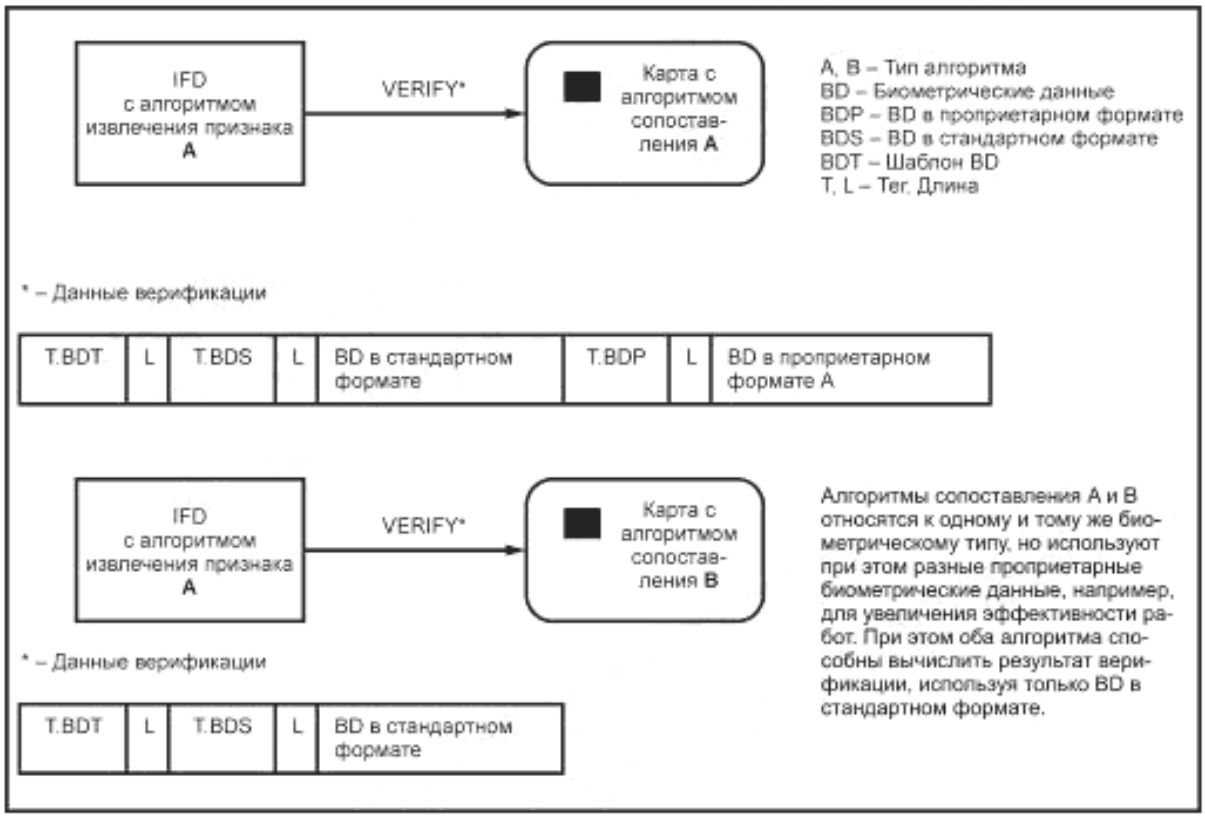


Рисунок 1 — Использование биометрических данных со стандартной и проприетарной структурой

6.3 Информация о требованиях к верификации

6.3.1 Назначение

Текущее требование к верификации обеспечивается либо:

- информационным объектом «информация о требованиях к верификации» VIDO (тег '96', сжатый формат), либо

- шаблоном «информация о требованиях к верификации» VIT (тег 'A6', длинный формат).

VIDO или VIT, если имеются, являются частью информации контрольного параметра файла соответствующего DF или хранятся в расширенном файле FCI (по ИСО/МЭК 7816-4). VIDO или VIT содержат информацию, которая указывает, являются ли эталонные данные для верификации пользователя (т.е. пароли и/или биометрические данные)

- разрешенными или запрещенными и

- применимыми или неприменимыми.

Примечание — Обычно флажок «разрешенный/запрещенный» находится под управлением владельца карты, а флажок «применимый/неприменимый» — под управлением провайдера приложения.

6.3.2 VIDO — сжатый формат

Первый байт VIDO (см. таблицу 4) указывает с помощью битового отображения, какие ключи (т.е. эталонные данные для верификации пользователя) являются разрешенными (бит установлен на 1) или запрещенными (бит установлен на 0). Второй бит указывает с помощью битового отображения, какие ключи являются применимыми (бит установлен на 1) или неприменимыми (бит установлен на 0). Каждый из следующих байтов является ссылкой на ключ. Первая ссылка на ключ соответствует биту b8 на битовой карте, вторая ссылка на ключ — b7, и т.д. Число ссылок на ключи задано неявно длиной VIDO, например, если L меньше или равно 10, то число ссылок на ключи равно L-2.

Таблица 4 — Структура VIDO

Тег VIDO	L	Флажки «разрешенный/ запрещенный»	Флажки «применимый/ неприменимый»	Ссылка на ключ	Ссылка на ключ	...
'96'	Перемен-ная	'xx'	'xx'	'xx'	'xx'	

6.3.3 VIT — длинный формат

VIT представляет информацию в длинном формате, при этом дополнительная информация может предоставляться в DO «квалификатор применимости». DO, которые могут входить в VIT, показаны в таблице 5.

Таблица 5 — Шаблон «информация о требованиях к верификации» (VIT) и вложенные DO

Тег	L	Значение		
'A6'	Пере-менная	Шаблон «информация о требованиях к верификации»		
		Тег	L	Значение
		'90'	1	Флажки «разрешенный/запрещенный» (Флажок DO)
		'95'	1	Квалификатор применимости по ИСО/МЭК 7816-4
		'83'	1	Ссылка на ключ

Флажки «разрешенный/запрещенный» являются обязательными. Как минимум один DO «ссылка на ключ» должен присутствовать. Каждый DO «ссылка на ключ» может предшествовать соответствующему DO «квалификатор применимости». Если с ключом не связан никакой квалификатор применимости, то применимость известна неявно. В данном контексте если квалификатор применимости установлен на ноль, то это значит, что соответствующий ключ не должен использоваться.

Примечание — Не обязательно применять VIT с тегом приложения, который должен быть получен командой GET DATA, потому что FCI или расширенный файл FCI могут быть всегда считаны.

Приложение А
(справочное)

Процесс биометрической верификации

А.1 Сокращения

ICC — Карта на интегральной(ых) схеме(ах) (Integrated Circuit(s) Card);
IFD — Устройство сопряжения (Interface Device);
OID — Идентификатор объекта (Object Identifier);
SM — Безопасный обмен сообщениями (Secure Messaging).

А.2 Процессы регистрации данных и верификации

На рисунке А.1 показана общая (упрощенная) схема процесса регистрации.

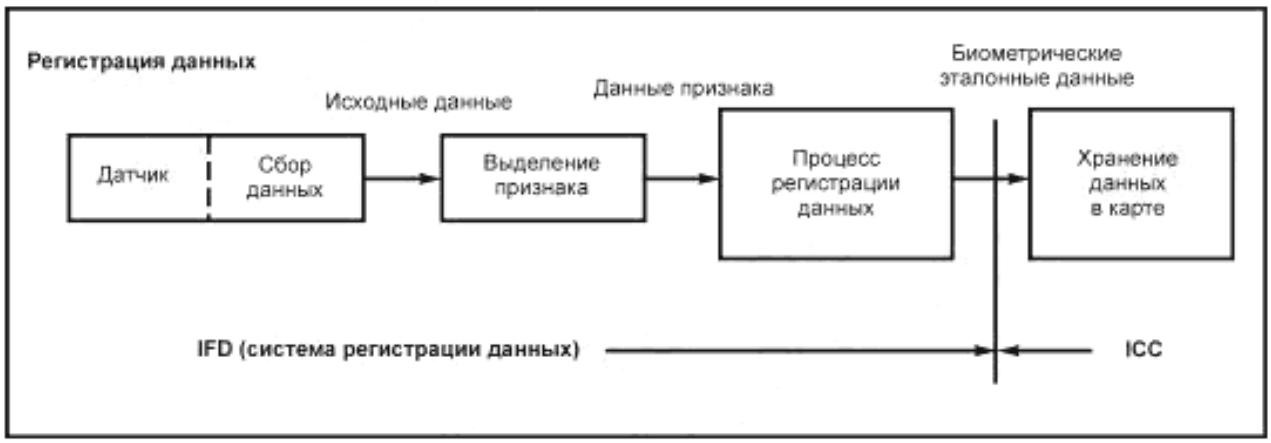


Рисунок А.1 — Общая схема процесса регистрации данных

Датчик и модуль сбора данных рассматриваются как одна логическая единица, хотя они могут быть отдельными модулями. Исходные данные обычно обрабатываются вне карты из-за большого размера исходных данных. Во время такой обработки биометрические признаки выделяются и форматируются для дальнейшего использования. В процессе регистрации данных или на более поздней стадии биометрические эталонные данные, возможно вместе с дополнительной информацией, посылают безопасным способом карте для хранения и последующего применения.

В случае «он-карт» сопоставления, эти данные не могут быть получены после сохранения. В случае «офф-карт» сопоставления, биометрические эталонные данные могут быть получены в качестве части BIT. Биометрические эталонные данные и, возможно BIT целиком, могут быть защищены, например, с помощью цифровой подписи. Также доступ к BIT может быть ограничен, например, доступ возможен только после успешного выполнения процедуры аутентификации.

Биометрические эталонные данные могут быть записаны в карту:

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

Хранение эталонных данных после выдачи карты держателю карты или при предоставлении карты держателю карты рассматривается в приложении В.

На рисунке А.2 показана упрощенная схема для верификации, охватывающая следующие конфигурации:

- с биометрическими эталонными данными и, возможно, параметрами, хранящимися в карте;
- с обработкой путем выявления совпадения и процессом принятия решений в карте;
- с выделением признака, форматированием, обработкой путем выявления совпадения и процессом принятия решений в карте;
- с датчиком на карте и выполнением полного процесса верификации в карте.

Другие конфигурации также возможны.

Примечание — Параметры для принятия решения обычно связаны с процессом принятия решений. Если карта предоставляет биометрические эталонные данные (возможно защищенные криптографическими методами) для внешнего сопоставления (самый нижний случай на рисунке А.2), то параметры для принятия решений могут присутствовать и извлекаться (безопасным способом), если они содержат компоненты, специфичные для пользователя.

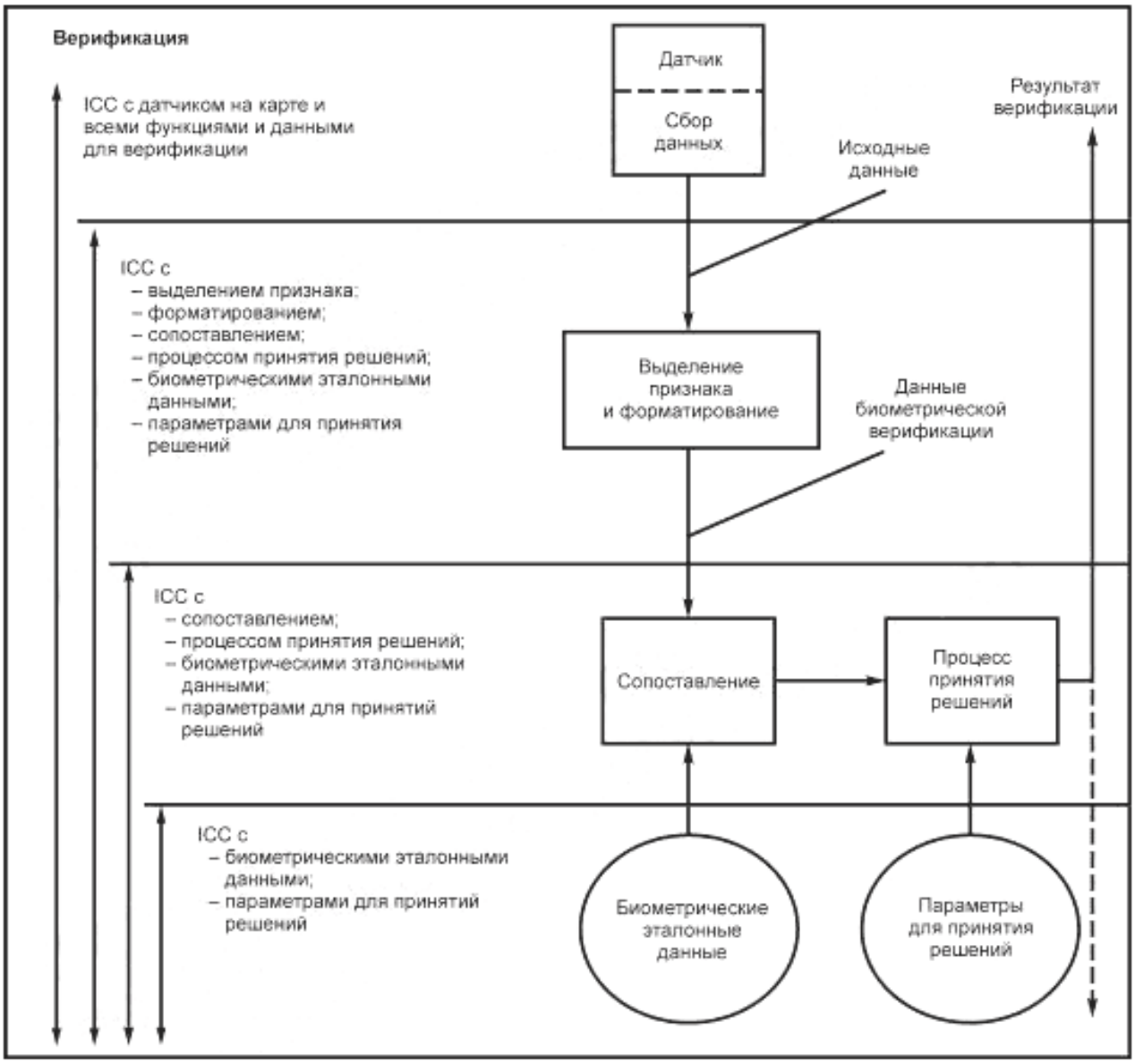


Рисунок А.2 — Общая схема процесса верификации

А.3 Классификация методов биометрической верификации

Принимая во внимание существование различной аппаратуры обмена сообщениями между картой и IFD, используют следующую классификацию:

- Метод статической биометрической верификации — это метод биометрической верификации, при котором требуется представление физического (т.е. статического) признака человека, которого необходимо аутентифицировать (см. тип А), или выполнение зарегистрированного, заранее заданного действия (см. тип В);

- Метод динамической биометрической верификации — это метод биометрической верификации, при котором требуется динамическое действие от человека, которого необходимо аутентифицировать (т.е. реакция человека на биометрическую задачу, см. тип В).

Примеры биометрического типа А:

форма ушей;

черты лица;

форма пальцев;

отпечаток пальца;

форма рук;

радужная оболочка глаза;

форма ладони;
сетчатка глаза;
рисунок вен.

Примечание — Данные биометрические типы могут быть использованы только для статической верификации.

Примеры биометрического типа В:
клавиатурный почерк;
движение губ;
изображение подписи;
спектр речевых сигналов (спектрограмма голоса);
динамическая запись (динамика рукописной подписи).

Примечание — Данные биометрические признаки могут быть использованы при статической верификации или при динамической верификации в зависимости от применения соответствующего типа.

Основными характеристиками признаков биометрического типа А являются:
- уникальный, не поддающийся изменению;
- выбираемый, если существует несколько экземпляров того же класса (например, большой палец, указательный палец);
- открытый, если любой человек может зафиксировать или измерить соответствующий признак (например, лицо, ухо, отпечаток пальца), т.е. соответствующие данные биометрической верификации должны быть представлены карте аутентичным способом (см. приложение В, рисунок В.4).

Основными характеристиками признаков биометрического типа В являются:
- уникальный, но поддающийся изменению;
- зависящий от задачи, если используется динамическая верификация.

На рисунках А.3 и А.4 показаны различия между статической и динамической биометрической верификацией при сопряжении карты в случае сопоставления и процесса принятия решений в карте.

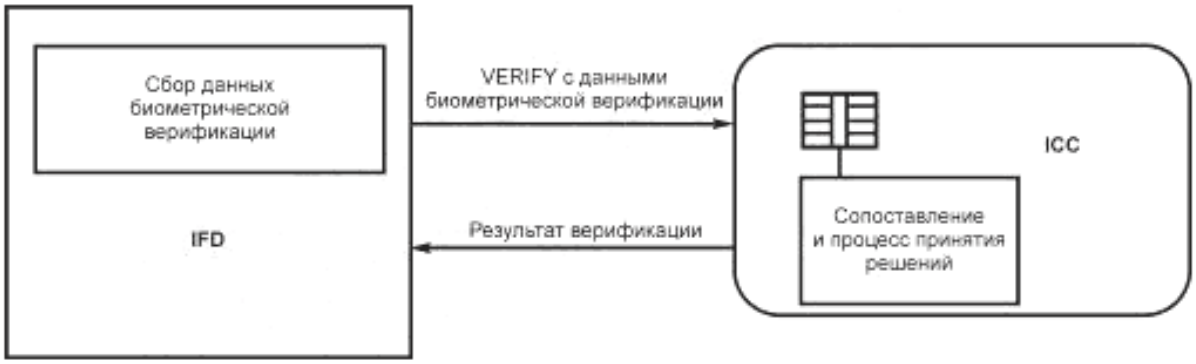
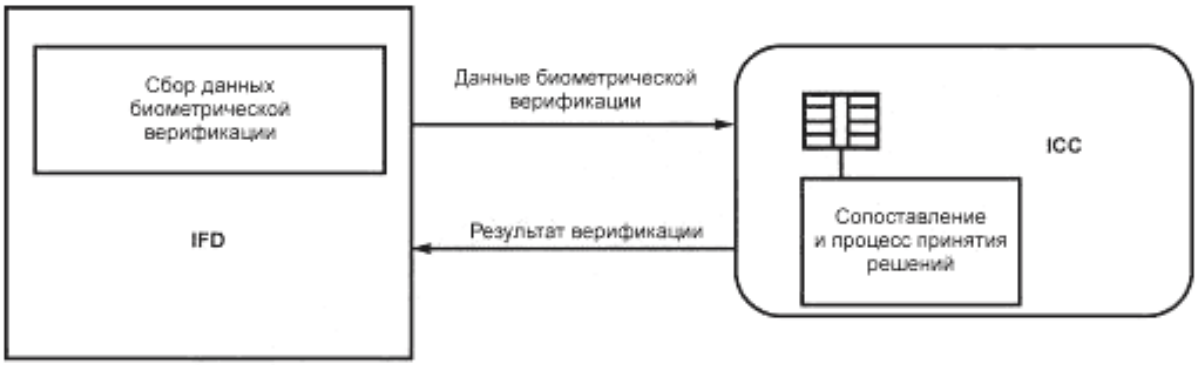


Рисунок А.3 — Команды для статической биометрической верификации

Рисунок А.4 — Команды для динамической биометрической верификации

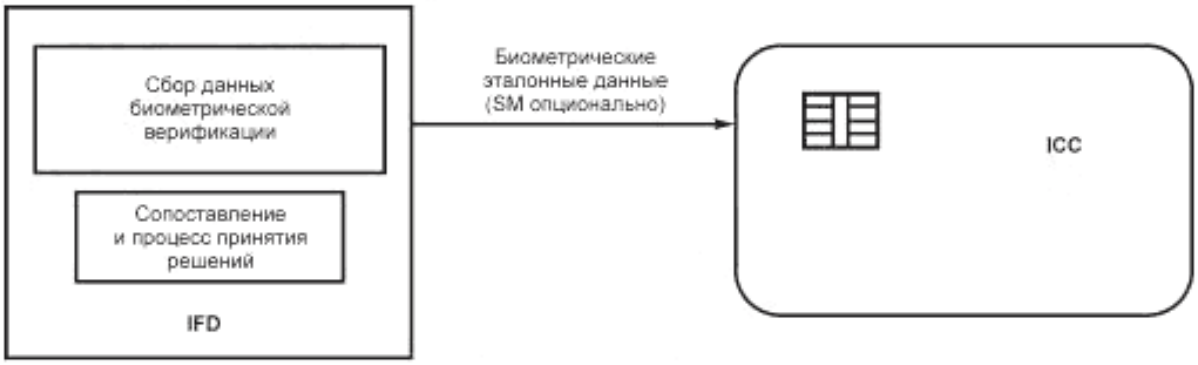
А.4 Сценарии

На рисунках А.5 и А.6 показаны некоторые сценарии, касающиеся биометрической верификации пользователя.

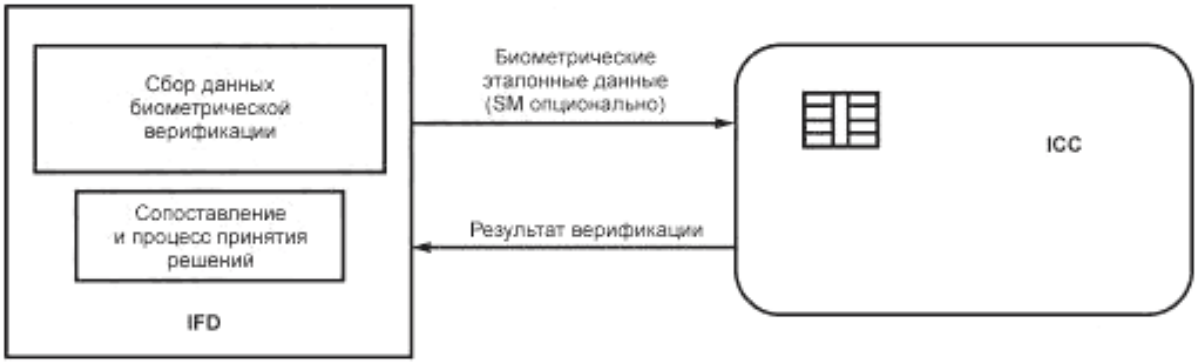


Результат процесса биометрической верификации изменяет состояние защиты карты. Если он также изменяет состояние защиты IFD, то он должен быть защищен с помощью безопасного обмена сообщениями.

Рисунок А.5 — Сценарий с сопоставлением и процессом принятия решений внутри карты



Условия доступа могут быть присоединены к биометрическим эталонным данным



Если результат процесса биометрической верификации изменяет состояние защиты карты, то она должна быть защищена с помощью безопасного обмена сообщениями

Рисунок А.6 — Сценарий с сопоставлением и процессом принятия решений вне карты

А.5 Извлечение информации, касающейся процесса биометрической информации

Для IFD может требоваться информация, касающаяся процесса верификации. Следующий перечень содержит элементы информации, которые могут быть необходимы для IFD:

- биометрический тип (например, отпечаток пальца, черты лица, ...);
- биометрический подтип, если он выделен (например, левый указательный палец);
- владелец формата или тип формата биометрических данных;
- ссылка на алгоритм, если имеется, как, например, в команде MANAGE SECURITY ENVIRONMENT;
- идентификатор биометрических эталонных данных (квалификатор эталонных данных в команде VERIFY или команде EXTERNAL AUTHENTICATE);
- произвольные данные, если имеются.

Приложение В
(справочное)

Примеры регистрации данных и верификации

В.1 Сокращения

AID — Идентификатор приложения (Application Identifier);
AT — Шаблон Аутентификации (Authentication Template);
BIT — Шаблон биометрической информации (Biometric Information Template);
BT — Биометрический тип (Biometric Type);
CRT — Шаблон управляющих ссылок (Control Reference Template);
DO — Информационный объект (Data Object);
DST — Шаблон цифровой подписи (Digital Signature Template);
FCI — Контрольная информация файла (File Control Information);
FO — Владелец формата (Format Owner);
FT — Тип формата (Format Type);
ID — Идентификатор (Identifier);
IFD — Устройство сопряжения (Interface Device);
OID — Идентификатор объекта (Object Identifier);
RD — Эталонные данные (Reference Data);
SM — Безопасный обмен сообщениями (Secure Messaging);
TAT — Шаблон органа распределения тегов (Tag allocation Authority Template);
UQ — Квалификатор применимости (Usage Qualifier);
VIT — Шаблон «информация о требованиях к верификации» (Verification Requirement Information Template);
|| — Сцепление (Concatenation).

В.2 Регистрация данных

Для данного примера предполагается, что карта:

- полностью персонализирована, за исключением хранения биометрических эталонных данных и соответствующего шаблона биометрической информации (это также включает наличие биометрической записи в файле ключа с соответствующими атрибутами для биометрических эталонных данных, т.е. повторение счетчика с начальным значением, восстановление кода с повторением счетчика с начальным значением, флажки разрешенного/запрещенного требования верификации и возможность замены);
- имеет верификацию паролем в дополнение к биометрической верификации.

С помощью команды CHANGE REFERENCE DATA пустые эталонные данные заменяются эталонными данными пользователя в процессе регистрации данных. Выполнение команды CHANGE REFERENCE DATA должно быть связано с условиями секретности, например с установлением необходимого состояния защиты после успешного выполнения процедуры аутентификации, основанной на криптографии, или с успешным предъявлением пароля.

Примечание — Условия секретности для команды CHANGE REFERENCE DATA после того, как произошла запись биометрических эталонных данных, могут отличаться из-за политики безопасности провайдера приложения (например, изменение эталонных данных больше не разрешено после регистрации данных).

После того как биометрические эталонные данные будут записаны, должен быть записан шаблон биометрической информации BIT, который используется IFD в процессе верификации в данном примере. BIT записывается после того, как все типы и подтипы биометрических эталонных данных будут зарегистрированы.

Обычно устройству сопряжения IFD (например, PC, открытый доступ в интернет или банкомат) не известно о том:

- принадлежит ли представленная карта пользователю, к которому применяют биометрические характеристики;
- имеет ли карта биометрический алгоритм, поддерживаемый IFD;
- какой биометрический тип используется;
- какое имеет значение соответствующая ссылка на ключ (т.е. квалификатор эталонных данных);
- какие должны соблюдаться параметры алгоритма сопоставления, специфичного для реализации (например, ограничение числа деталей, которые должны быть переданы в данные верификации).

Таким образом, шаблон биометрической информации BIT должен предоставлять следующую информацию:

- о квалификаторе биометрических эталонных данных;
- об OID органа распределения тегов и указании формата для данных верификации;

- о биометрическом типе и, возможно, о зарегистрированном биометрическом подтипе (например, правый большой палец);
- о дополнительных информационных объектах, если имеются;
- о повторении соответствующих DO, если, например, второй биометрический тип зарегистрирован.

На рисунке В.1 показаны команды, которые могут быть выполнены таким образом в процессе регистрации данных.

Команда/Ответ	Значение
VERIFY <Пароль> → ← OK	Установление состояния защиты для хранения биометрических эталонных данных
CHANGE RD <Биометрические эталонные данные> → ← OK	Замена пустых эталонных данных зарегистрированными биометрическими эталонными данными
SELECT <ID файла> → ← OK	Выбор элементарного файла для хранения шаблона биометрической информации BIT (должен быть извлечен с помощью GET DATA)
UPDATE BINARY <BIT> → ← OK	Хранение шаблона биометрической информации BIT

Рисунок В.1 — Команды для регистрации данных (примеры)

Примечания

1 Может возникнуть необходимость защитить регистрацию данных с помощью безопасного обмена сообщениями.

2 Для хранения и извлечения информации могут быть использованы и другие команды, чем те, что описаны в ИСО/МЭК 7816-4. Данное положение также действительно для рисунков В.4, В.6 и В.7.

На рисунке В.2 показан BIT со своими DO.

Рисунок В.2 — Пример шаблона биометрической информации (BIT), тегов, назначенных специальным органом распределения тегов

Примечание — Теги внутри шаблона 'A1' определяются обозначенным органом распределения тегов.

В.3 Верификация с помощью простого биометрического метода

Процесс верификации начинается с извлечения шаблона биометрической информации, например, применив команду GET DATA. Если IFD поддерживает требуемый формат данных биометрической верификации, как указано в BIT, и пользователь представил соответствующий биометрический объект, то данные верификации вычисляются и передаются карте, используя команду VERIFY (см. рисунок В.3).

Команда/Ответ	Значение
SELECT <AID> → OK ←	Выбор приложения с помощью идентификатора приложения (AID)
GET DATA <Тег BIT> → Шаблон биометрической информации ←	Извлечение шаблона биометрической информации BIT
VERIFY <Данные биометрической верификации> → OK ←	Верификация пользователя

Рисунок В.3 — Команды для верификации без использования безопасного обмена сообщениями (примеры)

Примечание — Если шаблон биометрической информации не присутствует, это означает в данном примере, что соответствующий пользователь не использует биометрические характеристики.

Если данные биометрической верификации общедоступные (например, черты лица, отпечаток пальца, форма ушей), то существует необходимость защитить их с помощью безопасного обмена сообщениями (см. рисунок В.4).

Команда/Ответ	Значение
SELECT <AID> → OK ←	Выбор приложения с идентификатором приложения (AID)
GET DATA <Тег BIT> → Шаблон биометрической информации ←	Извлечение шаблона биометрической информации (BIT)
MANAGE <DO Ссылка на ключ> → OK ←	Установление CRT DST с открытым ключом для верификации сертификата
VERIFY CERTIFICATE <сертификат> → OK ←	Верификация сертификата, принадлежащего биометрическому элементу
GET CHALENGE → Произвольное число ←	Запрашивающая задача, которая должна использоваться для безопасного обмена сообщениями
EXTERNAL AUTHENTICATE <данные, касающиеся аутентификации> → Данные, касающиеся аутентификации ←	Внешняя аутентификация с формированием ключей SM
VERIFY <Данные биометрической верификации, защищенные SM> → OK ←	Верификация пользователя с данными верификации, защищенными с помощью SM; ответ может быть также защищен с помощью SM

Рисунок В.4 — Команды для верификации с использованием безопасного обмена сообщениями (примеры)

Примечание — Описание безопасного обмена сообщениями (SM) изложено в ИСО/МЭК 7816-4.

В данном примере процесс верификации начинается с извлечения шаблона «информация о требованиях к верификации» (VIT) и соответствующего шаблона биометрической информации (BIT), которые могут храниться, например, в FCI расширенного файла (ID файла неявно известен). VIT содержит информацию о том, доступна ли биометрическая верификация и/или верификация с помощью пароля, разрешены или запрещены и какие соответствующие квалификаторы эталонных данных (KeyRef) должны использоваться при сопряжении с картой. BIT содержит в данном примере (см. рисунок В.5) информацию о ссылке на алгоритм, специфичный для карты (AlgID), квалификаторе эталонных данных (KeyRef) и дополнительную информацию, такую как биометрический тип, владелец формата и тип формата.

Рисунок В.5 — Пример шаблона биометрической информации (BIT)

Если IFD и представленная карта поддерживают один и тот же механизм, а пользователь представил соответствующие биометрические признаки, то данные верификации должны быть вычислены и переданы карте, используя команду VERIFY, которая предшествует команде MANAGE SECURITY ENVIRONMENT, чтобы выбрать метод верификации (см. рисунок В.6).

Команда/Ответ	Значение
SELECT <ID файла> → OK ←	Выбор расширенного файла FCI
READ BINARY → VIT ‖ BIT ←	Извлечение шаблона «информация о требованиях к верификации» VIT
MANAGE SE <DO UQ ‖ DO Ссылка на алгоритм ‖ DO Ссылка на ключ> → OK ←	Установление CRT AT с Квалификатором применимости UQ, Ссылки на алгоритм и Ссылка на ключ
VERIFY <Данные биометрической верификации> → OK ←	Верификация пользователя

Рисунок В.6 — Команды для верификации без использования безопасного обмена сообщениями (примеры)

Если статическая биометрическая верификация требует информацию от карты перед началом верификации, то такая информация может быть представлена в шаблоне биометрической информации.

В.4 Доступ к BIT в случае «офф-карт» сопоставления

BIT, возможно, в комбинации с другими данными (например, данными о водительском удостоверении) может быть защищен, например, подписью органа, выдающего удостоверение (примеры защиты таких данных см. в приложении D). Таким образом, BIT может быть извлечен простой командой READ BINARY, см. рисунок В.7.

Команда/Ответ	Значение
SELECT <ID файла> → ОК ←	Выбор файла, содержащего биометрическую информацию
READ BINARY → BIT ←	DO BIT содержит шаблон безопасного обмена сообщениями, например для гарантии аутентичности данных биометрической идентификации

Рисунок В.7 — Команды для извлечения BIT (пример)

Доступ к BIT может быть ограничен, т.е. перед началом считывания должна быть выполнена процедура аутентификации, как показано на рисунке В.8.

Команда/Ответ	Значение
GET CHALLENGE → ОК ←	Получение случайного числа
EXT. AYTHENTICATE <данные, касающиеся аутентификации> → BIT ←	Аутентификация объекта, который имеет право доступа к BIT
READ BINARY → BIT ←	Считывание BIT

Рисунок В.8 — Команды для извлечения BIT после выполнения процедуры аутентификации (пример)

Если BIT должен быть передан, например, по интернету, то для обеспечения конфиденциальности и аутентичности может возникнуть необходимость применения безопасного обмена сообщениями, как показано на рисунке В.4.

Приложение С
(справочное)

Информационные объекты «биометрическая информация»

В настоящем приложении определены информационные объекты «биометрическая информация», основанные на единой структуре CBEFF.

С.1 Сокращения

BDB — Блок биометрических данных (Biometric Data Block);
BHT — Шаблон биометрического заголовка (Biometric Header Template);
BIT — Шаблон биометрической информации (Biometric Information Template);
CBEFF — Единая структура форматов обмена биометрическими данными (Common Biometric Exchange Formats Framework);
DO — Информационный объект (Data Object);
IBIA — Международная ассоциация биометрической промышленности (International Biometric Industry Association);
IC — Интегральная(ые) схема(ы) (Integrated Circuit(s));
MAC — Аутентификационный код сообщения (Message Authentication Code);
OID — Идентификатор объекта (Object Identifier);
PID — Идентификатор продукта (Product Identifier);
SE — Безопасная среда (Security Environment);
SMT — Шаблон безопасного обмена сообщениями (Secure Messaging Template);
TLV — Тег-Длина-Значение (Tag-Length-Value).

С.2 Информационные данные биометрической информации, используемые в случае «он-карт» сопоставления

С.2.1 Использование простого биометрического типа или биометрического подтипа

До начала выполнения процесса верификации информация может быть извлечена из карты, представляющей области данных, которые можно наблюдать внешними устройствами при выполнении процесса верификации. Соответствующие информационные объекты показаны в таблице С.1.

Таблица С.1 — Информационные объекты «биометрическая информация» в случае «он-карт» сопоставления

Тег	L	Значение					Наличие
'7F60'	Переменная	Шаблон биометрической информации (BIT)					
		Тег	L	Значение			
		'80'	1	Ссылка на алгоритм для использования в командах VERIFY/EXT. AUTHENTICATE/MANAGE SE по ИСО/МЭК 7816-4, см. примечание 5			Дополнительно
		'83'	1	Квалификатор эталонных данных для использования в командах VERIFY/EXT.AUTH./MANAGE SE по ИСО/МЭК 7816-4			Дополнительно
		'06'	Переменная	OID стандартного объекта CBEFF, см. примечание 6			Обязательно, если не используется по умолчанию
		'A1'	Переменная	Шаблон биометрического заголовка (BHT) в соответствии с CBEFF			Обязательно
				Тег	L	Значение	
				'80'	2	Версия заголовка заказчика (по умолчанию '0101')	Обязательно, если не используется по умолчанию

Окончание таблицы С.1

Тег	L	Значение					Наличие
				'90'	Переменная	Индекс, уникальный идентификатор, используемый для обращения к этим биометрическим данным, установленным в контексте приложения вне карты	Дополнительно
				'81'	1-3	Биометрический тип, см. таблицу С.2	Дополнительно
				'82'	1	Биометрический подтип, см. таблицу С.3	Дополнительно, используется только с биометрическим типом
				'83'	7	Дата и время создания биометрических данных (CCYYMMDDhhmmss[1])	Дополнительно
				'84'	Переменная	Разработчик	Дополнительно
				'85'	8	Период действия (от CCYYMMDDhhmmss до CCYYMMDDhhmmss)	Дополнительно
				'86'	2	Идентификатор продукта (PID), который создал данные биометрической идентификации, значение, определенное IBIA, см. www.ibia.org	Дополнительно
				'87'	2	Владелец формата для данных биометрической верификации, значения, определенного IBIA, см. www.ibia.org	Обязательно
				'88'	2	Тип формата данных биометрической верификации, определенных владельцем формата	Обязательно
				'91'/'B1'	Переменная	Параметры алгоритма биометрического сопоставления (простые, составные), см. примечания 2 и 7	Дополнительно

[1] Год, месяц, число, час, минута, секунда.

Примечания

1 Представлены только те информационные объекты из CBEFF, которые связаны с сопоставлением с картой.

2 Дополнительные информационные объекты, которые не представлены в основной структуре CBEFF.

3 В таблице С.1 блок биометрических данных по ИСО/МЭК 19785 не присутствует, т.е. эталонные данные записаны в карту по отдельности и не в этот BIT, а данные биометрической идентификации должны быть представлены, используя команду VERIFY.

4 В таблице С.1 не представлено информационное наполнение, так как обычно доступ к информационному наполнению, если он используется приложением, предоставляется после успешного выполнения биометрической верификации. Информационное наполнение может быть извлечено, используя команды доступа, такие как GET DATA или READ BINARY.

5 Внешние устройства (например, IFD) используют данные о владельце формата/типе формата для идентификации необходимой структуры для данных верификации. К алгоритму сопоставления в карте обращаются с помощью ссылки на алгоритм.

6 Если используется версия стандарта ИСО для CBEFF (ИСО/МЭК 19785), то OID связанного со стандартом ИСО объекта (ИСО/МЭК СТК 1/ПК 37) является значением по умолчанию, т.е. DO с тегом '06' может отсутствовать. Если OID ссылается на NISTIR 6529, то используют OID для Регистра объектов компьютерной безопасности (CSOR[1)]) при NIST {join-iso-itu-t (2) country (16) us (840) organization (1) gov (101) csor (3)} (в шестнадцатеричном кодировании OID: '608648016503').

[1)] Computer Security Object Register.

7 DO обеспечивает специальными параметрами для реализации алгоритма «он-карт» сопоставления, например, максимальное число мелких деталей, ожидаемых в данных биометрической верификации. Содержание такого DO определяется владельцем формата.

Таблица С.2 — Биометрический тип по ИСО/МЭК 19785

Наименование биометрического типа	Значение
Информация не предоставлена	'00'
Использование многомерной биометрии	'01'
Черты лица	'02'
Голос	'04'
Отпечаток пальца	'08'
Радужная оболочка глаза	'10'
Сетчатка глаза	'20'
Форма ладони	'40'
Динамика рукописной подписи	'80'
Динамика удара по клавишам (клавиатурный почерк)	'0100'
Движение губ	'0200'
Тепловое изображение лица	'0400'
Тепловое изображение руки	'0800'
Походка	'1000'
Запах тела	'2000'
ДНК	'4000'
Форма ушей	'8000'
Форма пальцев	'010000'
Отпечаток ладони	'020000'
Рисунок вен	'040000'
Отпечаток ступни	'080000'
Другие значения RFU[1)]	
[1)] RFU — Зарезервированы для использования в будущем.	

Примечание — Некоторые биометрические типы могут быть неприменимыми для приложений используемых карт.

Таблица С.3 — Биометрический подтип по ИСО/МЭК 19785

b8	b7	b6	b5	b4	b3	b2	b1	Биометрический подтип
0	0	0	0	0	0	0	0	Информация не предоставлена
						0	1	Правый
						1	0	Левый
			0	0	0			Нет значения
			0	0	1			Большой палец
			0	1	0			Указательный палец
			0	1	1			Средний палец
			1	0	0			Безымянный палец
			1	0	1			Мизинец
								Другие значения RFU

С.2.2 Использование стандартных и проприетарных форматов биометрических данных

В случаях, когда данные биометрической верификации состоят из данных биометрической верификации со стандартной структурой, за которыми следуют данные биометрической верификации со структурой, определенной изготовителем, вложенная структура BHT должна применяться, как показано в таблице С.4

Таблица С.4 — BIT со сложенными BIT для биометрических данных стандартного и проприетарного форматов (пример)

<table>
<tr><td>Тег</td><td>L</td><td colspan="8">Значение</td></tr>
<tr><td>'7F60'</td><td>Переменная</td><td colspan="8">BIT</td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td colspan="6">Значение</td></tr>
<tr><td></td><td></td><td>'80'</td><td>1</td><td colspan="6">Ссылка на алгоритм</td></tr>
<tr><td></td><td></td><td>'83'</td><td>1</td><td colspan="6">Квалификатор эталонных данных</td></tr>
<tr><td></td><td></td><td>'06'</td><td>Переменная</td><td colspan="6">OID стандартного объекта CBEFF, см. примечание 6 таблицы С.1</td></tr>
<tr><td></td><td></td><td>'A1'</td><td>Переменная</td><td colspan="6">BHT (уровень 1)</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Тег</td><td>L</td><td colspan="4">Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td>...</td><td></td><td colspan="4">Общие DO, см. таблицу С.1</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'A1'</td><td>Переменная</td><td colspan="4">BHT 1 (уровень 2)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>L</td><td colspan="2">Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'87'</td><td>2</td><td colspan="2">Владелец формата для данных биометрической верификации, например идентификатор владельца формата ИСО/МЭК СТК 1/ПК 37</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'88'</td><td>2</td><td colspan="2">Тип формата данных биометрической верификации, определенных владельцем формата</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'A2'</td><td>Переменная</td><td colspan="4">BHT 2 (уровень 2)</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>Тег</td><td>L</td><td colspan="2">Значение</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'87'</td><td>2</td><td colspan="2">Владелец формата для данных биометрической верификации, например изготовитель карт</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>'88'</td><td>2</td><td colspan="2">Тип формата данных биометрической верификации, определенных владельцем формата</td></tr>
</table>

С.2.3 Использование нескольких биометрических типов или биометрических подтипов

Если в пределах одного и того же приложения несколько типов биометрических типов или биометрических подтипов используются независимо и обращение к ним происходит с помощью разных квалификаторов эталонных данных (с одним паролем для подписи и разными паролями для аутентификации), то применяют группу структур BIT с вложенными BIT, см. таблицу С.5.

Таблица С.5 — Шаблон группы BIT с вложенными BIT для приложений с несколькими эталонными данными, имеющими свой квалификатор эталонных данных (примеры)

Тег	L	Значение						
'7F60'	Переменная	Шаблон группы биометрической информации						
		Тег	L	Значение				
		'02'	1	'02' = Число BIT				
		'7F60'	Переменная	BIT 1				
				Тег	L	Значение		
				'80'	1	Ссылка на алгоритм		
				'83'	1	Квалификатор эталонных данных		
				'06'	Переменная	OID стандартного объекта CBEFF, см. примечание 6 таблицы С.1		
				'A1'	Переменная	ВНТ		
						Тег	L	Значение
						...		
						'81'	1-3	Биометрический тип, например отпечаток пальца
						'82'	1	Биометрический подтип, например правый указательный палец
						'87'	2	Владелец формата для данных биометрической верификации
						'88'	2	Тип формата данных биометрической верификации, определенных владельцем формата
		'7F60'	Переменная	BIT 2				
				Тег	L	Значение		
				'80'	1	Ссылка на алгоритм		
				'83'	1	Квалификатор эталонных данных		
				'06'	Переменная	OID стандартного объекта CBEFF, см. примечание 6 таблицы С.1		
				'A1'	Переменная	ВНТ		
						Тег	L	Значение
						...		
						'81'	1-3	Биометрический тип, например отпечаток пальца
						'82'	1	Биометрический подтип, например левый указательный палец
						'87'	2	Владелец формата для данных биометрической верификации
						'88'	2	Тип формата данных биометрической верификации, определенных владельцем формата

С.2.4 Использование мультимодальной биометрии

В случаях, когда необходимо верифицировать несколько биометрических признаков (мультимодальная или комбинированная биометрия), например для того, чтобы получить доступ к конкретным данным или специальному ключу, применяют группу BIT с вложенными BIT, и верификация выполняется при передаче нескольких команд VERIFY. Условия доступа, связанные с соответствующим защищенным объектом, определяют, какая комбинация биометрических признаков должна быть успешно верифицируема.

С.2.5 Представление данных биометрической верификации

Кодирование и формат команд биометрической верификации, который передает данные биометрической верификации в карту, выходят за рамки ИСО/МЭК 7816-4. Возможности кодирования для поля данных команды изложены в подразделе 6.2 ИСО/МЭК 7816-11. На рисунке С.1 показан пример поля данных команды, связанный с примером, представленным в таблице С.4.

Рисунок С.1 — Шаблон биометрических данных в поле данных команды (примеры)

С.3 Информационные объекты «биометрическая информация», используемые в случае «офф-карт» сопоставления

С.3.1 Общая структура и применение

Информационные объекты для «офф-карт» сопоставления представлены в качестве BIT, который содержит:
- шаблон биометрического заголовка BHT;
- блок биометрических данных BDB, состоящий из биометрических эталонных данных с последующим информационным наполнением и
- дополнительных DO, связанных с безопасностью, см. С.3.4.

Использование структур данных, представленных в последующих разделах, относится не только к картам IC, т.е. структуры данных могут быть также использованы в других типах карт, например в картах с магнитной полосой, картах с оптической памятью или картах с двумерным штрихкодом.

С.3.2 Применение простого биометрического типа или биометрического подтипа

В таблице С.6 определены DO, связанные с сопоставлением вне карты, если используются простой биометрический тип или подтип.

Таблица С.6 — Информационные объекты «биометрическая информация», используемые в случае «офф-карт» сопоставления

Тег	L	Значение					Наличие
'7F60'	Переменная	Шаблон биометрической информации (BIT)					
		Тег	L	Значение			
		'06'	Переменная	OID стандартного объекта CBEFF, см. примечание 6 таблицы С.1.			Обязательно, если не используется по умолчанию
		'A1'	Переменная	Шаблон биометрического заголовка (BHT) в соответствии с CBEFF			Обязательно
				Тег	L	Значение	

Окончание таблицы С.6

Тег	L	Значение					Наличие
				'80'	2	Номер версии заголовка заказчика (по умолчанию '0101')	Обязательно, если не используется по умолчанию
				'90'	Переменная	Индекс, уникальный идентификатор, используемый для обращения к этим биометрическим данным, установленным в контексте приложения вне карты	Дополнительно
				'81'	1-3	Биометрический тип, см. таблицу С.2	Дополнительно
				'82'	1	Биометрический подтип, см. таблицу С.3	Дополнительно, используется только с биометрическим типом
				'83'	7	Дата и время создания биометрических данных (CCYYMMDDhhmmss)	Дополнительно
				'84'	Переменная	Разработчик	Дополнительно
				'85'	8	Период действия (от CCYYMMDDhhmmss до CCYYMMDDhhmmss)	Дополнительно
				'86'	2	Идентификатор продукта (PID), который создал данные биометрической идентификации, значение, определенное IBIA, см. www.ibia.org	Дополнительно
				'87'	2	Владелец формата для данных биометрической верификации, значения, определенного IBIA, см. www.ibia.org	Обязательно
				'88'	2	Тип формата данных биометрической верификации, определенных владельцем формата	Обязательно
		'5F2E'/'7F2E'	Переменная	Биометрические эталонные данные (простые/составные, см. таблицу С.7)			Обязательное
		'53'/'73'	Переменная	Произвольные данные для информационного наполнения (простое/составное), см. примечания 2 и 3			Дополнительное

Примечания

1 Только те информационные объекты из CBEFF представлены, которые относятся к «офф-карт» сопоставлению.

2 Дополнительные информационные объекты, которые не представлены в основной структуре CBEFF.

3 Информационное наполнение, если имеется, доступно внешним устройствам, когда верификация произошла успешно.

Главное отличие в таблице С.1 — это то, что DO для ссылки на алгоритм и квалификатор эталонных данных (ссылка на ключ при использовании картой) не присутствуют и находятся вместо блока биометрических данных (BDB), состоящего из биометрических эталонных данных, и, возможно, присоединенное информационное наполнение следует за шаблоном биометрического заголовка BHT. Так называемый блок подписи (SB) может также присутствовать и закодироваться по ИСО/МЭК 7816, см. С.3.4.

Таблица С.7 — Шаблон биометрических данных

Тег	L	Значение		
'7F60'	Переменная	Шаблон биометрических данных		
		DO, которые могут быть включены в шаблон биометрических данных		
		Тег	L	Значение
		'80'/ 'A0'	Переменная	Вызов подсказки пользователю (простой/составной, см. таблицу С.8) Данный DO относится только к динамическим биометрическим типам
		'81'/ 'A1'	Переменная	Биометрические данные со стандартной структурой (простой/составной)
		'82'/ 'A2'	Переменная	Биометрические данные с проприетарной структурой (простой/составной)

Таблица С.8 — Шаблон задач

Тег	L	Значение		
'A0'	Переменная	Шаблон задач		
		DO, которые могут быть включены в шаблон задач		
		Тег	L	Значение
		'90'	Переменная	Квалификатор задач '00' = Информация не предоставлена (не определена) '01' = кодирование UTF8 (по умолчанию) Другие значения RFU
		'80'	Переменная	Задача

С.3.3 Применение вложенных структур

В таблице С.9 кратко изложен пример применения вложенных структур. Главное отличие от таблицы С.5 — указатель на биометрические эталонные данные (т.е. квалификатор эталонных данных) автоматически заменяется биометрическими эталонными данными.

Таблица С.9 — Шаблон группы BIT с вложенными BIT для приложений с биометрическими эталонными данными нескольких биометрических типов (примеры)

Тег	L	Значение				
'7F60'	Переменная	Шаблон группы биометрической информации				
		Тег	L	Значение		
		'02'	1	Число BIT в группе шаблонов		
		'7F60'	Переменная	BIT 1		
				Тег	L	Значение
				'06'	Переменная	OID стандартного объекта CBEFF, см. примечание 6 таблицы С.1
				'A1'	Переменная	BHT

Окончание таблицы С.9

Тег	L	Значение						
						Тег	L	Значение
						'81'	1-3	Биометрический тип, например черты лица
						'87'	2	Владелец формата для биометрических эталонных данных
						'88'	2	Тип формата биометрических эталонных данных, определенных владельцем формата
				'7F60'	Переменная	Биометрические эталонные данные		
		'7F60'	Переменная	BIT 2				
				Тег	L	Значение		
				'06'	Переменная	OID стандартного объекта CBEFF, см. примечание 6 таблицы С.1		
				'A1'	Переменная	BHT		
						Тег	L	Значение
						'81'	1-3	Биометрический тип, например отпечаток пальца
						'82'	1	Биометрический подтип, например левый указательный палец
						'87'	2	Владелец формата для биометрических эталонных данных
						'88'	2	Тип формата биометрических эталонных данных, определенных владельцем формата
				'5F2E'	Переменная	Биометрические эталонные данные		

С.3.4 Вопросы безопасности

Некоторые возможности, как обеспечить безопасность BIT или как предоставить доступ к BIT и передать его безопасным способом, изложены в приложениях B и D. Признаки безопасности, описанные в ИСО/МЭК 19785, относительно:

- указания дополнительно выбираемых средств безопасности;
- указания дополнительно выбираемых средств по обеспечению целостности;
- обеспечения поля для подписи или MAC —

полностью поддерживаются при использовании шаблона безопасного обмена сообщениями SMT и соответствующих DO (см. приложение D). Указания дополнительно выбираемых средств безопасности и обеспечения целостности в двух специальных полях в BHT не требуется, так как наличие криптограммы, цифровой подписи или MAC указано соответствующими тегами. Простой пример применения SMT показан на рисунке С.2. Далее, в приложении D, даны более сложные примеры.

T.BIT	L.BIT	T.SMT	L.SMT	T.PV	L.PV	Простое значение PV = BIT – DO (L = L.PV) (OID ‖ BHT ‖ Биометрические данные)	T.DS	L.DS	Цифровая подпись DS
'7F60'	Переменная	'7D'	Переменная	'81'	Переменная	'06… ‖ A1… ‖ 5F2E'	'9E'	Переменная	…

Рисунок С.2 — Защищенный шаблон биометрических данных (пример)

С.4 Сведения о регистрации IBIA

Соответствие CBEFF требует, чтобы владельцы формата зарегистрировали в IBIA заданный уникальный идентификатор владельца формата. Типы формата назначаются владельцем формата и представляют собой формат специальных биометрических данных, указанных владельцем формата. Рекомендуется, чтобы владельцы формата регистрировали типы формата, применяемые в IBIA для архивирования и публикации. IBIA также регистрирует ID продукта (см. таблицы С.1 и С.6). Число гарантированно должно быть уникальным.

IBIA не будет определять значения от 'FFF0' до 'FFFE' для владельцев формата и ID продукта. Данные значения доступны для испытаний.

Сведения о регистрации см. www.ibia.org.

Приложение D
(справочное)

Применение шаблона безопасного обмена сообщениями

D.1 Сокращения

BD — Биометрические данные (Biometric Data);
BER — Базовые правила кодирования (Basic Encoding Rules);
BHT — Шаблон биометрического заголовка (Biometric Header Template);
BIT — Шаблон биометрической информации (Biometric Information Template);
CC — Криптографическая контрольная сумма (Cryptographic Checksum);
CCT — Шаблон криптографической контрольной суммы (Cryptographic Checksum Template);
CT — Шаблон конфиденциальности (Confidentiality Template);
CG — Криптограмма (Cryptogram);
DE — Элемент данных (Data Element);
DO — Информационный объект (Data Object);
DS — Цифровая подпись (Digital Signature);
DST — Шаблон цифровой подписи (Digital Signature Template);
KR — Ссылка на ключ (Key Reference);
L — Длина (Length);
MAC — Аутентификационный код сообщения (Message Authentication Code);
PD — Персональные данные (Personal Data);
PDT — Шаблон персональных данных (Personal Data Template);
PV — Простое значение (Plain Value);
SM — Безопасный обмен сообщениями (Secure Messaging);
SMT — Шаблон безопасного обмена сообщениями (Secure Messaging Template);
T — Тег (Tag);
TLV — Тег-длина-значение (Tag-Length-Value);
|| — Сцепление (Concatenation).

D.2 Информационные объекты, относящиеся к безопасному обмену сообщениями, и их применение

Может возникнуть необходимость защитить шаблон биометрической информации BIT в том случае, когда карта используется в качестве носителя BIT (см. также NISTIR 6529 и ANSI X.9.84):

- BIT с конфиденциальностью (криптографическая защита);
- BIT с целостностью (подписанный или защищенный с помощью MAC);
- BIT с конфиденциальностью и целостностью.

Средства для конфиденциальности или целостности в содержании карты обеспечиваются с помощью безопасного обмена сообщениями (SM), как определено в ИСО/МЭК 7816-4. Существует два метода:

1) до считывания BIT ключи SM для обеспечения конфиденциальности и целостности динамически устанавливаются с помощью доставки ключей или механизмов согласования ключей;
2) BIT защищен сам по себе статичным способом, т.е. при применении метода шаблона SM, как описано ниже.

Если поле значения BIT должно быть защищено статичным способом, то поле значения включается в шаблон SM, в котором:

- все информационные объекты, оставшиеся как незашифрованный текст, помещаются в шаблон простого значения;
- все информационные объекты, которые должны быть зашифрованы, помещаются в криптограмму

и, если для обеспечения целостности требуется, присутствует криптографическая контрольная сумма или DO «цифровая подпись». Если необходимы информационные объекты, такие как ссылка на алгоритм или ссылка на ключ, позволяющие системе обслуживания верифицировать целостность и восстановить простое значение зашифрованных данных, то они присутствуют в шаблонах управляющих ссылок (см. рисунок D.1).

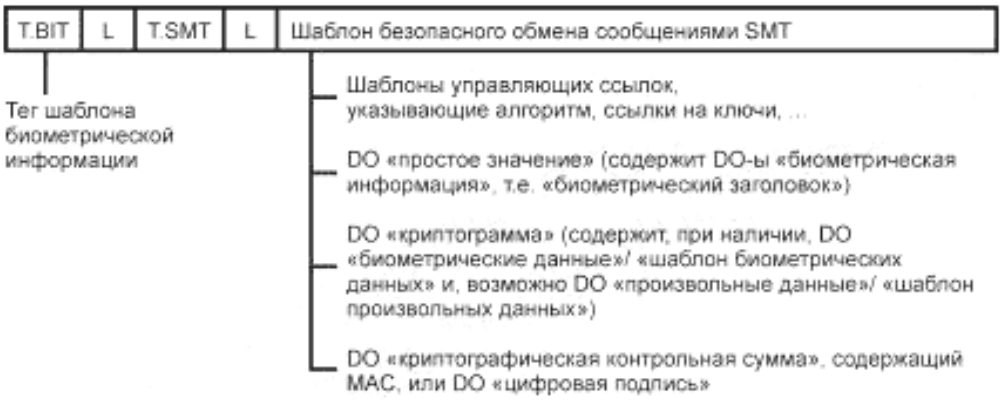


Рисунок D.1 — Шаблон биометрической информации в сочетании с SMT

Кодирование DO-ов, относящихся к шаблону безопасного обмена сообщениями SMT, показано в таблице D.1.

Таблица D.1 — Информационный объект SMT (подмножество)

Тег	L	Значение		
'7D'	Переменная	Шаблон безопасного обмена сообщениями SMT		
		Тег	L	Значение
		'xx'	Переменная	Шаблон контрольного управления, см. таблицу D.2 (защищен с помощью аутентификации)
		'81'	Переменная	Простое значение (PV), состоящее из последовательности DE-ов или DO-ов, кодированных в BER-TLV, но не DO, относящихся к SM, см примечание (защищено с помощью аутентификации)
		'85'	Переменная	Криптография (CG), простое значение, состоящее из DO-ов, кодированных в BER-TLV, но не DO, относящихся к SM, см примечание (защищено с помощью аутентификации)
		'8E'	Переменная	Криптографическая контрольная сумма (CC), т.е. аутентификационный код сообщения (MAC)
		'9E'	Переменная	Цифровая подпись (DS)

Примечание — С точки зрения SM, простое значение всегда элементарное.

Шаблон безопасного обмена сообщениями может содержать шаблоны контрольного управления:
- шаблон криптографической контрольной суммы (CCT);
- шаблон цифровой подписи (DST);
- шаблон конфиденциальности (CT).

Эти шаблоны управляющих ссылок содержат дополнительные информационные объекты, например, для определения ссылки на алгоритм и ключ (см. таблицу D.2).

Таблица D.2 — Шаблон управляющих ссылок и соответствующие DO (подмножество)

Тег	L	Значение		
'7D'	Переменная	Шаблон криптографической контрольной суммы (CCT)		
'B7'	Переменная	Шаблон цифровой подписи (DST)		
'B9'	Переменная	Шаблон конфиденциальности (CT)		
		DO, связанные с CCT, DST, CT		
		Тег	L	Значение

Окончание таблицы D.2

Тег	L	Значение		
		'80'	Переменная	- Ссылка на алгоритм
		'83'	Переменная	- Ссылка на секретный ключ для прямого использования (относится к симметричному алгоритму); - Ссылка на открытый ключ (относится к асимметричному алгоритму)
		'84'	Переменная	- Ссылка на секретный ключ для установления ключа (относится к симметричному алгоритму); - Ссылка на приватный ключ (относится к асимметричному алгоритму)

Примечание — Дополнительные информационные объекты определены в ИСО/МЭК 7816-4.

D.3 Примеры кодирования

Примеры кодирования показывают:

- шаблон биометрической информации, в котором после информационных объектов «биометрическая информация» (биометрический заголовок) следует криптограмма, содержащая биометрические данные, также защищенная с помощью MAC (см. рисунок D.2), и

- какие-нибудь данные приложения (например, персональные данные для аутентификации) объединены с помощью шаблона биометрической информации и защищены различными способами (см. рисунки D.2 — D.5).

Рисунок D.2 — Шаблон BIT со встроенным SMT (пример)

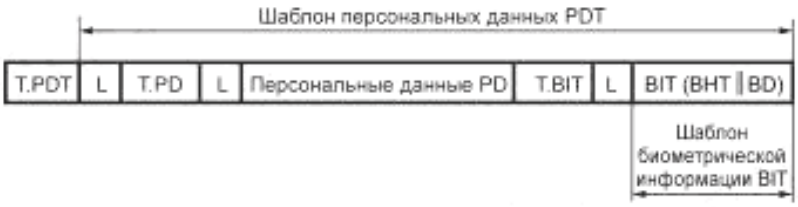


Рисунок D.3 — Шаблон персональных данных с BIT (пример)

Рисунок D.4 — Шаблон персональных данных с BIT, защищенных цифровой подписью (пример)

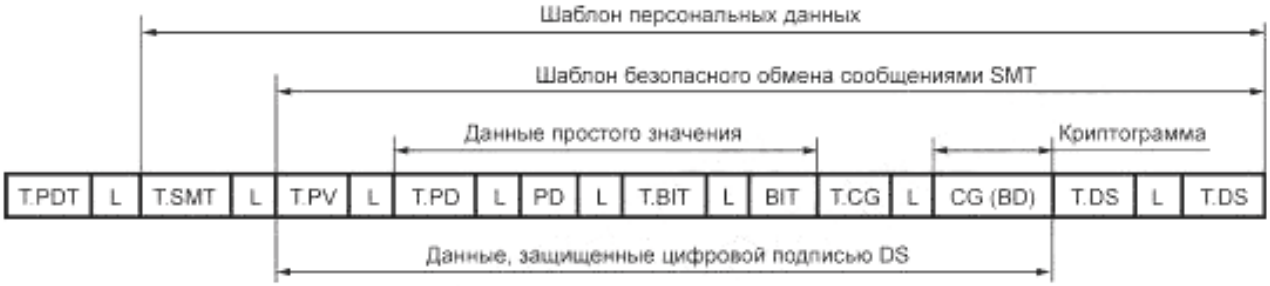


Рисунок D.5 — Шаблон персональных данных, защищенный цифровой подписью и содержащий помимо DO-ов криптограмму для биометрических данных (пример)

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 7816-4:2005	IDT	ГОСТ Р ИСО/МЭК 7816-4—2013 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
ИСО/МЭК 19785-1	IDT	ГОСТ Р ИСО/МЭК 19785-1—2008 «Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными. Часть 1. Спецификация элементов данных»
ИСО/МЭК 19785-2	IDT	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»
ИСО/МЭК 19785-3	—	*
ИСО/МЭК 19785-4	IDT	ГОСТ Р ИСО/МЭК 19785-4—2012 «Информационные технологии. Биометрия. Единая структура форматов обмена биометрическими данными. Часть 4. Спецификация формата блока защиты информации»

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1]	ISO/IEC 7816	Identification cards — Integrated circuit cards — All parts
	ИСО/МЭК 7816	Карты идентификационные. Карты на интегральных схемах. Все части
[2]	ISO/IEC 19784	BioAPI specification
	ИСО/МЭК 19784	Спецификация биометрического программного интерфейса
[3]	ANSI X9.84—2001	Biometric Information Management and Security
[4]	NISTIR 6529-A	Common Biometric Exchange Formats Framework

УДК 336.77:002:006.354 ОКС 35.240.15 Э46 ОКП 40 8470

Ключевые слова: обработка данных, обмен информацией, идентификационные карты, IC-карты, сообщения, способы защиты, аутентификация, биометрия

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 03.07.2014. Подписано в печать 12.08.2014. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,70. Тираж 56 экз. Зак. 3096.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru