ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 7816-8— 2011

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 8

Команды для операций по защите информации

ISO/IEC 7816-8:2004
Identification cards — Integrated circuit cards — Part 8: Commands for security operations
(IDT)

Издание официальное

Москва
Стандартинформ
2013

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

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 13 декабря 2011 г. № 1009-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 7816-8:2004 «Карты идентификационные. Карты на интегральных схемах. Часть 8. Команды для операций по защите информации» (ISO/IEC 7816-8:2004 «Identification cards — Integrated circuit cards — Part 8: Commands for security operations»).

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 объектами патентных прав. Международная организация по стандартизации не несет ответственность за идентификацию подобных патентных прав

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

Содержание

Введение

Серия стандартов ИСО/МЭК 7816 определяет требования к параметрам карт на интегральных схемах и способы их использования в рамках международного обмена информацией. Данные идентификационные карты предназначены для обмена информацией, основанного на согласованиях между внешним источником и интегральной схемой карты. В результате информационного обмена карта выдает информацию (результат вычислений, хранимые данные) и/или изменяет свое содержимое (память данных, память событий).

Пять стандартов относятся к картам с гальваническими контактами, три из них определяют электрический интерфейс:

ИСО/МЭК 7816-1 — определяет физические характеристики карт с контактами;

ИСО/МЭК 7816-2 — определяет размеры и расположение контактов;

ИСО/МЭК 7816-3 — определяет электрический интерфейс и протоколы передачи для асинхронных карт;

ИСО/МЭК 7816-10 — определяет электрический интерфейс и ответ на восстановление для синхронных карт;

ИСО/МЭК 7816-12 — определяет электрический интерфейс и рабочие процедуры для USB карт.

Все остальные стандарты не зависят от технологии физического интерфейса. Они применяются к картам, подключаемым при помощи контактов и/или радиочастоты:

ИСО/МЭК 7816-4 — определяет организацию, защиту и команды для обмена информацией;

ИСО/МЭК 7816-5 — определяет регистрацию провайдеров прикладных программ;

ИСО/МЭК 7816-6 — определяет элементы данных для межотраслевого обмена;

ИСО/МЭК 7816-7 — определяет команды для языка структурированных запросов для карты;

ИСО/МЭК 7816-8 — определяет команды, обеспечивающие операции по защите информации;

ИСО/МЭК 7816-9 — определяет команды для управления картами;

ИСО/МЭК 7816-11 — определяет удостоверение личности биометрическими методами;

ИСО/МЭК 7816-15 — определяет приложение с криптографической информацией;

ИСО/МЭК 10536 определяет обмен данными при помощи поверхностного действия. ИСО/МЭК 14443 и 15693 определяют радиочастотный доступ. Такие карты известны как бесконтактные карты.

Международный стандарт ИСО/МЭК 7816-8 подготовлен подкомитетом № 17 «Карты и идентификация личности» совместного технического комитета № 1 ИСО/МЭК «Информационные технологии».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 8

Команды для операций по защите информации

Identification cards. Integrated circuit cards. Part 8. Commands for information security operations

Дата введения — 2013—01—01

1 Область применения

Настоящий стандарт определяет межотраслевые команды для карты, которые могут быть использованы для операций криптографии.

Выбор и условия использования механизмов криптографии могут влиять на экспортные возможности карты.

Настоящий стандарт не устанавливает требования к оценке приемлемости алгоритмов и протоколов.

Настоящий стандарт не распространяется на реализацию обмена данными внутри карты и/или внешнего окружения.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий международный стандарт:

ИСО/МЭК 7816-4:2005 Идентификационные карты. Карты на интегральных схемах. Организация, защита и команды для обмена информацией (ISO/IEC 7816-4:2005, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 7816-4:

3.1 **метод асимметричного криптографического алгоритма** (asymmetric cryptographic technique): Криптографический метод, который использует две связанные между собой операции: общедоступную операцию, определенную общедоступным набором чисел или открытым ключом, и закрытую операцию, определенную закрытым набором чисел или секретным ключом.

Примечание — Две операции обладают таким свойством, что при наличии общедоступной операции невозможно произвести закрытую операцию.

3.2 **сертификат** (certificate): Цифровая подпись, связывающая определенный субъект или объект с его связанным открытым ключом.

Примечание — Организация, выдающая сертификат, также выступает в качестве органа распределения тега по отношению к элементам данных в сертификате.

3.3 **цифровая подпись** (digital signature): Присоединенные данные или криптографическое преобразование строковых данных, которые доказывают подлинность и целостность строковых данных и защиту от подделок, например, получателем строковых данных.

3.4 **ключ** (key): Последовательность символов управления криптографической операцией (например, шифровка, расшифровка, закрытая или общедоступная операция в динамической аутентификации, подписи производства, верификация подписи).

3.5 **безопасный обмен сообщениями** (secure messaging): Совокупность средств для криптографической защиты пары (частей пары) команда-ответ.

Издание официальное

4 Обозначения и сокращения

В настоящем стандарте применяют следующие сокращения:

CCT — шаблон криптографической контрольной суммы (control reference template for cryptographic checksum);

CRT — шаблон контрольного управления (control reference template);

CT — шаблон конфиденциальности (control reference template for confidentiality);

DSA — алгоритм цифровой подписи (digital signature algorithm);

DST — шаблон цифровой подписи (control reference template for digital signature);

ECDSA — алгоритм цифровой подписи на базе математического аппарата эллиптических кривых (elliptic curve digital signature algorithm);

HT — шаблон хэш-кода (control reference template for hash-code);

MSE — команда УПРАВЛЕНИЕ СРЕДОЙ ЗАЩИТЫ (MANAGE SECURITY ENVIRONMENT command);

PK — открытый ключ (public key);

PSO — команда ВЫПОЛНИТЬ ОПЕРАЦИЮ ЗАЩИТЫ (PERFORM SECURITY OPERATION command);

GQ — Гийу и Кискатер (Guillou and Quisquater);

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

RSA — критосистема Райвеста—Шамира—Адлемана (Rivest, Shamir, Adleman);

SE — среда защиты (security environment);

SEID — идентификатор защитной среды (security environment identifier).

5 Межотраслевые команды для криптографических операций

Настоящий стандарт не устанавливает обязательное требование к соблюдению всех нижеприведенных команд или всех параметров поддерживаемых команд для карт, соответствующих настоящему стандарту.

5.1 Команда ГЕНЕРИРОВАТЬ ПАРУ АСИММЕТРИЧНЫХ КЛЮЧЕЙ (GENERATE ASYMMETRIC KEY PAIR)

Команда GENERATE ASYMMETRIC KEY PAIR либо запускает генерацию и хранение асимметричной пары ключей в карте, т. е. открытого ключа и секретного ключа, либо получает доступ к асимметричной паре ключей, созданной ранее в карте (см. таблицу 1).

Данная команда может предшествовать команде MANAGE SECURITY ENVIRONMENT с целью установить генерацию ключей связанных параметров (например, справочник по алгоритмам). Команда может быть выполнена в один или несколько этапов, возможно, с использованием цепочки команд (см. ИСО/МЭК 7816-4).

Таблица 1 — Пара команда-ответ GENERATE ASYMMETRIC KEY PAIR

CLA INS P1 P2	Как определено в ИСО/МЭК 7816-4 «46» или «47» Управление генерацией в соответствии с таблицей 2 «00» (информация не предоставлена) или ссылка на ключ будет сгенерирована
Поле L_c	Отсутствует для кодирования Nc = 0, присутствует для кодирования Nc > 0
Поле данных	Отсутствует или представляет собой закрытые данные, если P1-P2 установлено как «0000», или один или более шаблонов CPT, связанных с генерацией ключа, если значение P1-P2 отлично от «0000» (см. примечание)
Поле L_e	Отсутствует для кодирования Ne = 0, присутствует для кодирования Ne > 0

Поле данных	Отсутствует или представляет собой открытый ключ в виде последовательности данных элементов либо объектов данных или последовательность объектов данных в соответствии с расширенным списком заголовков
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, где соответствие, например 6985

Примечание — Если пара ключей сгенерирована для нескольких пользователей, то имеется несколько шаблонов CRT. В поле данных шаблон CRT может иметь нулевую длину.

Таблица 2 — Управление генерацией в P1

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое значение
0	0	0	0	0	0	0	0	Информация не предоставлена
1	0	0	0	0	x	x	x	Предоставлена дополнительная информация
1	0	0	0	0	—	—	x	**Генерация ключа:**
—	—	—	—	—	x	x	0	- генерация асимметричной пары ключей
—	—	—	—	—	x	x	1	- доступ к существующей паре открытых ключей
1	0	0	0	0	—	x	—	**Формат возвращенных данных открытого ключа:**
—	—	—	—	—	x	0	x	- закрытый формат данных открытого ключа
—	—	—	—	—	x	1	x	- выходной формат данных открытого ключа в соответствии с расширенным заголовком
1	0	0	0	0	x	—	—	**Выходной индикатор:**
—	—	—	—	—	0	x	x	- данные открытого ключа в поле данных ответа
—	—	—	—	—	1	x	x	- нет данных ответа, если поле L_e отсутствует, или закрытые данные, если имеется поле L_e
Любое другое значение зарезервировано для будущего использования ISO/IEC JTC1/SC17								

Для генерации пары ключей при отсутствии поля L_e пара ключей хранится в карте, возможно, в файле EF, ссылка на который известна до подачи команды.

Для организации доступа к паре ключей (без генерации) поле данных команды может быть пустым.

В зависимости от четности кода INS (см. ИСО/МЭК 7816-4) открытый ключ в поле данных ответа представляет собой либо последовательность элементов данных («46»), либо последовательность объектов данных («47»).

Если расширенный список заголовков описывает поле данных ответа, то он неявно известен до подачи команды. Он охватывает открытый ключ объектов данных и другие запрашиваемые объекты данных.

Когда бит 1 устанавливается как единица в INS, т. е. INS устанавливается в значение «47», и открытый ключ возвращается в поле данных ответа, тогда межотраслевой шаблон используется для вложения одного соответствующего набора открытых ключей объектов данных в соответствии с таблицей 3. Если алгоритм не указан в команде, то он известен до подачи команды. В шаблоне открытого ключа контекстно-зависимый класс (первый байт от «80» до «BF») предназначен для открытого ключа объектов данных.

Таблица 3 — Открытый ключ объектов данных

Тег		Смысловое значение
«7F49»		Межотраслевой шаблон для вложения одного набора объектов данных открытых ключей со следующими тегами
	«06»	Идентификатор объекта алгоритма, дополнительно
	«80»	Ссылочный алгоритм, используемый в контрольном управлении объектов данных для безопасного обмена сообщениями, дополнительно
		Совокупность объектов данных открытого ключа для RSA
	«81»	Модуль (число обозначается как *n*, кодируется в *x* байтах)
	«82»	Открытая экспонента (число обозначается как *v*, например, 65537)
		Совокупность объектов данных открытого ключа для DSA
	«81»	Первое простое (число обозначается как *p*, кодируется в *y* байтах)
	«82»	Второе простое (число обозначается как *q*, делитель для *p*-1, например 20 байт)
	«83»	Основание (число обозначается как *g* порядка *q*, кодируется в *y* байтах)
	«84»	Открытый ключ (число обозначается как *y*, равное *g* в степени *x* на модуль *p*, где *x* — закрытый ключ, кодируется в *y* байтах)

Окончание таблицы 3

Тег	Смысловое значение
	Совокупность объектов данных открытого ключа для ECDSA
«81»	Простое (число обозначается как *p*, кодируется в *z* байтах)
«82»	Первый коэффициент (число обозначается как *a*, кодируется в *z* байтах)
«83»	Второй коэффициент (число обозначается как *b*, кодируется в *z* байтах)
«84»	Генератор (точка на кривой обозначается как PB на кривой, кодируется в 2*z* или *z* + 1 байтах)
«85»	Порядок (простое число, обозначается как *q*, порядок генератора PB, кодируется в *z* байтах)
«86»	Открытый ключ (точка на кривой, обозначается как PP, равна *x*, умноженному на PB, где *x* — закрытый ключ, кодируется в 2*z* или *z* + 1 байтах)
«87»	Кофактор
	Совокупность объектов данных открытого ключа для GQ2
«81»	Модуль (число обозначается как *n*, кодируется в *x* байтах)
«83»	Количество основных чисел (числа обозначают как *m*, кодируются в 1 байте). Если тег «83» присутствует, то тег «A3» должен отсутствовать и *m* основных чисел, обозначенных как *g*, g_2,..., g_m, являются первыми *m* простыми числами 2, 3, 5, 7, 11 ...)
«84»	Параметр верификации (число обозначается как *k*, кодируется в 1 байте)
«A3»	Множество *m* основных чисел обозначается как *g*, g_2,..., g_m, каждый из которых кодирован в 1 байте с тегом «80». (Если тег «A3» присутствует, то тег «83» должен отсутствовать)
В данном случае ISO/IEC JTC 1/SC 17 резервирует любой другой объект данных контекстно-зависимого класса (первый байт в диапазоне от «80» до «BF»)	

5.2 Команда ВЫПОЛНИТЬ ОПЕРАЦИЮ ЗАЩИТЫ (PERFORM SECURITY OPERATION)

Команда PERFORM SECURITY OPERATION запускает следующие операции защиты в соответствии с объектами данных, определенных в P1—P2 (см. таблицу 4):

- вычисление криптографической контрольной суммы;
- вычисление цифровой подписи;
- вычисление хэш-кода;
- верификация криптографической контрольной суммы;
- верификация цифровой подписи;
- верификация хэш-кода;
- шифровка;
- расшифровка.

Таблица 4 — Пара команда-ответ PERFORM SECURITY OPERATION

CLA	Как определено в ИСО/МЭК 7816-4
INS	«2A»
P1	Тег (поле данных ответа в элементе данных, если присутствует) или «00» (поле данных ответа всегда отсутствует); «FF» = PFU (зарезервировано для будущего использования)
P2	Тег (поле данных команды в элементе данных, если присутствует) или «00» (поле данных команды всегда отсутствует); «FF» = PFU (зарезервировано для будущего использования) для ISO/IEC JTC1/SC17
Поле L_c	Отсутствует для кодирования Nc = 0, присутствует для кодирования Nc > 0
Поле данных	Отсутствует или имеет значение объектов данных, заданных в P2
Поле L_e	Отсутствует для кодирования Ne = 0, присутствует для кодирования Ne > 0

Поле данных	Отсутствует или имеет значение объектов данных, заданных в P1
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, где соответствие, например 6985

Если операция защиты требует выполнить несколько команд, то необходимо применять цепочку команд (см. ИСО/МЭК 7816-4).

Команда PERFORM SECURITY OPERATION может предшествовать команде MANAGE SECURITY ENVIRONMENT.

Например, ссылочный ключ, а также ссылочный алгоритм должны быть либо неявно известны, либо заданы в шаблоне CRT в команде MANAGE SECURITY ENVIRONMENT.

Такая команда может быть выполнена, только если защитный статус удовлетворяет атрибутам секретности операции. Успешное выполнение команды может зависеть от успешного завершения предыдущей команды (например, VERIFY (ПРОВЕРИТЬ) перед вычислением цифровой подписи).

Список заголовков или расширенный список заголовков определяет порядок и пункты данных, которые формируют вход для операций защиты.

Команда PERFORM SECURITY OPERATION использует шаблоны входа, перечисленные в таблице 5. Эти шаблоны являются основными объектами данных для безопасного обмена сообщениями (см. ИСО/МЭК 7816-4).

Таблица 5 — Входные шаблоны

Тег	Значение
«A0»	Входной шаблон для вычисления хэш-кода (шаблон хэширован)
«A2»	Входной шаблон для проверки криптографической контрольной суммы (шаблон интегрирован)
«A8»	Входной шаблон для проверки цифровой подписи (шаблон подписан)
«AC»	Входной шаблон для вычисления цифровой подписи (связанные поля значений подписаны)
«AE»	Входной шаблон для проверки сертификата (связанные поля значений сертифицированы)
«BC»	Входной шаблон для вычисления цифровой подписи (шаблон подписан)
«BE»	Входной шаблон для проверки сертификата (шаблон сертифицирован)

Входные шаблоны, контекстно-зависимый класс (первый байт в диапазоне от «80» до «BF») зарезервированы для входных объектов данных. В таблице 6 перечислены объекты данных во входных шаблонах.

Таблица 6 — Входные объекты данных

Тег	Значение	«A0»	«A2»	«A8»	«AC», «BC»	«AE», «BE»
«80»	Явное значение	x	x	x	x	x
«8E»	Криптографическая контрольная сумма		x			x
«90»	Хэш-код	x		x	x	x
«92»	Сертификат					x
«9C»	Открытый ключ			x		x
«9E»	Цифровая подпись			x		x

5.3 Операция ВЫЧИСЛЕНИЕ КРИПТОГРАФИЧЕСКОЙ КОНТРОЛЬНОЙ СУММЫ (COMPUTE CRYPTOGRAPHIC CHECKSUM)

Операция COMPUTE CRYPTOGRAPHIC CHECKSUM запускает вычисление криптографической контрольной суммы (см. таблицу 7).

Таблица 7 — Параметры и поля данных для операции COMPUTE CRYPTOGRAPHIC CHECKSUM

P1 P2	«8E» «80»
Командное поле данных	Данные, для которых должна быть вычислена криптографическая контрольная сумма

Ответное поле данных	Криптографическая контрольная сумма

5.4 Операция ВЫЧИСЛЕНИЕ ЦИФРОВОЙ ПОДПИСИ (COMPUTE DIGITAL SIGNATURE)

Операция COMPUTE DIGITAL SIGNATURE запускает вычисление цифровой подписи (см. таблицу 8). Алгоритм может представлять собой либо алгоритм цифровой подписи, либо комбинацию хэш-алгоритма и алгоритма цифровой подписи. В приложении А приведены примеры операций цифровой подписи.

Для вычисления цифровой подписи данные, которые должны быть подписаны или интегрированы в процесс подписания, передаются в командное поле данных или отправляются в предыдущую команду, например PSO: HASH. В P2 цифровая подпись определяется тегами «9А», «АС» или «ВС» в соответствии со структурой на входе (см. ИСО/МЭК 7816-4).

Если вспомогательные данные должны быть включены во ввод цифровой подписи, то ссылка должна быть представлена в шаблоне CRT (см. ИСО/МЭК 7816-4). Если имеется пустая ссылка на объект данных для вспомогательных данных, то тогда вспомогательные данные должны быть вставлены картой. Вспомогательные данные, которые присутствуют или к которым обращаются в поле данных, имеют приоритет над любым списком заголовка.

Значение, подлежащее возврату картой, является цифровой подписью (P1 = «9E»).

Таблица 8 — Параметры и поля данных для операции COMPUTE DIGITAL SIGNATURE

P1 P2	«9E» «9А», «АС» или «ВС»
Командное поле данных	Отсутствует (данные уже в карте) или если P2 = «9А», данные должны быть подписаны или интегрированы в процесс подписания, если P2 = «АС», объекты данных, значения полей которых подписаны или интегрированы в процесс подписания, или если P2 = «ВС», объекты данных должны быть подписаны или интегрированы в процесс подписания

Ответное поле данных	Цифровая подпись

Примечание — Теги «АС» и «ВС» не интегрированы во ввод цифровой подписи.

5.5 Операция ХЭШИРОВАТЬ (HASH)

Операция HASH запускает вычисление хэш-кода двумя способами (см. таблицу 9):

- полное вычисление внутри карты или
- частичное вычисление внутри карты (например, последний цикл хэширования).

Шаблон хэш-кода HT («АА», «АВ») указывает ссылочный алгоритм для вычисления хэш-кода (см. ИСО/МЭК 7816-4).

Входные данные должны быть представлены карте в виде последовательных блоков (один или более одновременно). В зависимости от алгоритма хэширования последние входные данные имеют длину, равную или меньшую длины блока. Заполняющий алгоритм, если это целесообразно, является частью определения алгоритма хэширования.

Для последующей обработки вычисленного хэш-кода следует различать следующие два случая:

- вычисленный хэш-код хранится в карте и доступен для использования в более поздней команде; тогда поле L_e отсутствует либо
- хэш-код доставляется картой в ответе; тогда поле L_e должно быть установлено на соответствующую длину.

Таблица 9 — Параметры и поле данных для операции HASH

P1 P2	«90» «80» или «А0»
Командное поле данных	Если P2 = «80», данные для хэширования Если P2 = «А0», объекты данных, имеющие отношение к хэшированию («90» для промежуточного хэш-кода, «80» для последнего блока)

Ответное поле данных	Хэш-код или отсутствует

5.6 Операция ПРОВЕРИТЬ КРИПТОГРАФИЧЕСКУЮ КОНТРОЛЬНУЮ СУММУ (VERIFY CRYPTOGRAPHIC CHECKSUM)

Операция VERIFY CRYPTOGRAPHIC CHECKSUM запускает проверку криптографической контрольной суммы (см. таблицу 10).

Таблица 10 — Параметры и поле данных для операции VERIFY CRYPTOGRAPHIC CHECKSUM

P1 P2	«00» «A2»
Командное поле данных	Объекты данных, имеющие отношение к операции (например, «80», «8E»)

Ответное поле данных	Отсутствует

Примечание — Поле значений простого значения объекта данных (тег «80») содержит данные (элементы данных или объекты данных), защищенные криптографической контрольной суммой.

5.7 Операция ПРОВЕРИТЬ ЦИФРОВУЮ ПОДПИСЬ (VERIFY DIGITAL SIGNATURE)

Операция VERIFY DIGITAL SIGNATURE запускает проверку цифровой подписи, которая передается как объект данных в поле данных команды (см. таблицу 11). Другие данные, имеющие отношение к проверке, либо передаются в процессе формирования цепочки команд, либо присутствуют в карте. Алгоритм может представлять собой либо только алгоритм цифровой подписи, либо комбинацию хэш-алгоритма и алгоритма цифровой подписи. В приложении А приведены примеры операций цифровой подписи.

Открытый ключ, а также алгоритм могут быть:

- или неявно известны,
- или к ним обращаются в шаблоне DST («B6») команды MANAGE SECURITY ENVIRONMENT,
- или доступны как результат предшествующей операции VERIFY CERTIFICATE (ПРОВЕРИТЬ СЕРТИФИКАТ).

Если ссылочный алгоритм в карте объявляет только алгоритм подписи, то данные состоят из хэш-кода или подпись представляет собой сообщение типа восстановление (см. ИСО/МЭК 9796). В противном случае вычисление хэш-кода осуществляется в карте и ссылочный алгоритм дополнительно содержит ссылку на алгоритм хэширования.

Таблица 11 — Параметры и поле данных для операции VERIFY DIGITAL SIGNATURE

P1 P2	«00» «A8»
Командное поле данных	Объекты данных, имеющие отношение к операции (например, либо «9A», «AC», либо «BC» и «9E»)

Ответное поле данных	Отсутствует

Если поле данных команды содержит пустой объект данных, то предполагается, что карта знает его значения для использования в проверке.

5.8 Операция ПРОВЕРИТЬ СЕРТИФИКАТ (VERIFY CERTIFICATE)

Для проверки сертификата в карте (см. приложение В) цифровая подпись сертификата, подлежащая проверке, передается как объект данных в поле данных команды. Открытый ключ органа по сертификации, который применяется при проверке, либо находится в карте, либо выбирается неявно, либо к нему можно обратиться в шаблоне DST, используя команду MANAGE SECURITY ENVIRONMENT (см. таблицу 12). Алгоритм, который должен применяться, неявно известен или к нему можно обратиться в шаблоне DST. Если есть другие объекты данных, которые должны использоваться в процессе проверки (например, хэш-код), то они должны находиться в карте или передаваться, используя процесс формирования цепочки команд.

Необходимо различать следующие два случая:

- если сертификат не требует дополнительного описания (P2 = «BE»), то карта извлекает открытый ключ, установленный по его тегу, в (восстановленном) содержании сертификата;
- если сертификат требует дополнительного описания (P2 = «AE»), то карта извлекает открытый ключ в сертификате неявно или явно, используя тег открытого ключа в списке заголовка, описывающего содержание сертификата.

Если открытый ключ хранится в памяти, то он будет ключом по умолчанию для последующей операции VERIFY DIGITAL SIGNATURE.

Таблица 12 — Параметры и поле данных для операции VERIFY CERTIFICATE

P1 P2	«00» «92», «AE» или «BE»
Командное поле данных	Элементы данных или объекты данных, имеющих отношение к операции

Ответное поле данных	Отсутствует

Примечание — Если используется схема частичного восстановления сообщения и часть информации уже записана в карте, то объект данных для вспомогательных данных должен посылаться пустым, а данные должны быть вставлены картой позднее.

5.9 Операция ШИФРОВКА (ENCIPHER)

Операция ENCIPHER шифрует данные, переданные в поле данных команды (см. таблицу 13).

Примечание — Эта операция может использоваться для генерации различных ключей.

Таблица 13 — Параметры и поле данных для операции ENCIPHER

P1 P2	«82», «84», «86» (криптограмма) «80» (простое значение)
Командное поле данных	Отсутствует (данные уже в карте) или данные, подлежащие шифровке

Ответное поле данных	Зашифрованные данные

5.10 Операция РАСШИФРОВКА (DECIPHER)

Операция DECIPHER расшифровывает данные, переданные в поле данных команды (см. таблицу 14).

Таблица 14 — Параметры и поле данных для операции DECIPHER

P1 P2	«80» (простое значение) «82», «84», «86» (криптограмма)
Командное поле данных	Данные, подлежащие расшифровке

Ответное поле данных	Отсутствует (расшифрованные данные остаются в карте) или зашифрованные данные

Приложение А
(справочное)

Примеры операций, связанных с цифровой подписью

А.1 Последовательность команд для управления средой защиты

В таблице А.1 представлена последовательность команд MANAGE SECURITY ENVIRONMENT для компонентов SET DST, CCT, CT текущей среды защиты и для STORE (ХРАНЕНИЕ) с идентификатором защитной среды SEID, указанным в P2.

Таблица А.1 — Установка компонентов среды защиты

Команда	Операция	P1-P2	Поле данных команды
MSE	SET DST	«41» — «B6»	{«84» — L — Ссылочный ключ } — {«91» — L = 0}
MSE	SET CCT	«41» — «B4»	{«83» — L — Ссылочный ключ } — {«87» — L — Значение инициализации}
MSE	SET CT	«41» — «B8»	{«83» — L — Ссылочный ключ }
MSE	STORE (SEID = 1)	«F2» — «01»	—

Операция SET DST обращается к открытому ключу при использовании вычисления подписи и определяет интегрирование случайного числа во вход цифровой подписи. Операция SET CCT обращается к закрытому ключу и начальному значению при использовании вычисления криптографической контрольной суммы. Операция SET CT обращается к сессии закрытого ключа при использовании конфиденциальности.

А.2 Последовательность команд для вычисления цифровой подписи

В таблице А.2 показан синтаксис для создания цифровой подписи при использовании схемы подписи с приложением. Вводом является хэш-код с заполняющими байтами. Этот пример иллюстрирует вычисление цифровой подписи с объединенным алгоритмом, включая операцию хэширования. В данном случае хэш-вход поступает на карту.

Таблица А.2 — Первый пример схемы цифровой подписи с приложением

Команда	Операция	P1-P2	Поле данных команды	Поле данных ответа
MSE	RESTORE[1)]	«F3» — «01»	—	—
PSO	COMPUTE DIGITAL SIGNATURE	«9E» — «9A»	Хэш-код с заполняющими байтами	Цифровая подпись

[1)] ВОССТАНОВЛЕНИЕ.

Примечание — Этот пример является чисто иллюстративным, и его применение ограничено с точки зрения реализации экспортных возможностей, которые могут применяться, и по причинам общей безопасности (в некоторых обстоятельствах желательно избегать повтора подписей).

В таблице А.3 показан синтаксис для создания цифровой подписи с приложением. Ввод цифровой подписи состоит из хэш-кода без заполняющих байтов.

Таблица А.3 — Второй пример схемы цифровой подписи с приложением

Команда	Операция	P1-P2	Поле данных команды	Поле данных ответа
MSE	RESTORE	«F3» — «01»	—	—
PSO	COMPUTE DIGITAL SIGNATURE	«9E» — «9A»	Хэш-код без заполняющих байтов	Цифровая подпись

Примечание 1 — Для того чтобы избежать ограничений на экспорт, можно использовать объединение подписи и хэш-алгоритма.

Примечание 2 — В некоторых случаях избежать повторение подписей не удается.

В таблице А.4 показана схема подписи с приложением. Ввод цифровой подписи содержит хэш-код без заполняющих байтов, который передается в карту, и карта запрашивается для того, чтобы сгенерировать случайное число, как указано в расширенном списке заголовков шаблона цифровой подписи DST в поле данных команды для команды MSE.

Таблица А.4 — Третий пример схемы цифровой подписи с приложением

Команда	Операция	P1-P2	Поле данных команды	Поле данных ответа
MSE	SET[1)]	«41» — «B6»	{«4D» — L — {«90» — L — «91» — L = 0)} — — {«84» — L — Ссылочный ключ}	—
PSO	COMPUTE DIGITAL SIGNATURE	«9E» — «BC»	{«90» — L — Хэш-код}	Цифровая подпись

[1)] УСТАНОВИТЬ.

В таблице 5 показан синтаксис для цифровой подписи с ограниченным восстановлением сообщения. Данные для подписи сконфигурированы в соответствии со схемой подписи, задающей ограниченное восстановление сообщения, используя объекты данных, представленные в поле данных команды, в результате чего счетчик цифровой подписи используется как внутреннее сообщение, предоставляемое картой.

Таблица А.5 — Четвертый пример схемы цифровой подписи с приложением

Команда	Операция	P1-P2	Поле данных команды	Поле данных ответа
MSE	RESTORE	«F3» — «02»	—	—
PSO	COMPUTE DIGITAL SIGNATURE	«9E» — «AC»	{«90» — L — Хэш-код}	Цифровая подпись

Примечание —Заполнение для вычисления хэш-кода, а также цифровой подписи осуществляется в соответствии с ИСО/МЭК 9796-2.

В таблице А.6 показано, как карта выполняет хэширование (или последний цикл вычислений с хэшированием). Ввод цифровой подписи остается пустым в операции COMPUTE DIGITAL SIGNATURE, т. к. все входные данные присутствуют в карте.

Таблица А.6 — Пятый пример схемы цифровой подписи с приложением

Команда	Операция	P1-P2	Поле данных команды	Поле данных ответа
MSE	RESTORE	«F3» — «01»	—	—
PSO	HASH	«90» — «80»	Данные для хэширования	—
PSO	COMPUTE DIGITAL SIGNATURE	«9E» — «9A»	—	Цифровая подпись

А.3 Последовательность команд для проверки цифровой подписи

В таблице А.7 показано, как расширенный список заголовков определяет структуру сертификата, требующего дополнительного описания (см. приложение В). ввод цифровой подписи состоит из элементов данных. Операция VERIFY CERTIFICATE выполняется, используя цепочку команд.

Таблица А.7 — Первый пример проверки цифровой подписи

Команда	Операция	P1-P2	Поле данных команды
MSE	SET DST	«41» — «B6»	{«4D» — L — {«42» — L — «5F20» — L — «5F49» — L)} — {«83» — L — Ссылочный ключ}
PSO	VERIFY CERTIFICATE (CLA = «1X»)	«00» — «AE»	{«5F4E» — L — Содержание сертификата}
PSO	VERIFY CERTIFICATE (CLA = «0X»)	«00» — «AE»	{«5F37» — L — Цифровая подпись сертификата}
PSO	HASH	«90» — «80»	Ввод с хэшированием
PSO	VERIFY DIGITAL SIGNATURE	«00» — «A8»	{«9E» — L — Цифровая подпись}

На первом этапе предоставляется объект данных содержания сертификата (сцепление элементов данных: идентификационный номер эмитента (тег «42»), имя держателя карты (тег «5F20») и открытый ключ держателя карты («5F49»)). Карта выполняет хэширование, используя содержание сертификата в качестве хэшированных входных данных.

На втором этапе цифровая подпись, принадлежащая сертификату, возвращается в прежнее состояние, и результат сравнивается с хэш-кодом, вычисленным ранее. Затем выполняется операция HASH. Для проверки цифровой подписи открытый ключ должен быть уже извлечен и проверен предыдущей командой VERIFY CERTIFICATE. Ввод хэшированных данных зависит от алгоритма хэширования, либо от простого значения, возможно, представленного цепочкой команд, либо от предварительно обработанного хэш-кода, если карта выполняет только последний цикл вычислений с хэшированием.

На последнем этапе выполняется операция VERIFY DIGITAL SIGNATURE.

В таблице А.8 показана проверка сертификата, не требующего дополнительного описания (см. приложение В): ввод цифровой подписи состоит из объектов данных. Операция VERIFY CERTIFICATE использует цепочку команд. На первом этапе представляются объекты данных, интегрированные в сертификат (например, обращение к органу по сертификации, имя держателя карты и открытый ключ держателя карты). Карта использует это объединение в качестве хэшированных входных данных. Дальнейшие этапы идентичны тем, что описаны в предыдущем примере.

Таблица А.8 — Второй пример проверки цифровой подписи

Команда	Операция	P1-P2	Поле данных команды
MSE	SET DST	«41» — «B6»	{«83» — L — Ссылочный ключ}
PSO	VERIFY CERTIFICATE (CLA=«1X»)	«00» — «BE»	{«42» — L — Идентификационный номер эмитента} — {«5F20» — L — Имя держателя карты} — {«5F49» — L — Открытый ключ держателя карты}
PSO	VERIFY CERTIFICATE (CLA= «0X»)	«00» — «AE»	{«5F37» — L — Цифровая подпись сертификата}
PSO	HASH	«90» — «80»	Ввод с хэшированием
PSO	VERIFY DIGITAL SIGNATURE	«00» — «A8»	{«9E» — L — Цифровая подпись}

В таблице А.9 показано использование открытого ключа, установленного в карте.

Таблица А.9 — Третий пример проверки цифровой подписи

Команда	Операция	P1-P2	Поле данных команды
MSE	SET DST	«41» — «B6»	{«83» — L — Ссылочный ключ}
PSO	HASH	«90» — «A8»	Ввод с хэшированием
PSO	VERIFY DIGITAL SIGNATURE	«00» — «A8»	{«9E» — L — Цифровая подпись}

Приложение В
(справочное)

Примеры сертификатов, интерпретированных картой

В.1 Объекты данных для сертификатов, верифицируемых картой

В таблице В.1 показаны объекты данных, имеющих отношение к сертификатам, верифицируемым картой.

Таблица В.1 — Межотраслевые объекты данных (примеры) для сертификатов, верифицируемых картой

Тег	Элемент данных
«42»	Идентификационный номер эмитента
«5F20»	Имя держателя карты
«5F37»	Статическая внутренняя аутентификация (подпись сертификата, произведенная эмитентом)
«5F49»	Открытый ключ держателя карты
«5F4C»	Сертификат полномочий владельца
«5F4E»	Содержание сертификата
«7F21»	Сертификат держателя карты

Эмитент может определять дальнейшие объекты данных, такие как серийный номер сертификата, номер версии, дата истечения срока действия и т. д.

Следует различать две структуры сертификатов, верифицируемых картой:

- сертификат, верифицируемый картой и не требующий дополнительного описания, состоит из объединения BER-TLV объектов данных;
- сертификат, верифицируемый картой и требующий дополнительного описания, состоит из объединения элементов данных.

В.2 Сертификаты, верифицируемые картой и не требующие дополнительного описания

Для подписания сертификата может использоваться схема цифровой подписи с или без восстановления сообщения. В таблице В.2 показан пример сертификата, верифицируемого картой и не требующего дополнительного описания, со схемой цифровой подписи с восстановлением сообщения.

Таблица В.2 — Сертификат держателя карты, верифицируемый картой и не требующий дополнительного описания (примеры)

«7F21»	Длина	Значение последовательности объектов данных	
		{«42» — L — Идентификационный номер эмитента} — {«5F20» — L — Имя держателя карты} — {«5F49» — L — Открытый ключ держателя карты}	{«5F37» — L — Цифровая подпись}
Тег сертификата (составленный)	Длина сертификата	Значение сертификата, состоящего из объектов данных, интегрированных в цифровую подпись (имеется только при отсутствии восстановления сообщений)	Объекты данных для подписи: {«42» — L — Идентификационный номер эмитента} {«5F20» — L — Имя держателя карты} {«5F49» — L — Открытый ключ держателя карты}

Примечание 1 — Идентификационные данные органа по сертификации могут ссылаться на свой открытый ключ.

Примечание 2 — Идентификационные данные держателя карты могут быть использованы для управления правами доступа к данным, хранящимся в карте.

Примечание 3 — Открытый ключ владельца карты может быть использован в последующей операции VERIFY DIGITAL SIGNATURE.

В.3 Сертификаты, верифицируемые картой и требующие дополнительного описания

Объект данных расширенного списка заголовков может находиться в карте для того, чтобы проверить этот тип сертификата; с другой стороны, он должен быть защищен при передаче его в карту. Объект данных расширенного списка заголовков (тег «4D», см. ИСО/МЭК 7816-4) описывает объединение элементов данных по парам тег/длина в том же порядке, что и в цифровой подписи (см. таблицу В.3).

Таблица В.3 — Сертификат держателя карты, верифицируемый картой и требующий дополнительного описания (примеры)

«7F21»	Длина	Значение последовательности объектов данных		
		{'4D' — L — ('42' — L — '5F20' — L — '5F49' — L)}	{«5F4E» — L — Идентификационный номер эмитента — - Имя держателя карты — - Открытый ключ держателя карты}	{«5F37» — L — Цифровая подпись}
Тег сертификата (составленный)	Длина сертификата	Расширенный список заголовков (присутствует только, если структура сертификата известна явно)	Объект данных содержания сертификата, интегрированный в подпись (имеется только при отсутствии сообщения восстановления, он содержит элементы данных в соответствии с расширенным списком заголовков)	Элементы данных для подписи: - идентификационный номер эмитента; - имя держателя карты; - открытый ключ держателя карты

Приложение С
(справочное)

Примеры импорта/экспорта асимметричного ключа

С.1 Использование команды GET DATA (ИЗВЛЕЧЬ ДАННЫЕ) для экспорта открытого ключа

Предполагается, что объекты данных, описывающие открытый ключ (PK), находятся в карте и закодированы в форме, показанной в таблице С.1.

Таблица С.1 — Кодирование для объекта данных открытого ключа (PK), находящегося в карте

«A8»	L	Пара T — L для указания шаблона для проверки цифровой подписи				
		«B6»	L	DST		
				«83»	L	Ссылочный ключ на открытый ключ (PK.CH.DS)
		«7F49»	L			Объект данных открытого ключа
				«81»	L	Модуль
				«82»	L	Открытая экспонента
		«9E»	L			Цифровая подпись (все байты шаблона проверки цифровой подписи предшествующего тега «9E» со знаком)

С помощью команды MSE выбирается открытый ключ PK, который должен быть восстановлен. Далее команда GET DATA (нечетный INS, P1-P2 = «3FFF») используется в 3 этапа, в соответствии с которыми поля данных, показанные в таблицах С.2—С.7, осуществляются в интерфейсе карты.

Таблица С.2 — Поле данных команды GET DATA, этап 1 из 3

«4D»	0B	Расширенный список заголовков						
		«A8»	09	Пара T — L для указания шаблона для проверки цифровой подписи				
				«B6»	02	Пара T — L, которая указывает объект данных DST		
						«83»	00	Пара T — L, которая указывает ссылку на открытый ключ
		«7F49»	02	Пара T — L, которая указывает объект данных открытого ключа				
				«81»	00	Пара T — L, которая указывает модуль		

Таблица С.3 — Поле данных ответа GET DATA, этап 1 из 3

«A8»	L					
		«B6»	L	DST		
				«83»	L	Ссылочный ключ PK.CH.DS
		«7F49»	L	Открытый ключ		
				«81»	L	Модуль

Таблица С.4 — Поле данных команды GET DATA, этап 2 из 3

«4D»	07	Расширенный список заголовков						
		«A8»	07	Пара T — L для указания шаблона для проверки цифровой подписи				
				«7F49»	02	Пара T — L, которая указывает объект данных открытого ключа		
						«82»	00	Пара T — L, которая указывает модуль

Таблица С.5 — Поле данных ответа GET DATA, этап 2 из 3

«A8»	L					
		«7F49»	L	Открытый ключ		
				«82»	L	Открытая экспонента

Таблица С.6 — Поле данных команды GET DATA, этап 3 из 3

«4D»	04	Расширенный список заголовков				
		«A8»	02	Пара T — L для указания шаблона для проверки цифровой подписи		
				«9E»	00	Пара T — L, которая указывает объект данных цифровой подписи

Таблица С.7 — Поле данных ответа GET DATA, этап 3 из 3

«A8»	L			
	«9E»	L	Цифровая подпись	

С.2 Использование команды PUT DATA (ПОМЕСТИТЬ ДАННЫЕ) для импорта закрытого ключа

Первоначально команда MSE должна отправить ссылку на соответствующий закрытый ключ (т. е. ссылочный ключ уже известен карте) (см. таблицу С.8). Далее используют команду PUT DATA (нечетный INS, P1-P2 = «3FFF») с полем данных команды, как показано в таблице С.9.

Таблица С.8 — Расширенный список заголовков, описывающий объект закрытого ключа

«4D»	0B	Расширенный список заголовков						
		«A8»	L	Пара T — L для указания шаблона для проверки цифровой подписи				
				«B6»	L	Пара T — L для указания DST		
						«84»	L	Пара T — L для указания ссылочного ключа на SK.CH.DS
		«7F48»	L	Пара T — L для указания объекта данных закрытого ключа				
				«81»	00	Пара T — L, которая указывает модуль		
						«92»	L	Пара T — L для параметра p
						«93»	L	Пара T — L для параметра q
						«94»	L	Пара T — L для параметра $1/q \bmod p$
						«95»	L	Пара T — L для параметра $d \bmod (p-1)$
						«96»	L	Пара T — L для параметра $d \bmod (q-1)$
				«9E»	L	Пара T — L для указания цифровой подписи		

Таблица С.9 — Поле данных команды PUT DATA

«4D»	L	Расширенный список заголовков						
		«A8»	L	Пара T — L для указания шаблона для проверки цифровой подписи				
				«B6»	L	Пара T — L для указания DST		
						«84»	L	Пара T — L для указания ссылочного ключа на SK.CH.DS
		«7F48»	L	Пара T — L для указания объекта данных закрытого ключа				
						«92»	L	Пара T — L для параметра p
						«93»	L	Пара T — L для параметра q
						«94»	L	Пара T — L для параметра $1/q \bmod p$
						«95»	L	Пара T — L для параметра $d \bmod (p-1)$
						«96»	L	Пара T — L для параметра $d \bmod (q-1)$
				«9E»	L	Пара T — L для указания цифровой подписи		
«5F48»	L	Объединение элементов данных параметров ключа в соответствии с расширенным списком заголовков. Элементы данных, которые связаны с наполнением тегов «00» в расширенном списке заголовков, считываются, но при этом игнорируются						
«9E»	L	Цифровая подпись						

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным 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—2004 «Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 4. Межотраслевые команды для обмена»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1]	ИСО/МЭК 7816 (все части)	Карты идентификационные — Карты на интегральных схемах с контактами
	ISO/IEC 7816 (all parts)	Identification cards — Integrated circuit cards
[2]	ИСО/МЭК 9796 (все части)	Информационная технология — Методы защиты — Схема цифровой подписи с восстановлением сообщения
	ISO/IEC 9796 (all parts)	Information technology — Security techniques — Digital signature scheme giving message recovery
[3]	ИСО/МЭК 9798-5:1999[1)]	Информационные технологии — Методы защиты — Аутентификация объектов — Часть 5: Механизмы с применением методов с «нулевым знанием»
	ISO/IEC 9798-5:1999	Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero knowledge techniques
[4]	ИСО/МЭК 10536 (все части)	Карты идентификационные — Карты на интегральных схемах бесконтактные — Карты поверхностного действия
	ISO/IEC 10536 (all parts)	Identification cards — Contactless integrated circuits cards — Close coupled cards
[5]	ИСО/МЭК 14443 (все части)	Карты идентификационные — Карты на интегральных схемах бесконтактные — Карты близкого действия
	ISO/IEC 14443 (all parts)	Identification cards — Contactless integrated circuits cards — Proximity cards
[6]	ИСО/МЭК 15693 (все части)	Карты идентификационные — Карты на интегральных схемах бесконтактные — Карты удаленного действия
	ISO/IEC 15693 (all parts)	Identification cards — Contactless integrated circuits cards — Vicinity cards

[1)] Отменен. Действует ИСО/МЭК 9798-5:2009.

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

Редактор *Н.Н. Кузьмина*
Технический редактор *В.Н. Прусакова*
Корректор *Ю.М. Прокофьева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 18.01.2013. Подписано в печать 11.02.2013. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 1,95. Тираж 96 экз. Зак. 135.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.