Distr.: General
25 April 2017

Original: Russian only

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по автомобильному транспорту

Группа экспертов по Европейскому соглашению, касающемуся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР)

Пятнадцатая сессия
Женева, 12 июня 2017 года

Данный документ, представленный Европейской Комиссией, содержит добавление 2 к приложению IC к регламенту (ЕС) 2016/799.

RU

ПРИЛОЖЕНИЕ 2. СПЕЦИФИКАЦИЯ КАРТОЧЕК ТАХОГРАФОВ

Дата: 02-02-2016

Содержание

1. Введение

1.1. Сокращения

В настоящем приложении употребляются следующие сокращения:

AC	Условия доступа
AES	Расширенный стандарт шифрования
AID	Идентификатор приложения
ALW	Всегда
APDU	Прикладной протокольный блок данных (структура команды)
ATR	Отклик на сигнал сброса
AUT	Аутентифицированный
C6, C7	Контакты № 6 и 7 карточки, как описано в ISO/IEC 7816-2
cc (вц)	временные циклы
CHV	Информация проверки данных владельца карточки
CLA	Классовый байт команды APDU
DSRC	Выделенная связь ближнего действия
DF	Выделенный файл. DF может содержать другие файлы (EF или DF)
ECC	Эллиптическая криптография
EF	Элементарный файл
etu (эев)	элементарная единица времени
G1	Первое поколение
G2	Второе поколение
IC	Интегральная схема
ICC	Карточка с интегральной схемой
ID	Идентификатор
IFD	Устройство интерфейса
IFS	Размер информационного поля
IFSC	Размер информационного поля для карточки
IFSD	Устройство размера информационного поля (для терминала)
INS	Командный байт команды APDU
Lc	Длина входных данных для команды APDU
Le	Длина ожидаемых данных (выходные данные для команды)
MF	главный файл (корневой DF)
NAD	Адрес узла, используемый в протоколе T=1
NEV	Никогда
P1-P2	Байты параметров
PIN	Персональный идентификационный номер
PRO SM	Криптозащищённое сообщение
PTS	Выбор передачи протокола
RFU	Зарезервировано для будущего пользования
RST	Перезагрузка (карточки)
SFID	Короткий идентификатор EF
SM	Безопасный обмен сообщениями
SW1-SW2	Статусные байты
TS	Исходный символ ATR
VPP	Напряжение программирования
VU (БУ)	Бортовое устройство
XXh	Значение XX в шестнадцатеричном исчислении
‘XXh’	Значение XX в шестнадцатеричном исчислении
||	Символ конкатенации 03||04=0304

1.2. Ссылки

В настоящем приложении используются следующие источники:

ISO/IEC 7816-2	Идентификационные карточки – карточки с интегральными микросхемами. Часть 2: размеры и расположение контактов. ISO/IEC 7816-2:2007.
ISO/IEC 7816-3	Идентификационные карточки – карточки с интегральными микросхемами. Часть 3: электрический интерфейс и протоколы передачи. ISO/IEC 7816-3:2006.
ISO/IEC 7816-4	Идентификационные карточки – карточки с интегральными микросхемами. Часть 4: организация, безопасность и команды обмена. ISO/IEC 7816-4:2013 + Cor 1: 2014.
ISO/IEC 7816-6	Идентификационные карточки – карточки с интегральными микросхемами. Часть 6: межсекторные элементы данных для обмена. ISO/IEC 7816-6:2004 + Cor 1: 2006.
ISO/IEC 7816-8	Идентификационные карточки – карточки с интегральными микросхемами. Часть 8: команды операций по обеспечению безопасности. ISO/IEC 7816-8:2004.
ISO/IEC 9797-2	Информационные технологии. Техники обеспечения безопасности. Коды аутентификации сообщений (MAC). Часть 2: механизмы с использованием хэш-функции. ISO/IEC 9797-2:2011

2. Электрические и физические характеристики

TCS_01 Все электрические сигналы соответствуют стандарту ISO/IEC 7816-3, если не указано иначе.

TCS_02 Расположение и размеры контактов карточки соответствуют стандарту ISO/IEC 7816-2.

2.1. Напряжение питания и потребление тока

TCS_03 Карточка работает в соответствии со спецификациями в рамках предельных значений потребления, указанных в стандарте ISO/IEC 7816-3.

TCS_04 Карточка работает при Vcc = 3 V (± 0,3V) или Vcc = 5 V (± 0,5 V).

Выбор напряжения производится в соответствии со стандартом ISO/IEC 7816-3.

2.2. Напряжение программирования V_{pp}

TCS_05 Карточка не требует напряжения программирования на выводе C6. Предполагается, что вывод C6 к IFD не подсоединяется. Контакт C6 может быть соединён с Vcc карточки, но не заземлён. В любом случае это напряжение не должно интерпретироваться.

2.3. Формирование и частота тактовых сигналов

TCS_06 Карточка работает в диапазоне частот 1-5 МГц и может поддерживать более высокие частоты. В рамках одного сеанса использования карточки тактовая частота может варьироваться в пределах ± 2%. Тактовая частота генерируется бортовым устройством, а не самой карточкой. Рабочий цикл может варьироваться в пределах 40-60%.

TCS_07 В соответствии с параметрами, заложенными в файле карточки EF ICC, внешние часы можно остановить. Первый байт основного файла EF ICC кодирует условия режима остановки часов:

Низкий	**Высокий**		
Бит 3	**Бит 2**	**Бит 1**	
0	0	1	Остановка часов разрешена, предпочитаемый уровень отсутствует
0	1	1	Остановка часов разрешена, предпочитаемый уровень – высокий
1	0	1	Остановка часов разрешена, предпочитаемый уровень – низкий
0	0	0	Остановка часов не разрешена

0	1	0	Остановка часов разрешена только на высоком уровне
1	0	0	Остановка часов разрешена только на низком уровне

Биты 4-8 не используются.

2.4. Контакт ввода/вывода

TCS_08 Контакт ввода/вывода C7 используется для получения данных из IFD и передачи данных в IFD. Во время работы в режиме передачи может находиться только карточка или только IFD. Если оба устройства работают в режиме передачи, никакого вреда карточке не наносится. Если передача данных не производится, карточка переключается в режим приёма.

2.5. Состояния карточки

TCS_09 В случае подачи на карточку напряжения она может находиться в двух состояниях:

В рабочем состоянии при выполнении команд или обмене данными с цифровым блоком,
В нерабочем состоянии в остальное время; в этом состоянии все данные на карточке сохраняются.

3. Аппаратное обеспечение и связь

3.1. Введение

В настоящем пункте излагаются минимальные требования к функциям карточек тахографа и БУ в целях обеспечения правильной работы и эксплуатационной совместимости.

Карточки тахографа в максимальной степени соответствуют применимым нормам стандарта ISO/IEC (прежде всего ISO/IEC 7816). Однако в целях уточнения некоторых ограниченных видов использования или различий, в случае их наличия, характеристики всех команд и протоколов указываются полностью. Указанные команды полностью соответствуют упомянутым выше стандартам, если не оговорено иное.

3.2. Протокол передачи данных

TCS_10 Протокол передачи данных соответствует ISO/IEC 7816-3 при T = 0 и T = 1. В частности, БУ должно распознавать сигналы продления времени ожидания, передаваемые карточкой.

3.2.1 Протоколы

TCS_11 Карточка поддерживает и протокол **T=0**, и протокол **T=1**. Кроме того, карточка может поддерживать дополнительные протоколы, ориентированные на контакты.

TCS_12 **T=0** – протокол по умолчанию, поэтому для изменения протокола на **T=1** нужна команда PTS.

TCS_13 Устройства поддерживают **прямую связь** в обоих протоколах: таким образом, прямая связь для карточки обязательна.

TCS_14 Байт **карточки размера информационного поля** в ATR представлен символами TA3. Это значение составляет не менее ‘F0h’ (=240 байтов).

К протоколам применяются следующие ограничения.

TCS_15 **T=0**

- Интерфейс принимает ответ на входе и выходе после нарастания сигнала на RST начиная с 400 вц.
- Интерфейс способен считывать символы, отделённые во времени на 12 эев.
- Интерфейс распознаёт ошибочные символы и их повторение, если они разделены во времени на 13 эев. В случае обнаружения ошибочного символа контакт ввода/вывода может отражать сигнал ошибки в интервале 1-2 эев. Устройство реагирует на задержку продолжительностью 1 эев.
- Интерфейс принимает ATR размером 33 байта (TS+ 32)
- Если в ATR есть TC1, для символов, передаваемых интерфейсом, должно быть предусмотрено дополнительное время хранения, хотя временной интервал между символами, посылаемыми

карточкой, может и в этом случае составлять 12 эев. Это также применимо к символу ACK, посылаемому карточкой после передачи символа P3 интерфейсом.

- Интерфейс принимает символ NUL, передаваемый карточкой.
- Интерфейс принимает дополнительный режим для ACK.
- Команда на получение ответа не может использоваться в режиме прямого вывода для получения данных, длина которых может превышать 255 байтов.

TCS_16 **T=1**

- Байт NAD не используется (NAD устанавливается на ‘00’).
- S-block ABORT: не используется.
- S-block VPP state error: не используется.
- Общая длина цепочки вывода данных для поля данных не превышает 255 байтов (обеспечивается IFD).
- Размер информационного поля для интерфейса (IFSD) указывается IFD сразу же после ATR: IFD передаёт запрос S-Block IFS после ATR, после чего карточка передаёт обратно данные S-Block IFS. Рекомендуемое значение для IFSD: 254 байта.
- Карточка не требует корректировки IFS.

3.2.2 ATR

TCS_17 Устройство проверяет байты ATR в соответствии со стандартом ISO/IEC 7816-3. Проверка архивных символов ATR не производится.

Пример базового бипротокола AID согласно ISO/IEC 7816-3

Символ	**Значение**	**Примечания**
TS	‘3Bh’	Указывает на прямую связь.
T0	‘85h’	TD1 присутствует; имеются 5 архивных байтов.
TD1	‘80h’	TD2 присутствует; следует применять T=0
TD2	‘11h’	TA3 присутствует; следует применять T=1
TA3	‘XXh’ (не менее ‘F0h’)	Размер информационного поля карточки (IFSC)
TH1-TH5	‘XXh’	Архивные символы
TCK	‘XXh’	Проверочный символ (исключительно OR)

TCS_18 После ответа на сигнал перезагрузки (ATR) выбирается по косвенным признакам главный файл (MF), который становится текущей директорией.

3.2.3 PTS

TCS_19 Протоколом по умолчанию является T=0. Для перехода на протокол T=1 устройство должно передать на карточку сигнал PTS (также обозначаемый сокращением PPS).

TCS_20 Поскольку для карточки оба протокола T=0 и T=1 обязательны, базовый сигнал PTS для перехода с одного протокола на другой обязателен и для карточки.

PTS может использоваться, как указано в стандарте ISO/IEC 7816-3, для перехода на более высокие скорости передачи данных в бодах, чем скорость по умолчанию, предлагаемая в соответствующих случаях карточкой в ATR (байт (TA(1)).

Более высокие скорости передачи в бодах для карточки факультативны.

TCS_21 Если другая скорость передачи в бодах, помимо скорости по умолчанию, не поддерживается (или если не поддерживается выбранная скорость передачи в бодах), карточка передаёт правильную команду PTS в соответствии со стандартом ISO/IEC 7816-3, опустив байт PPS1.

Примеры базовой команды PTS для выбора протокола указаны ниже:

Символ	**Значение**	**Примечания**

PPSS	‘FFh’	Начальный символ
PPS0	‘00h’ или ‘01h’	PPS1-PPS3 не присутствуют; ‘00h’ для выбора T0, ‘01h’ для выбора T1.
PK	‘XXh’	Проверочный символ: ‘XXh’ = ‘FFh’, если PPS0 = ‘00h’, ‘XXh’ = ‘FFh’, если PPS0 = ‘01h’.

3.3. Правила доступа

TCS_22 Правило доступа указывает режим доступа, т.е. команду, и соответствующие условия обеспечения безопасности. Если эти условия соблюдены, обрабатывается соответствующая команда.

TCS_23 Для карточки тахографа действительны следующие условия безопасности:

Сокращение	Значение
ALW	Действие возможно во всех случаях и может быть выполнено без ограничений. Команда и ответ APDU передаются простым текстом, т.е. без защищённого обмена сообщениями.
NEV	Действие невозможно ни в каких случаях.
PLAIN-C	Команда APDU передаётся простым текстом, т.е. без защищённого обмена сообщениями.
PWD	Действие может быть выполнено только в том случае, если ПИН-код карточки мастерской успешно прошёл проверку, т.е. если установлен внутренний статус безопасности карточки «PIN_Verified». Команда должна отправляться без защищённого обмена сообщениями.
EXT-AUT-G1	Действие может выполняться, только если успешно выполнена команда внешней аутентификации первого поколения (см. также приложение 11, часть А).
SM-MAC-G1	APDU (команда и ответ) должны применяться при защищённом обмене сообщениями первого поколения только в режиме аутентификации (см. приложение 11, часть А).
SM-C-MAC-G1	Команда APDU должна применяться при защищённом обмене сообщениями первого поколения только в режиме аутентификации (см. приложение 11, часть А).
SM-R-ENC-G1	Ответ APDU должен применяться при защищённом обмене сообщениями первого поколения в зашифрованном виде (см. приложение 11, часть А), т.е. код аутентификации сообщения не выдаётся.
SM-R-ENC-MAC-G1	Ответ APDU должен применяться при защищённом обмене сообщениями первого поколения в режиме шифрования с последующей аутентификацией (см. приложение 11, часть А).
SM-MAC-G2	APDU (команда и ответ) должны применяться при защищённом обмене сообщениями второго поколения только в режиме аутентификации (см. приложение 11, часть Б).
SM-C-MAC-G2	Команда APDU должна применяться при защищённом обмене сообщениями второго поколения только в режиме аутентификации (см. приложение 11, часть Б).
SM-R-ENC-MAC-G2	Ответ APDU должен применяться при защищённом обмене сообщениями второго поколения в режиме шифрования с последующей аутентификацией (см. приложение 11, часть Б).

TCS_24 Данные условия обеспечения безопасности могут быть связаны следующими способами:

- **AND**: Должны быть выполнены все условия безопасности
- **OR**: Должно быть выполнено хотя бы одно условие безопасности

Правила доступа к системе файлов, т.е. команды SELECT, READ BINARY и UPDATE BINARY, представлены в главе 4. Правила доступа для остальных команд представлены в таблицах ниже.

TCS_25 В приложении DF Tachograph G1 соблюдаются следующие правила доступа:

Команда	Карточка водителя	Карточка мастерской	Контрольная карточка	Карточка предприятия

External Authenticate				
• Аутентификация первого поколения	ALW	ALW	ALW	ALW
• Аутентификация второго поколения	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Hash	Неприменимо	Неприменимо	ALW	Неприменимо
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Неприменимо	Неприменимо	ALW	Неприменимо
Verify	Неприменимо	ALW	Неприменимо	Неприменимо

TCS_26 В приложении DF Tachograph_G2 соблюдаются следующие правила доступа:

Команда	**Карточка водителя**	**Карточка мастерской**	**Контрольная карточка**	**Карточка предприятия**
External Authenticate				
• Аутентификация первого поколения	Неприменимо	Неприменимо	Неприменимо	Неприменимо
• Аутентификация второго поколения	ALW	PWD	ALW	ALW
Internal Authenticate	Неприменимо	Неприменимо	Неприменимо	Неприменимо
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Неприменимо	ALW	ALW	Неприменимо
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Hash	Неприменимо	Неприменимо	ALW	Неприменимо
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Неприменимо	Неприменимо
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Неприменимо	Неприменимо	ALW	Неприменимо
Verify	Неприменимо	ALW	Неприменимо	Неприменимо

TCS_27 В MF соблюдаются следующие правила доступа:

Команда	**Карточка водителя**	**Карточка мастерской**	**Контрольная карточка**	**Карточка предприятия**
External Authenticate				
• Аутентификация первого поколения	Неприменимо	Неприменимо	Неприменимо	Неприменимо
• Аутентификация второго поколения	ALW	PWD	ALW	ALW
Internal Authenticate	Неприменимо	Неприменимо	Неприменимо	Неприменимо
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW

MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Compute Digital Signature	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Hash	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Hash of File	Неприменимо	Неприменимо	Неприменимо	Неприменимо
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Неприменимо	ALW	Неприменимо	Неприменимо

TCS_28 Карточка тахографа может принять или не принять команду с более высоким уровнем безопасности, нежели указано в условиях безопасности. Это значит, что если условие безопасности – ALW (или PLAIN-C), карточка может принять команду с защищённым обменом сообщениями (в режиме шифрования и/или аутентификации). Если по условию безопасности требуется защищённый обмен сообщениями в режиме аутентификации, карточка тахографа может принять команду с защищённым обменом сообщениями того же поколения в режиме аутентификации и шифрования.

Примечание: Описания команд предлагают более подробную информацию о поддержке команд различными типами карточек тахографов и различными DF.

3.4. Обзор команд и кодов ошибок

Команды и структура файлов определяются стандартом ISO/IEC 7816-4 и соответствуют ему.

В настоящем разделе описаны следующие пары команд и ответов APDU. Варианты команд, которые поддерживает приложение 1 и 2 поколений, представлены в соответствующих описаниях команд.

Команда	**INS**
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’
• VERIFY CERTIFICATE	
• COMPUTE DIGITAL SIGNATURE	
• VERIFY DIGITAL SIGNATURE	
• HASH	
• PERFORM HASH OF FILE	
• PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
• SET DIGITAL SIGNATURE TEMPLATE	
• SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Характеристики состояния SW1 SW2 включаются в любое ответное сообщение и означают состояние обработки команды.

SW1	**SW2**	**Значение**
90	00	Нормальная обработка
61	XX	Нормальная обработка. XX = число имеющихся байтов для ответа.
62	81	Обработка предупреждения. Часть передаваемых обратно данных может быть повреждена
63	00	Аутентификация неуспешна (предупреждение)
63	CX	Неправильный код CHV (PIN). Счётчик оставшихся попыток указывается с помощью ‘X’.
64	00	Ошибка исполнения – состояние постоянной памяти не изменилось. Ошибка целостности
65	00	Ошибка исполнения – состояние постоянной памяти изменилось
65	81	Ошибка исполнения – состояние постоянной памяти изменилось – отказ памяти
66	88	Ошибка безопасности: неверная криптографическая контрольная сумма (во время защищённого обмена сообщениями) или неправильный сертификат (во время проверки сертификата) или неправильная криптограмма (во время внешней аутентификации) или неправильная подпись (во время проверки подписи)
67	00	Неправильная длина (неправильные значения Lc или Le)
68	82	Защищённый обмен сообщениями не поддерживается
68	83	Ожидается последняя команда цепочки
69	00	Запрещённая команда (отсутствие ответа в T=0)
69	82	Статус защиты неприемлем
69	83	Метод аутентификации заблокирован
69	85	Условия использования неприемлемы
69	86	Команда не разрешена (активный EF отсутствует)

69	87	Отсутствие предусмотренных криптозащищённых объектов данных
69	88	Неверные криптозащищённые объекты данных
6A	80	Неверные параметры в поле данных
6A	82	Файл не найден
6A	86	Неправильные параметры P1-P2
6A	88	Исходные данные не найдены
6B	00	Неправильные параметры (выход за пределы EF)
6C	XX	Неправильная длина, SW2 указывает точную длину. Поле данных не выдаётся
6D	00	Командный код не поддерживается или недействителен
6E	00	Класс не поддерживается
6F	00	Другие контрольные ошибки

TCS_30 Если выполняется более чем одно условие ошибки в одной команде APDU, карточка может выдать любой из соответствующих статусов.

3.5. Описания команд

В настоящей главе описываются параметры обязательных команд для карточек тахографа.

Дополнительные соответствующие данные, относящиеся к криптографическим операциям, представлены в приложении 11 «Общие механизмы защиты» для тахографов первого и второго поколений.

Все команды описываются независимо от используемого протокола (T=0 или T=1). Байты APDU: CLA, INS, P1, P2, Lc и Le указываются всегда. Если байты Lc или Le для данной команды не нужны, относящаяся к ней длина, значение и описание не заполнены.

TCS_31 Если запрашиваются оба байта длины (Lc и Le), описываемая команда разделяется на две части; если IFD использует протокол T=0: IFD передаёт команду, описанную с помощью данных P3=Lc + данные, после чего направляет команду GET_RESPONSE (см. пункт 3.5.6) с P3=Le.

TCS_32 Если запрашиваются оба байта длины и если Le=0 (защищённый обмен сообщениями):

- В случае использования протокола T=1 карточка выдает Le=0, передавая все имеющиеся выходные данные.
- В случае использования протокола T=0 IFD передает первую команду с P3=Lc + данные, карточка передаёт ответ (на это имплицитное значение Le=0) с помощью байтов состояния '**61La**', где La – число байтов, имеющихся для ответа. После этого IFD генерирует команду GET REPONSE с P3 = La для чтения данных.

TCS_33 Карточка тахографа может поддерживать поля расширенной длины в соответствии с ISO/IEC 7816-4 как дополнительную функцию. Карточка тахографа, поддерживающая поля расширенной длины,

- Указывает на поддержку полей расширенной длины в ATR
- Обеспечивает поддерживаемые размеры буфера посредством информации о расширенной длине в EF ATR/INFO; см. TCS_146.
- Указывает, поддерживает ли она поля расширенной длины для T = 1 и/или T = 0 в EF расширенной длины; см. TCS_147.
- Поддерживает поля расширенной длины для приложений тахографов первого и второго поколений.

Примечания:
Все команды указываются для полей короткой длины. Применение APDU расширенной длины разъясняется в ISO/IEC 7816-4.
В целом, команды указываются в режиме простого текста, т.е. без защищённого обмена сообщениями, а уровень защищённого обмена сообщениями описан в приложении 11. По правилам доступа, касающимся команды, понятно, поддерживает ли команда защищённый обмен сообщениями или нет и поддерживает ли команда защищённый обмен сообщениями первого и/или второго поколений. Некоторые варианты команды описываются и с точки зрения защищённого обмена сообщениями, чтобы проиллюстрировать применение защищённого обмена сообщениями.

TCS_34 БУ полностью выполняет протокол взаимной аутентификации БУ и карточки второго поколения во время сеанса использования карточки, включая проверку сертификата (если требуется) в DF Tachograph, DF Tachograph_G2 или MF.

3.5.1 SELECT

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда SELECT используется:

- для выбора приложения DF (должен использоваться выбор по названию);
- для выбора элементарного файла, соответствующего представленному файлу ID

3.5.1.1 Выбор по названию (AID)

Данная команда позволяет выбрать приложение DF на карточке.

TCS_35 Данная команда может быть выполнена из любой точки структуры файла (после ATR или в любое время).

TCS_36 Выбор приложения приводит к перезагрузке текущей среды защиты. После выбора приложения текущий открытый ключ больше не выбирается. Условие доступа EXT-AUT-G1 также теряется. Если команда выполняется без защищённого обмена сообщениями, ключи предыдущего сеанса защищённого обмена сообщениями больше не доступны.

TCS_37 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Выбор по названию (AID)
P2	1	‘0Ch’	Ответа не ожидается
Lc	1	‘NNh’	Число байтов, переданных на карточку (длина AID): ‘06h’ для приложения тахографа
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ для приложения тахографа первого поколения AID: ‘FF 53 4D 52 44 54’ для приложения тахографа второго поколения

Ответ на команду SELECT не требуется (в случае T=1 Le отсутствует, а в случае T=0 запрос на ответ не передаётся).

TCS_38 **Ответное сообщение (запроса на ответ нет)**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если приложение, соответствующее AID, не найдено, статус обработки выдаётся в виде ‘**6A82**’.
- При T=1, если присутствует байт Le, состояние выдаётся в виде **‘6700’.**
- При T=0, если запрос на ответ поступает после команды SELECT, статус выдаётся в виде **‘6900’.**
- Если выбранное приложение считается повреждённым (в атрибутах файла обнаружена ошибка целостности), статус обработки выдаётся в виде ‘**6400**’ или ‘**6581**’.

3.5.1.2 Выбор элементарного файла с использованием идентификатора файла

TCS_39 **Командное сообщение**

TCS_40 Карточка тахографа поддерживает защищённый обмен сообщениями второго поколения, как указано в части Б приложения 11 для данного варианта команды.

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘A4h’	

P1	1	‘02h’	Выбор EF в текущем DF
P2	1	‘0Ch’	Ответа не ожидается
Lc	1	‘02h’	Число байтов, переданных на карточку
#6-#7	2	‘XXXXh’	Идентификатор файла

Ответ на команду SELECT не требуется (в случае T=1 Le отсутствует, а в случае T=0 запрос на ответ не передаётся).

TCS_41 **Ответное сообщение (запроса на ответ нет)**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если приложение, соответствующее идентификатору файла, не найдено, статус обработки выдаётся в виде ‘**6A82**’.
- При T=1, если присутствует байт Le, состояние выдаётся в виде **‘6700’.**
- При T=0, если запрос на ответ поступает после команды SELECT, статус выдаётся в виде **‘6900’.**
- Если выбранный файл считается повреждённым (в атрибутах файла обнаружена ошибка целостности), статус обработки выдаётся в виде ‘**6400**’ или ‘**6581**’.

3.5.2 READ BINARY

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда READ BINARY используется для считывания данных с прозрачного файла.

Ответ карточки сводится к обратной передаче считанных данных, которые могут быть включены в структуру защищённого обмена сообщениями.

3.5.2.1 Команда со смещением в P1-P2

Эта команда позволяет IFD считывать данные с выбранного в данный момент файла EF в незащищённом виде.

Примечание: Данная команда без защищённого обмена сообщениями может использоваться только для чтения файла, который поддерживает условие безопасности ALW для режима доступа Read.

TCS_42 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Смещение в байтах от начала файла: Самый значимый байт
P2	1	‘XXh’	Смещение в байтах от начала файла: Наименее значимый байт
Le	1	‘XXh’	Ожидаемая длина данных. Число байтов, подлежащих извлечению.

Примечание: бит 8 байта P1 должен быть равен 0.

TCS_43 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#X	X	‘XX..XXh’	Прочитанные данные
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если EF не выбран, статус обработки выдаётся в виде **‘6986’.**
- Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей ‘**6982**’.
- Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **‘6B00’.**
- Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размер EF), статус обработки выдаётся в виде ‘**6700’** или ‘**6Cxx’**, где 'xx' указывает точную длину.
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **‘6400’** или ‘**6581’.**
- Если в хранящихся данных обнаружена ошибка целостности, карточка выдаёт требуемые данные, и статус обработки выдаётся в виде **‘6281’.**

3.5.2.1.1 Команда с защищённым обменом сообщениями (примеры)

Данная команда позволяет IFD считывать данные из EF, выбранного для защищённого обмена сообщениями, чтобы проверить целостность получаемых данных и обеспечить их конфиденциальность, если применяется условие безопасности SM-R-ENC-MAC-G1 (первого поколения) или SM-R-ENC-MAC-G2 (второго поколения).

TCS_44 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘0Ch’	Требуется защищённый обмен сообщениями
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (смещение в байтах от начала файла): Самый значимый байт
P2	1	‘XXh’	P2 (смещение в байтах от начала файла): Наименее значимый байт

Lc	1	‘XXh’	Длина вводимых данных в защищённом виде
#6	1	‘97h’	T_{LE} : метка, указывающая на спецификацию ожидаемой длины
#7	1	‘01h’	L_{LE} : длина ожидаемой длины
#8	1	‘NNh’	Спецификация ожидаемой длины (исходное значение Le): Число байтов, подлежащих извлечению
#9	1	‘8Eh’	T_{CC} : метка, указывающая на криптографическую контрольную сумму
#10	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘04h’ для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#11-#(10+L)	L	‘XX..XXh’	Криптографическая контрольная сумма
Le	1	‘00h’	Как указано в стандарте ISO/IEC 7816-4

TCS_45 **Ответное сообщение, если не требуется SM-R-ENC-MAC-G1 (первого поколения)/SM-R-ENC-MAC-G2 (второго поколения) и если формат ввода защищённого обмена сообщениями верен:**

Байт	Длина	Значение	Описание
#1	1	‘99h’	Метка статуса обработки (SW1-SW2) – факультативно для защищённого обмена сообщениями первого поколения
#2	1	‘02h’	Длина статуса обработки
#3 - #4	2	‘XX XXh’	Статус обработки для незащищённого ответа APDU
#5	1	‘81h’	T_{PV} : метка, указывающая на значение обычных данных
#6	L	‘NNh’ или ‘81 NNh’	L_{PV}: длина переданных обратно данных (= исходное значение Le) L равна 2 байтам, если L_{PV} > 127 байтов.
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Значения обычных данных
#(6+L+NN)	1	‘8Eh’	T_{CC} : метка, указывающая на криптографическую контрольную сумму
#(7+L+NN)	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘04h’ для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Криптографическая контрольная сумма
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

TCS_46 **Ответное сообщение, если требуется SM-R-ENC-MAC-G1 (первого поколения)/SM-R-ENC-MAC-G2 (второго поколения) и если формат ввода защищённого обмена сообщениями верен:**

Байт	Длина	Значение	Описание
#1	1	‘87h’	$T_{PI\,CG}$: Метка, указывающая на зашифрованные данные (криптограмма)
#2	L	‘MMh’ или ‘81 MMh’	$L_{PI\,CG}$: длина выданных зашифрованных данных (отличная от исходного значения Le команды, что обусловлено заполнением). L равна 2 байтам, если $L_{PI\,CG}$ > 127 байтов.
#(2+L)-#(1+L+MM)	MM	‘01XX..XXh’	Зашифрованные данные: Показатель заполнения и криптограмма
#(2+L+MM)	1	‘99h’	Метка статуса обработки (SW1-SW2) – факультативно для защищённого обмена сообщениями первого поколения
#(3+L+MM)	1	‘02h’	Длина статуса обработки

#(4+L+MM) - #(5+L+MM)	2	‘XX XXh’	Статус обработки для незащищённого ответа APDU
#(6+L+MM)	1	‘8Eh’	T_{CC} : метка, указывающая на криптографическую контрольную сумму
#(7+L+MM)	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘04h’ для защищённого обмена сообщениями первого поколения (см. часть A приложения 11) ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(8+L+MM)- #(7+N+L+MM)	N	‘XX..XXh’	Криптографическая контрольная сумма
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

Команда READ BINARY может выдавать статусы регулярной обработки, перечисленные в TCS_43 с меткой ‘99h’, как описано в TCS_59 с применением структуры ответов защищённого обмена сообщениями.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с защищённым обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_47 **Ответное сообщение, если формат ввода защищённого обмена данными неправильный**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если ключ текущего сеанса отсутствует, статус обработки выдается в виде **‘6A88’**. Это происходит либо по той причине, что ключ сеанса ещё не создан, либо потому, что ключ сеанса больше недействителен (в этом случае IFD должен повторить процесс взаимной аутентификации в целях генерации нового ключа сеанса).
- Если некоторые ожидаемые объекты данных (как указано выше) в формате защищённого обмена данными отсутствуют, статус обработки выдаётся в виде **‘6987’**: эта ошибка имеет место в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- Если некоторые объекты данных неправильны, статус обработки выдается в виде **‘6988’**: эта ошибка имеет место в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой.
- Если проверка криптографической контрольной суммы показала неправильный результат, статус обработки выдаётся в виде **‘6688’.**

3.5.2.2 Команда с коротким идентификатором EF (элементарного файла)

Данный вариант команды позволяет IFD выбрать EF при помощи короткого идентификатора EF и считывать данные из этого EF.

TCS_48 Карточка тахографа поддерживает данный вариант команды для всех элементарных файлов с указанным коротким идентификатором EF. Такие короткие идентификаторы EF представлены в главе 4.

TCS_49 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Бит 8 устанавливается на 1 Биты 7 и 6 устанавливаются на 00 Бит 5 – 1 кодирует короткий идентификатор EF соответствующего EF
P2	1	‘XXh’	Кодирует смещение от 0 до 255 байтов в EF с указанием P1
Le	1	‘XXh’	Ожидаемая длина данных. Число байтов, подлежащих извлечению.

Примечание: Короткие идентификаторы EF, используемые в приложении тахографов второго поколения, представлены в главе 4.

Если P1 кодирует короткий идентификатор EF и команда проводится успешно, идентифицированный EF становится текущим выбранным EF (текущий EF).

TCS_50 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#L	L	‘XX..XXh’	Прочитанные данные
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если приложение, соответствующее короткому идентификатору EF, не найдено, статус обработки выдаётся в виде ‘**6A82**’.
- Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей ‘**6982**’.
- Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **‘6B00’.**
- Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размер EF), статус обработки выдаётся в виде ‘**6700’** или ‘**6Cxx’**, где 'xx' указывает точную длину.
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **‘6400’** или ‘**6581’.**
- Если в хранящихся данных обнаружена ошибка целостности, карточка выдаёт требуемые данные, и статус обработки выдаётся в виде **‘6281’.**

3.5.2.3 Команда с нечётным командным байтом

Данный вариант команды позволяет IFD считывать данные с EF с 32768 или более байтов.

TCS_51 Карточка тахографа, поддерживающая EF с 32768 или более байтов, поддерживает данный вариант команды для данных EF. Карточка тахографа может поддерживать или не поддерживать данный вариант команды для других EF, за исключением EF Sensor_Installation_Data; см. TCS_156 и TCS_160.

TCS_52 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘B1h’	Read Binary
P1	1	‘00h’	Текущий EF
P2	1	‘00h’	
Lc	1	‘NNh’	Длина Lc смещённого объекта данных.
#6-#(5+NN)	NN	‘XX..XXh’	Смещённый объект данных: Метка ‘54h’ Длина ‘01h’ или ‘02h’ Значение смещение
Le	1	‘XXh’	Число байтов, подлежащих извлечению.

IFD кодирует длину смещённого объекта данных с минимальным возможным числом октетов, т.е. с помощью байта длины ‘01h’ IFD кодирует смещение от 0 до 255, а с помощью байта длины ‘02h’ – смещение от ‘256’ до ‘65535’ байтов.

TCS_53 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#L	L	‘XX..XXh’	Считываемые данные включаются в дискретный объект данных с меткой ‘53h’.
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если EF не выбран, статус обработки выдаётся в виде **‘6986’.**
- Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей ‘**6982**’.

- Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **‘6B00’**.
- Если размер данных, подлежащих извлечению, не соответствует размеру EF (смещение + Le > размер EF), статус обработки выдаётся в виде ‘**6700’** или ‘**6Cxx’**, где 'xx' указывает точную длину.
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **‘6400’** или ‘**6581’.**
- Если в хранящихся данных обнаружена ошибка целостности, карточка выдаёт требуемые данные, и статус обработки выдаётся в виде **‘6281’**.

3.5.2.3.1 Команда с защищённым обменом сообщениями (пример)

Следующий пример иллюстрирует применение защищённого обмена сообщениями, если применяется условие безопасности SM-MAC-G2.

TCS_54 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	‘0Ch’	Требуется защищённый обмен сообщениями
INS	1	‘B1h’	Read Binary
P1	1	‘00h’	Текущий EF
P2	1	‘00h’	
Lc	1	‘XXh’	Длина поля защищённых данных
#6	1	‘B3h’	Метка данных простого значения, кодируемых в BER-TLV
#7	1	‘NNh’	L_{PV}: длина переданных данных
#(8)-#(7+NN)	NN	‘XX..XXh’	Простые данные, закодированные в BER-TLV, т.е. смещённый объект данных с меткой ‘54’
#(8+NN)	1	‘97h’	T_{LE} : метка, указывающая на спецификацию ожидаемой длины
#(9+NN)	1	‘01h’	L_{LE} : Длина ожидаемой длины
#(10+NN)	1	‘XXh’	Спецификация ожидаемой длины (исходное значение Le): Число байтов, подлежащих извлечению
#(11+NN)	1	‘8Eh’	T_{CC} : Метка, указывающая на криптографическую контрольную сумму
#(12+NN)	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Криптографическая контрольная сумма
Le	1	‘00h’	Как указано в стандарте ISO/IEC 7816-4

TCS_55 Ответное сообщение, если команда выполнена успешно

Байт	Длина	Значение	Описание
#1	1	‘B3h’	Простые данные, закодированные в BER-TLV
#2	L	‘NNh’ или ‘81 NNh’	L_{PV}: длина переданных обратно данных (= исходное значение Le). L равна 2 байтам, если L_{PV} > 127 байтов.
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	Простые данные, закодированные с BER-TLV, т.е. прочитанные данные, включённые в дискретный объект данных с меткой ‘53h’.
#(2+L+NN)	1	‘99h’	Статус обработки для незащищённого ответа APDU
#(3+L+NN)	1	‘02h’	Длина статуса обработки
#(4+L+NN) - #(5+L+NN)	2	‘XX XXh’	Статус обработки для незащищённого ответа APDU
#(6+L+NN)	1	‘8Eh’	T_{CC} : Метка, указывающая на криптографическую контрольную сумму
#(7+L+NN)	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа

			AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(8+L+NN)- #(7+M+L+NN)	M	‘XX..XXh’	Криптографическая контрольная сумма
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

3.5.3 UPDATE BINARY

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Командное сообщение UPDATE BINARY начинает обновление (удаление + запись) битов, которые уже присутствуют в данных файла EF с помощью битов, содержащихся в команде APDU.

3.5.3.1 Команда со смещением в P1-P2

Данная команда позволяет IFD записывать данные в выбранный в данный момент EF без проверки целостности полученных данных карточкой.

Примечание: Данная команда без защищённого обмена сообщениями может использоваться только для обновления файла, который поддерживает условие безопасности ALW для режима доступа Update.

TCS_56 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Смещение в байтах от начала файла: Самый значимый байт
P2	1	‘XXh’	Смещение в байтах от начала файла: Наименее значимый байт
Lc	1	‘NNh’	Длина Lc данных, подлежащих обновлению. Число байтов, подлежащих записи.
#6-#(5+NN)	NN	‘XX..XXh’	Данные, подлежащие записи

Примечание: бит 8 байта P1 должен быть равен 0.

TCS_57 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если EF не выбран, статус обработки выдаётся в виде **‘6986’.**
- Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей ‘**6982**’.
- Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **‘6B00’.**
- Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размер EF), статус обработки выдаётся в виде ‘**6700’.**
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **‘6400’** или ‘**6500’.**
- Если запись неуспешна, статус обработки выдаётся в виде **‘6581’.**

3.5.3.1.1 Команда с защищённым обменом сообщениями (примеры)

Данная команда позволяет IFD записывать данные в выбранный в данный момент EF с проверкой целостности полученных данных карточкой. Поскольку требование конфиденциальности отсутствует, данные не шифруются.

TCS_58 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘0Ch’	Требуется защищённый обмен сообщениями
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Смещение в байтах от начала файла: Самый значимый байт
P2	1	‘XXh’	Смещение в байтах от начала файла: Наименее значимый байт
Lc	1	‘XXh’	Длина поля защищённых данных

#6	1	‘81h’	T_{PV} : Метка, указывающая на значение обычных данных
#7	L	‘NNh’ или ‘81 NNh’	L_{PV}: длина переданных данных. L равна 2 байтам, если L_{PV} > 127 байтов.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Значение простых данных (данные, подлежащие записи)
#(7+L+NN)	1	‘8Eh’	T_{CC} : Метка, указывающая на криптографическую контрольную сумму
#(8+L+NN)	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘04h’ для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Криптографическая контрольная сумма
Le	1	‘00h’	Как указано в стандарте ISO/IEC 7816-4

TCS_59 **Ответное сообщение, если формат ввода защищённого обмена данными правильный**

Байт	Длина	Значение	Описание
#1	1	‘99h’	T_{SW} : Метка, указывающая на характеристики статуса (должна быть защищена с помощью криптографической суммы)
#2	1	‘02h’	L_{SW}: длина переданных обратно характеристик статуса
#3-#4	2	‘XXXXh’	Статус обработки для незащищённого ответа APDU
#5	1	‘8Eh’	T_{CC} : Метка, указывающая на криптографическую контрольную сумму
#6	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘04h’ для защищённого обмена сообщениями первого поколения (см. часть А приложения 11) ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#7-#(6+L)	L	‘XX..XXh’	Криптографическая контрольная сумма
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

Данные о статусах «нормальной» обработки, описанные для команды UPDATE BINARY, передаваемой в незащищённом виде (см. пункт 3.5.3.1), могут возвращаться с использованием структур ответного сообщения, описанных выше.

Кроме того, могут иметь место некоторые ошибки, которые конкретно связаны с защищённым обменом сообщениями. В этом случае данные о состоянии обработки просто возвращаются, не задействуя использованную структуру защиты данных:

TCS_60 **Ответное сообщение в случае ошибки в защищённом обмене сообщениями**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если ключ текущего сеанса отсутствует, статус обработки выдается в виде **‘6A88’.**
- Если некоторые ожидаемые объекты данных (как указано выше) в формате защищённого обмена данными отсутствуют, статус обработки выдаётся в виде **‘6987’**: эта ошибка имеет место в том случае, если ожидаемая метка отсутствует или если основная часть команды составлена неправильно.
- Если некоторые объекты данных неправильны, статус обработки выдается в виде **‘6988’**: эта ошибка имеет место в том случае, если требуемые метки есть, но длина некоторых из них отличается от ожидаемой.
- Если проверка криптографической контрольной суммы показала неправильный результат, статус обработки выдаётся в виде **‘6688’.**

3.5.3.2 Команда с коротким идентификатором EF

Данный вариант команды позволяет IFD выбрать EF при помощи короткого идентификатора EF и записывать данные из этого EF.

TCS_61 Карточка тахографа поддерживает данный вариант команды для всех элементарных файлов с указанным коротким идентификатором EF. Такие короткие идентификаторы EF представлены в главе 4.

TCS_62 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Бит 8 устанавливается на 1 Биты 7 и 6 устанавливаются на 00 Бит 5 – 1 кодирует короткий идентификатор EF соответствующего EF
P2	1	‘XXh’	Кодирует смещение от 0 до 255 байтов в EF с указанием P1
Lc	1	‘NNh’	Длина Lc данных, подлежащих обновлению. Число байтов, подлежащих записи.
#6-#(5+NN)	NN	‘XX..XXh’	Данные, подлежащие записи

TCS_63 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

Примечание: Короткие идентификаторы EF, используемые в приложении тахографов второго поколения, представлены в главе 4.

Если P1 кодирует короткий идентификатор EF и команда проводится успешно, идентифицированный EF становится текущим выбранным EF (текущий EF).

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если приложение, соответствующее короткому идентификатору EF, не найдено, статус обработки выдаётся в виде ‘**6A82**’.
- Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей ‘**6982**’.
- Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **‘6B00’.**
- Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размер EF), статус обработки выдаётся в виде ‘**6700’.**
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **‘6400’** или ‘**6581’.**
- Если запись неуспешна, статус обработки выдаётся в виде **‘6581’.**

3.5.3.3 Команда с нечётным командным байтом

Данный вариант команды позволяет IFD записывать данные в EF с 32768 или более байтов.

TCS_64 Карточка тахографа, поддерживающая EF с 32768 или более байтов, поддерживает данный вариант команды для данных EF. Карточка тахографа может поддерживать или не поддерживать данный вариант команды для других EF.

TCS_65 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘D7h’	Update Binary
P1	1	‘00h’	Текущий EF
P2	1	‘00h’	
Lc	1	‘NNh’	Lc Длина данных в поле командных данных
#6-#(5+NN)	NN	‘XX..XXh’	Смещённый объект данных с меткой ‘54h’ || Дискретный объект данных с меткой ‘53h’, включающий в себя данные, подлежащие

			записи

IFD кодирует длину смещённого объекта данных и дискретного объекта данных с минимальным возможным числом октетов, т.е. с помощью байта длины ‘01h’ IFD кодирует смещение/длину от 0 до 255, а с помощью байта длины ‘02h’ – смещение/длину от ‘256’ до ‘65535’ байтов.

TCS_66 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если EF не выбран, статус обработки выдаётся в виде **‘6986’.**
- Если условия безопасности выбранного файла не удовлетворены, команда прерывается с выдачей ‘**6982**’.
- Если смещение не соответствует размеру EF (смещение > размер EF), статус обработки выдаётся в виде **‘6B00’.**
- Если размер данных, подлежащих записи, не соответствует размеру EF (смещение + Lc > размер EF), статус обработки выдаётся в виде ‘**6700’.**
- Если в атрибутах файла обнаружена ошибка целостности, карточка считает, что файл повреждён и не может быть восстановлен, и статус обработки выдаётся в виде **‘6400’** или ‘**6500’.**
- Если запись неуспешна, статус обработки выдаётся в виде **‘6581’.**

3.5.3.3.1 Команда с защищённым обменом сообщениями (пример)

Следующий пример иллюстрирует применение защищённого обмена сообщениями, если применяется условие безопасности SM-MAC-G2.

TCS_67 Командное сообщение

Байт	Длина	Значение	Описание
CLA	1	‘0Ch’	Требуется защищённый обмен сообщениями
INS	1	‘D7h’	Update Binary
P1	1	‘00h’	Текущий EF
P2	1	‘00h’	
Lc	1	‘XXh’	Длина поля защищённых данных
#6	1	‘B3h’	Метка данных простого значения, кодируемых в BER-TLV
#7	L	‘NNh’ или ‘81 NNh’	L_{PV}: длина переданных данных. L равна 2 байтам, если L_{PV} > 127 байтов.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Простые данные, закодированные в BER-TLV, т.е. смещённый объект данных с меткой ‘54h’ || Дискретный объект данных с меткой ‘53h’, включающий в себя данные, подлежащие записи
#(7+L+NN)	1	‘8Eh’	T_{CC} : Метка, указывающая на криптографическую контрольную сумму
#(8+L+NN)	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Криптографическая контрольная сумма
Le	1	‘00h’	Как указано в стандарте ISO/IEC 7816-4

TCS_68 Ответное сообщение, если команда выполнена успешно

Байт	Длина	Значение	Описание
#1	1	‘99h’	T_{SW} : Метка, указывающая на характеристики статуса (должна быть защищена с помощью криптографической суммы)
#2	1	‘02h’	L_{SW}: длина переданных обратно характеристик статуса
#3-#4	2	‘XXXXh’	Статус обработки для незащищённого ответа APDU
#5	1	‘8Eh’	T_{CC} : Метка, указывающая на криптографическую контрольную сумму

#6	1	‘XXh’	L_{CC} : Длина следующей криптографической контрольной суммы ‘08h’, ‘0Ch’ или ‘10h’ в зависимости от длины ключа AES для защищённого обмена сообщениями (см. часть Б приложения 11)
#7-#(6+L)	L	‘XX..XXh’	Криптографическая контрольная сумма
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

3.5.4 GET CHALLENGE

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда GET CHALLENGE предлагает карточке выдать запрос для его использования в процедуре, связанной с защитой, которая предусматривает передачу карточке криптограммы или некоторых зашифрованных данных.

TCS_69 Challenge, выданный карточкой, действителен только для следующей команды, которая использует запрос, переданный карточке.

TCS_70 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (ожидаемая длина Challenge).

TCS_71 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#8	8	‘XX..XXh’	Запрос
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если Le отличается от ‘08h’, статус обработки выдаётся в виде **‘6700’.**
- Если параметры P1-P2 неправильны, статус обработки выдаётся в виде **‘6A86’.**

3.5.5 VERIFY

Данная команда соответствует стандарту ISO/IEC 7816-4, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Для поддержки этой команды требуется только карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду, но для таких карточек исходное значение CHV не персонализируется. Таким образом, такие карточки не могут успешно выполнять данную команду. В случае других типов карточек тахографов, кроме карточек мастерской, поведение, т.е. передаваемый обратно код ошибки, не попадает в область применения данной спецификации, если команда отправлена.

Команда Verify инициирует сравнение на уровне карточки между переданными данными CHV (PIN) и исходными данными CHV, записанными на карточке.

TCS_72 ПИН-код, введённый пользователем, должен быть закодирован в ASCI и заполнен IFD с правой стороны байтами ‘FFh’ до достижения длины 8 байтов; см. также тип данных WorkshopCardPIN в приложении 1.

TCS_73 Приложения тахографа первого и второго поколений используют одно и то же исходное значение CHV.

TCS_74 Карточка тахографа проверяет, правильно ли закодирована команда. Если команда закодирована неправильно, карточка не сравнивает значения CHV, не понижает показания счётчика оставшихся попыток CHV и не восстанавливает статус безопасности PIN_Verified, а отменяет команду. Команда закодирована правильно, если байтам CLA, INS, P1, P2, Lc присвоены конкретные значения, Le отсутствует, а поле командных данных имеет правильную длину.

TCS_75 Если команда проходит, счётчик оставшихся попыток CHV выставляется на исходное значение. Исходное значение счётчика оставшихся попыток CHV составляет 5. Если команда проходит, карточка передаёт внутренний статус безопасности PIN_Verified. Карточка сбрасывает этот статус безопасности, если её перезагрузили или если переданный в команду код CHV не соответствует сохранившемуся исходному значению CHV.

Примечание: Использование одного и того же исходного значения CHV и глобального статуса безопасности не позволяют работнику мастерской снова ввести ПИН-код после выбора другого приложения тахографа DF.

TCS_76 Сравнение, которое дало неправильные результаты, регистрируется на карточке, т.е. значение счётчика оставшихся попыток CHV понижается на единицу, с целью ограничить число дальнейших попыток использования исходных данных CHV.

TCS_77 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘20h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2 (проверенные данные CHV известны по косвенным признакам)
Lc	1	‘08h’	Длина переданного кода CHV
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если исходное значение CHV не найдено, статус обработки выдаётся в виде ‘**6A88**’.
- Если данные CHV заблокированы (счётчик оставшихся попыток CHV показывает ноль), статус обработки выдаётся в виде **‘6983’**. В этом состоянии данные CHV больше никогда не принимаются.
- Если сравнение дало неправильные результаты, показание счётчика оставшихся попыток уменьшается и статус обработки выдаётся в виде **‘63CX’** (X > 0 и X равен показанию счётчика оставшихся попыток CHV.
- Если исходное значение CHV считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’.**
- Если Lc отличается от ‘08h’, статус обработки выдаётся в виде **‘6700’.**

3.5.6 GET RESPONSE

Данная команда соответствует стандарту ISO/IEC 7816-4.

Данная команда (необходимая и доступная только для протокола T = 0) используется для передачи подготовленных данных с карточки на интерфейс (случай, когда команда включает в себя оба байта Lc и Le).

Команда GET_RESPONSE должна выдаваться сразу же после команды на подготовку данных, в противном случае данные потеряются. После выполнения команды GET RESPONSE (за исключением случаев ошибки '**61xx**' или '**6Cxx**', см. ниже) данные, подготовленные ранее, становятся недоступны.

TCS_79 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Число ожидаемых байтов

TCS_80 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#X	X	'XX..XXh'	Данные
SW	2	'XXXXh'	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт '**9000**'.
- Если данные карточкой подготовлены не были, статус обработки выдаётся в виде **'6900'** или **'6F00'**.
- Если Le превышает число имеющихся байтов или если Le равна нулю, статус обработки выдаётся в виде **'6Cxx'**, где xx указывает на точное число имеющихся байтов. В этом случае подготовленные данные всё ещё доступны для следующей команды GET RESPONSE.
- Если Le не равна нулю и меньше, чем число имеющихся байтов, требуемые данные нормально передаются карточкой, а статус обработки выдаётся в виде **'61xx'**, где 'xx' указывает число дополнительных байтов, всё ещё имеющихся для выполнения следующей команды GET RESPONSE.
- Если команда не поддерживается (протокол T=1), карточка выдает **'6D00'**.

3.5.7 PSO: VERIFY CERTIFICATE

Данная команда соответствует стандарту ISO/IEC 7816-8, однако её использование ограничено по сравнению с командой, определённой в указанном стандарте.

Команда VERIFY CERTIFICATE используется карточкой для получения открытого ключа извне и проверки его действительности.

3.5.7.1 Команда первого поколения – пара ответов

TCS_81 Данный вариант команды поддерживается только приложением тахографа первого поколения.

TCS_82 Если команда VERIFY CERTIFICATE проходит, открытый ключ записывается для будущего использования в среде защиты. Этот ключ прямо конфигурируется для использования команд, связанных с защитой (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE или VERIFY CERTIFICATE) с помощью команды MSE (см. пункт 3.5.11), использующей идентификатор этого ключа.

TCS_83 В любом случае команда VERIFY CERTIFICATE использует открытый ключ, ранее выбранный командой MSE для открытия сертификата. Этот открытый ключ должен быть ключом государства-члена или Европы.

TCS_84 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘00h’	P1
P2	1	‘AEh’	P2: закодированные данные к классу BER-TLV не относятся (конкатенация элементов данных)
Lc	1	‘C2h’	Lc : Длина сертификата, 194 байта
#6-#199	194	‘XX..XXh’	Сертификат: конкатенация элементов данных (как указано в приложении 11)

TCS_85 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если проверка сертификата не удалась, статус обработки выдаётся в виде **‘6688’**. Процесс проверки и расшифровки сертификата для первого и второго поколений описан в приложении 11.
- Если открытый ключ среды защиты отсутствует, выдается **‘6A88’.**
- Если выбранный открытый ключ (используемый для расшифровки сертификата) считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’.**
- Только для первого поколения: Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) отличается от '00' (т.е. не является ключом государства-члена или Европы), статус обработки выдаётся в виде **‘6985’.**

3.5.7.2 Команда второго поколения – пара ответов

В зависимости от размера кривой сертификаты ECC могут быть такими длинными, что их невозможно будет передать в одном APDU. В подобном случае должно применяться формирование цепочки команд в соответствии с ISO/IEC 7816-4, и сертификат передаётся двумя последовательными APDU PSO: Verify Certificate.

Структура сертификата и параметры области представлены в приложении 11.

TCS_86 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G2; также см. TCS_33.

TCS_87 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘X0h’	Байт CLA, указывающий на формирование цепочки команд: ‘00h’ единственная или последняя команда цепочки

			‘10h’ не последняя команда цепочки
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘00h’	
P2	1	‘BEh’	Проверка самодокументированного сертификата
Lc	1	‘XXh’	Длина поля командных данных; см. TCS_88 и TCS_89.
#6-#5+L	L	‘XX..XXh’	Данные, закодированные в DER-TLV: Объект данных сертифицирующего органа ECC как первый объект данных, конкатенированный с объектом данных подписи сертификата ECC как вторым объектом данных, или частью этой конкатенации. Метка '7F21' и соответствующая длина не передаются. Последовательность этих объектов данных фиксирована.

TCS_88 В отношении коротких APDU применяются следующие положения: IFD использует минимальное число APDU, требуемое для передачи команды, и передаёт максимальное число байтов в первой команде APDU в соответствии со значением байтов карточки размера информационного поля; см. TCS_14. Если IFD ведёт себя по-другому, поведение карточки в область применения не попадает.

TCS_89 В отношении APDU расширенной длины применяются следующие положения: Если сертификат не помещается в один APDU, карточка поддерживает формирование цепочек команд. IFD использует минимальное число APDU, требуемое для передачи команды, и передаёт максимальное число байтов в первой команде APDU. Если IFD ведёт себя по-другому, поведение карточки в область применения не попадает.

Примечание: В соответствии с приложением 11 карточка сохраняет сертификат или соответствующее содержание сертификата и обновляет его currentAuthenticatedTime.

Структура ответного сообщения и характеристики статуса представлены в TCS_85.

TCS_90 Помимо кодов ошибок, перечисленных в TCS_85, карточка может выдавать следующие коды ошибок:

- Если параметр выбранного открытого ключа (используемого для расшифровки сертификата) CHA.LSB (CertificateHolderAuthorisation.equipmentType), который не подходит для проверки сертификата соответствии с приложением 11, статус обработки выдаётся в виде ‘**6985**’.
- Если значение currentAuthenticatedTime карточки позднее, чем дата истечения срока действия сертификата, статус обработки выдаётся в виде ‘**6985**’.
- Если ожидается последняя команда цепочки, карточка выдаёт ‘**6883**’.
- Если в поле командных данных передаются неверные параметры, карточка выдаёт ‘**6A80**’ (как и в случае, когда объекты данных не передаются в определённом порядке).

3.5.8 INTERNAL AUTHENTICATE

Данная команда соответствует стандарту ISO/IEC 7816-4.

TCS_91 Данную команду поддерживают все карточки тахографов в DF Tachograph первого поколения. Команда может быть доступной или недоступной в MF и/или DF Tachograph_G2. Если она доступна, она прерывается при помощи подходящего кода ошибки, так как закрытый ключ карточки (Card.SK) для протокола аутентификации первого поколения доступен только в DF_Tachograph первого поколения.

Используя команду INTERNAL AUTHENTICATE, IFD может произвести аутентификацию карточки. Процесс аутентификации описывается в приложении 11. Он включает в себя следующие сообщения:

TCS_92 Команда INTERNAL AUTHENTICATE использует закрытый ключ карточки (выбранный по косвенным признакам) для подтверждения данных аутентификации, включая K1 (первый элемент, указывающий на соответствие ключа сеанса) и RND1, и использует открытый ключ, выбранный в данный момент (на основании последней команды MSE) для шифрования подписи и создания маркера аутентификации (более подробно см. в приложении 11).

TCS_93 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Длина данных, переданных на карточку
#6 - #13	8	‘XX..XXh’	Запрос, использованный для аутентификации карточки
#14 -#21	8	‘XX..XXh’	VU.CHR (см. приложение 11)
Le	1	‘80h’	Длина данных, ожидаемых с карточки

TCS_94 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#128	128	‘XX..XXh’	Маркер аутентификации карточки (см. приложение 11)
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если открытый ключ среды защиты отсутствует, статус обработки выдаётся в виде **‘6A88’.**
- Если закрытый ключ среды защиты отсутствует, статус обработки выдаётся в виде **‘6A88’.**
- Если VU.CHR не соответствует данному идентификатору открытого ключа, статус обработки выдаётся в виде **‘6A88’.**
- Если выбранный закрытый ключ считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’**.

TCS_95 Если команда INTERNAL AUTHENTICATE проходит, ключ текущего сеанса, если он существует, стирается и более не доступен. Для создания нового ключа сеанса должна быть успешно выполнена команда EXTERNAL AUTHENTICATE для механизма аутентификации первого поколения.

3.5.9 EXTERNAL AUTHENTICATE

Данная команда соответствует стандарту ISO/IEC 7816-4.

Используя команду EXTERNAL AUTHENTICATE, карточка может произвести аутентификацию IFD. Процесс аутентификации описывается в приложении 11 для тахографов первого и второго поколений (аутентификация БУ).

TCS_96 Вариант команды для механизма взаимной аутентификации первого поколения поддерживается только приложением тахографа первого поколения.

TCS_97 Вариант команды для взаимной аутентификации БУ и карточки второго поколения может выполняться в MF, DF Tachograph и DF Tachograph_G2; также см. TCS_34.

TCS_98 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘82h’	INS
P1	1	‘00h’	Косвенно известные ключи и алгоритмы
P2	1	‘00h’	
Lc	1	‘XXh’	Lc (Длина данных, переданных на карточку)
#6-#(5+L)	L	‘XX..XXh’	Аутентификация для первого поколения: Криптограмма (см. часть А приложения 11) Аутентификация для второго поколения: Подпись, которую генерирует IFD (см. часть Б приложения 11)

TCS_99 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если CHA выбранного открытого ключа не соответствует конкатенации AID приложения тахографа и типа БУ, статус обработки выдаётся в виде **‘6F00’.**
- Если этой команде не предшествует непосредственно команда GET CHALLENGE, статус обработки выдаётся в виде **‘6985’.**

Приложение тахографа первого поколения может выдавать следующие дополнительные коды ошибок:

- Если открытый ключ среды защиты отсутствует, выдаётся **‘6A88’.**
- Если закрытый ключ среды защиты отсутствует, статус обработки выдаётся в виде **‘6A88’.**
- Если проверка криптограммы показала неправильный результат, статус обработки выдаётся в виде **‘6688’.**
- Если выбранный закрытый ключ считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’.**

Вариант команды для аутентификации для второго поколения может выдать следующий дополнительный код ошибки:

- Если проверка подписи не удалась, карточка выдаёт **‘6300’.**

3.5.10 GENERAL AUTHENTICATE

Данная команда используется для протокола аутентификации микросхемы второго поколения, как указано в части Б приложения 11, и соответствует ISO/IEC 7816-4.

TCS_100 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G2; также см. TCS_34.

TCS_101 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘86h’	
P1	1	‘00h’	Косвенно известные ключи и протокол
P2	1	‘00h’	
Lc	1	‘NNh’	Lc: длина последующего поля данных
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} + ‘XX..XXh’	Динамическое значение открытого ключа, закодированного в DER-TLV (см. приложение 11) БУ передаёт объекты данных в этом порядке.

TCS_102 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#L	L	‘7Ch’ + L_{7C} + ‘81h’ + ‘08h’ + ‘XX..XXh’ + ‘82h’ + L_{82} + ‘XX..XXh’	Данные динамической аутентификации, закодированные в DER-TLV: временное значение и маркер аутентификации (см. приложение 11)
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Карточка выдаёт ‘**6A80**’, чтобы указать на неверные параметры в поле данных.
- Карточка выдаёт ‘**6982**’, если команду External Authenticate не удалось выполнить успешно.

Ответ объекта данных динамической аутентификации ‘7Ch’

- должен выдаваться, если операция выполнена успешно, т.е. характеристика статуса – ‘**9000**’,
- должен отсутствовать в случае ошибки выполнения или проверки, т.е. характеристики статуса находятся в интервале ‘**6400**’ – ‘**6FFF**’, и
- может отсутствовать в случае предупреждения, т.е. характеристики статуса находятся в интервале ‘**6200**’ – ‘**63FF**’.

3.5.11 MANAGE SECURITY ENVIRONMENT

Данная команда используется для определения открытого ключа в целях аутентификации.

3.5.11.1 Команда первого поколения – пара ответов

Данная команда соответствует стандарту ISO/IEC 7816-4. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_103 Данная команда поддерживается только приложением тахографа первого поколения.

TCS_104 Ключ, указанный в поле данных MSE, продолжает оставаться действующим открытым ключом до следующей правильной команды MSE, выбора DF или перезагрузки карточки.

TCS_105 Если указанный ключ (пока) отсутствует на карточке, среда защиты остаётся без изменений.

TCS_106 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘22h’	INS
P1	1	‘C1h’	P1: исходный ключ, действительный для всех криптографических операций
P2	1	‘B6h’	P2 (исходные данные, касающиеся цифровой подписи)
Lc	1	‘0Ah’	Lc: длина последующего поля данных
#6	1	‘83h’	Метка, указывающая на открытый ключ в асимметричных случаях
#7	1	‘08h’	Длина исходных данных ключа (идентификатор ключа)
#8-#15	8	‘XX..XXh’	Идентификатор ключа, указанный в приложении 11

TCS_107 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если указанный ключ на карточке отсутствует, статус обработки выдаётся в виде ‘**6A88**’.
- Если некоторые ожидаемые объекты данных в формате защищённого обмена сообщениями отсутствуют, статус обработки выдается в виде **‘6987’**. Это может произойти, если отсутствует метка ‘83h’.
- Если некоторые объекты данных неверны, статус обработки выдаётся в виде **‘6988’**. Это может произойти в том случае, если длина идентификатора ключа не соответствует ‘08h’.
- Если выбранный ключ считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’**.

3.5.11.2 Команда второго поколения – пары ответов

Для аутентификация для второго поколения карточки тахографа поддерживает следующую команду MSE: Установленные версии команды, соответствующие стандарту ISO/IEC 7816-4. Данные версии команды не поддерживаются для аутентификации для первого поколения.

3.5.11.2.1 MSE:SET AT для аутентификации микросхемы

Следующая команда MSE:SET AT используется для выбора параметров аутентификации микросхемы, проводимой при помощи следующей команды General Authenticate.

TCS_108 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G2; также см. TCS_34.

TCS_109 **Командное сообщение MSE:SET AT для аутентификации микросхемы**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘41h’	Установлено для внутренней аутентификации
P2	1	‘A4h’	Аутентификация
Lc	1	‘NNh’	Lc: длина последующего поля данных

#6-#(5+L)	L	’80h’ + ‘0Ah’ + ‘XX..XXh’	Указанный криптографический механизм, закодированный в DER-TLV: Идентификатор объекта аутентификации микросхемы (только значение, метка ‘06h’ опускается). Значения идентификаторов объектов см. в приложении 1; применяется нотация байтов. По вопросу, как выбирать один из этих идентификаторов объектов, см. приложение 11.

3.5.11.2.2 MSE:SET AT для аутентификации БУ

Следующая команда MSE:SET AT используется для выбора параметров и ключей аутентификации БУ, проводимой при помощи следующей команды External Authenticate.

TCS_110 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G2; также см. TCS_34.

TCS_111 **Командное сообщение MSE:SET AT для аутентификации БУ**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Установлено для внешней аутентификации
P2	1	‘A4h’	Аутентификация
Lc	1	‘NNh’	Lc: длина последующего поля данных
#6-#(5+L)	L	’80h’ + ‘0Ah’ + ‘XX..XXh’	Указанный криптографический механизм, закодированный в DER-TLV: Идентификатор объекта аутентификации БУ (только значение, метка ‘06h’ опускается). Значения идентификаторов объектов см. в приложении 1; применяется нотация байтов. По вопросу, как выбирать один из этих идентификаторов объектов, см. приложение 11.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Указание на открытый ключ БУ, закодированное в DER-TLV, в рамках указания держателя сертификата, упомянутого в сертификате.
		‘91h’ + L_{91} + ‘XX..XXh’	Компактное выражение динамического открытого ключа БУ, закодированное в DER-TLV, которое будет использоваться для аутентификации микросхемы (см. приложение 11)

3.5.11.2.3 MSE:SET DST

Следующая команда MSE:SET DST используется для установления открытого ключа

- для проверки подписи при помощи последующей команды PSO: Verify Digital Signature или
- для проверки подписи сертификата при помощи последующей команды PSO: Verify Certificate

TCS_112 Команда может выполняться в MF, DF Tachograph и DF Tachograph_G2; также см. TCS_33.

TCS_113 **Командное сообщение MSE:SET DST**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Установлено для проверки
P2	1	‘B6h’	Цифровая подпись
Lc	1	‘NNh’	Lc: длина последующего поля данных
#6-#(5+L)	L	’83h’ + ‘08h’ + ‘XX...XXh’	Указание на открытый ключ, закодированное в DER-TLV, т.е. указание держателя сертификата в сертификате открытого ключа (см. приложение 11)

Для всех версий команды структура ответного сообщения и характеристики статуса задаются следующим образом:

TCS_114 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’. Протокол выбран и активирован.
- **‘6A80’** указывает на неверные параметры в поле данных команды.
- **‘6A88’** указывает на то, что указанные данные (т.е. указанный ключ) не доступны.

3.5.12 PSO: HASH

Данная команда используется для передачи карточке результата расчёта хеширования некоторых данных. Она используется для проверки цифровых подписей. Значение хэша временно хранится для последующей команды PSO: Verify Digital Signature

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.
Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только контрольная карточка.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. Команда может быть доступной или недоступной в MF.

Приложение контрольной карточки первого поколения поддерживает только SHA-1.

TCS_115 Временно хранящееся значение хеширования удаляется, если при помощи команды PSO: HASH вычисляется новое значение хеширования, если выбран DF и если произведена перезагрузка карточки тахографа.

TCS_116 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘90h’	Возврат хеш-кода
P2	1	‘A0h’	Метка: поле данных содержит объекты данных, относящиеся к хешированию
Lc	1	‘XXh’	Длина Lc последующего поля данных
#6	1	‘90h’	Метка для хеш-кода
#7	1	‘XXh’	Длина L хеш-кода: ‘14h’ для приложения первого поколения (см. часть A приложения 11) ‘20h’, ‘30h’ или ‘40h’ для приложения второго поколения (см. часть Б приложения 11)
#8-#(7+L)	L	‘XX..XXh’	Хеш-код

TCS_117 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, статус обработки выдаётся в виде **‘6987’**. Это может произойти, если отсутствует одна из меток ‘90h’.
- Если некоторые объекты данных неверны, статус обработки выдаётся в виде **‘6988’**. Данная ошибка возникает, если требуемая метка присутствует, но её длина отличается от ‘14h’ в случае SHA-1, от ‘20h’ в случае SHA-256, от ‘30h’ в случае SHA-384, от ‘40h’ в случае SHA-512 (приложение второго поколения).

3.5.13 PERFORM HASH of FILE

Данная команда не соответствует стандарту ISO/IEC 7816-8. Поэтому байт CLA этой команды указывает на собственное использование команды PERFORM SECURITY OPERATION / HASH.

Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только карточка водителя и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. Если карточка предприятия или контрольная карточка выполняют данную команду, она выполняется, как указано в настоящей главе.

Команда может быть доступной или недоступной в MF. Если она доступна, команда выполняется так, как указано в настоящей главе, т.е. не позволяет вычислять значение хеширования и прерывается на основании подходящего кода ошибки.

TCS_118 Команда PERFORM HASH FILE используется для хеширования зоны данных выбранного в данный момент транспарентного EF.

TCS_119 Карточка тахографа поддерживает данную команду только для EF, перечисленных в главе 4 в DF_Tachograph и DF_Tachograph_G2 с учётом следующего исключения. Карточка тахографа не поддерживает команду для EF Sensor_Installation_Data в DF Tachograph_G2..

TCS_120 Результат операции хеширования временно хранится на карточке. Он может затем использоваться для получения цифровой подписи файла с использованием команды PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Временно хранящееся значение хеширования удаляется, если при помощи команды PSO: HASH FILE вычисляется новое значение хеширования, если выбран DF и если произведена перезагрузка карточки тахографа.

TCS_122 Приложение тахографа первого поколения поддерживает SHA-1.

TCS_123 Приложение тахографа второго поколения поддерживает SHA-1 и SHA-2 (256, 384 и 512 бит).

TCS_124 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘90h’	Метка: Хеш
P2	1	‘XXh’	P2: Указывает на алгоритм, используемый для хеширования данных выбранного в данный момент транспарентного файла: ‘00h’ для SHA-1 ‘01h’ для SHA-256 ‘02h’ для SHA-384 ‘03h’ для SHA-512

TCS_125 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если текущий EF не позволяет выполнять такую команду (EF Sensor_Installation_Data в DF Tachograph_G2), статус обработки выдаётся в виде **’6985’.**
- Если выбранный EF считается повреждённым (в атрибутах файла или хранящихся данных обнаружены ошибки целостности), статус обработки выдаётся в виде ‘**6400**’ или ‘**6581**’.
- Если выбранный файл не является транспарентным файлом или нет текущего EF, статус обработки выдаётся в виде ‘**6986**’.

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

Данная команда используется для расчёта цифровой подписи ранее рассчитанного хеш-кода (см. PERFORM HASH of FILE, пункт 3.5.13).

Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только карточка водителя и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду, но для них нет ключа подписи. Таким образом, такие карточки не могут успешно выполнять эту команду и прерывают её на основании подходящего кода ошибки.

Команда может быть доступной или недоступной в MF. Если она доступна, она прерывается при помощи подходящего кода ошибки.

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

TCS_126 Данная команда не вычисляет цифровую подпись ранее рассчитанного хеш-кода по команде PSO: HASH.

TCS_127 Закрытый ключ карточки используется для расчёта цифровой подписи и известен карточке по косвенным признакам.

TCS_128 Приложение тахографа первого поколения производит цифровую подпись с использованием метода заполнения, соответствующего PKCS1 (более подробно см. приложение 11).

TCS_129 Приложение тахографа второго поколения рассчитывает цифровую подпись на основе эллиптической кривой (более подробно см. приложение 11).

TCS_130 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘9Eh’	Цифровая подпись, подлежащая возврату
P2	1	‘9Ah’	Метка: поле данных содержит данные, требующие подписи. Если поле данных не включено, то предполагается, что эти данные уже записаны на карточке (хеширование файла)
Le	1	‘NNh’	Длина ожидаемой подписи

TCS_131 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#L	L	‘XX..XXh’	Подпись ранее рассчитанного хеширования
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если косвенно выбранный закрытый ключ считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’.**
- Если хеш, рассчитанный в рамках предыдущей команды Perform Hash of File, статус обработки выдаётся в виде **‘6985’.**

3.5.15 PSO: VERIFY DIGITAL SIGNATURE

Данная команда используется для проверки цифровой подписи, представленной в качестве входных данных, хеш-код которых карточке известен. Алгоритм подписи известен карточке по косвенным признакам.

Данная команда соответствует стандарту ISO/IEC 7816-8. Использование этой команды по сравнению с указанным стандартом ограничено.

Для поддержки данной команды в DF Tachograph и DF Tachograph_G2 требуется только контрольная карточка.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду. Команда может быть доступной или недоступной в MF.

TCS_132 Команда VERIFY DIGITAL SIGNATURE всегда использует открытый ключ, выбранный на основании предыдущей команды Manage Security Environment MSE: Set DST, а предыдущий хеш-код вносится командой PSO: HASH.

TCS_133 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘00h’	
P2	1	‘A8h’	Метка: поле данных содержит объекты данных, относящиеся к проверке
Lc	1	‘83h’	Длина Lc последующего поля данных
6	1	‘9Eh’	Метка, указывающая на цифровую подпись
#7-#8	2	‘81 XXh’	Длина цифровой подписи: 128 байтов, закодированные в соответствии с частью A приложения 11 для приложения тахографа первого поколения В зависимости от выбранной кривой для приложения тахографа второго поколения (см. часть Б приложения 11)
#9-#(8+L)	L	‘XX..XXh’	Содержание цифровой подписи

TCS_134 **Ответное сообщение**

Байт	Длина	Значение	Описание
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- Если проверка подписи показала неправильный результат, статус обработки выдаётся в виде **‘6688’.** Процесс проверки описывается в приложении 11.
- Если открытый ключ не выбран, статус обработки выдаётся в виде **‘6A88’.**
- Если некоторые ожидаемые объекты данных (как указано выше) отсутствуют, статус обработки выдаётся в виде **‘6987’**. Это может произойти, если отсутствует одна из требуемых меток.
- Если хеш-кода для обработки команды нет (в результате предыдущей команды PSO: Hash), статус обработки выдаётся в виде **‘6985’.**
- Если некоторые объекты данных неверны, статус обработки выдаётся в виде **‘6988’**. Это может произойти, если длина одного из требуемых объектов данных неверна.
- Если выбранный открытый ключ считается повреждённым, статус обработки выдаётся в виде **‘6400’** или **‘6581’.**

3.5.16 PROCESS DSRC MESSAGE

Данная команда используется для проверки целостности и подлинности сообщения DSRC и для расшифровки данных, передаваемых БУ контрольному органу или мастерской через соединение DSRC. Карточка генерирует ключ шифрования и ключ MAC, используемые для защиты сообщения DSRC, как описано в приложении, часть Б, глава 13.

Для поддержки данной команды в DF Tachograph_G2 требуется только контрольная карточка и карточка мастерской.

Другие типы карточек тахографов могут поддерживать или не поддерживать данную команду, но для них нет главного ключа DSRC. Таким образом, такие карточки не могут успешно выполнять эту команду и прерывают её на основании подходящего кода ошибки.

Команда может быть доступной или недоступной в MF и/или DF Tachograph. Если она доступна, она прерывается при помощи подходящего кода ошибки.

TCS_135 Главный ключ DSRC доступен только в DF Tachograph_G2, т.е. контрольная карточка и карточка мастерской поддерживают успешное выполнение команды только в DF Tachograph_G2.

TCS_136 Команда расшифровывает только данные DSRC и проверяет криптографическую контрольную сумму, но не интерпретирует входные данные.

TCS_137 Порядок объектов данных в поле данных команды фиксируется в соответствии с настоящей спецификацией.

TCS_138 **Командное сообщение**

Байт	Длина	Значение	Описание
CLA	1	‘80h’	Собственный CLA
INS	1	‘2Ah’	Выполнение операции обеспечения безопасности
P1	1	‘80h’	Ответные данные: простое значение
P2	1	‘B0h’	Командные данные: простое значение, закодированное в BER-TLV и включающее в себя объекты данных SM
Lc	1	‘NNh’	Длина Lc последующего поля данных
#6-#(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	Байт показателя заполненного содержания, закодированный в DER-TLV, с последующими зашифрованными данными тахографа. Для байта показателя заполненного содержания используется значение ‘00h’ (в соответствии с таблицей 52 стандарта ISO/IEC 7816-4:2013 «дополнительно не указывается»). По вопросу механизма шифрования см. приложение 11, часть Б, глава 13. Допустимые значения длины L_{87} являются кратными длине блока AES плюс 1 с учётом байта показателя заполненного содержания, т.е. с 17 байтов и выше и включая 193 байтов. Примечание: См. таблицу 49 стандарта ISO/IEC 7816-4:2013 по поводу объекта данных SM с меткой ‘87h’.
		‘81h’ + ‘10h’	Шаблон управляющих ссылок конфиденциальности, закодированный в DER-TLV, в котором хранится конкатенация следующих элементов данных (см. приложение 1, DSRCSecurityData и приложение 11, часть Б, глава 13): • отметка времени 4 байта • счётчик 3 байта • серийный номер БУ 8 байтов • версия главного ключа DSRC 1 байт Примечание: См. таблицу 49 стандарта ISO/IEC 7816-4:2013 по поводу объекта данных SM с меткой ‘81h’.
		‘8Eh’ + L_{8E} +	MAC, закодированный в DER-TLV, в рамках сообщения

		‘XX..XXh’	DSRC. По вопросу алгоритма и расчёта MAC см. приложение 11, часть Б, глава 13. Примечание: См. таблицу 49 стандарта ISO/IEC 7816-4:2013 по поводу объекта данных SM с меткой ‘8Eh’.

TCS_139 **Ответное сообщение**

Байт	Длина	Значение	Описание
#1-#L	L	‘XX..XXh’	Данные отсутствуют (в случае ошибки) или расшифрованы (без заполнения)
SW	2	‘XXXXh’	Характеристики статуса (SW1,SW2)

- Если команда проходит успешно, карточка выдаёт ‘**9000**’.
- **‘6A80’** указывает на то, что в поле данных команды содержатся неверные параметры (как и в случае, когда объекты данных не передаются в определённом порядке).
- **‘6A88’** указывает на то, что указанные данные отсутствуют, т.е. указанный главный ключ DSRC не доступен.
- **‘6900’** указывает на то, что проверка криптографической контрольной суммы или расшифровка данных дали неверный результат.

4. Структура карточек тахографов

В настоящем пункте уточняются структуры файлов карточек тахографа для хранения доступных данных.

В нём не указываются внутренние структуры, определяемые по усмотрению производителя, такие как заголовки файлов, а также элементы хранения и обработки данных, необходимые только для внутреннего пользования, например, `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` или `WorkshopCardPin`.

TCS_140 Карточка тахографа второго поколения хранит главный файл MF и приложение тахографа первого и второго поколений одного и того же типа (например, приложения карточки водителя).

TCS_141 Карточка тахографа поддерживает хотя бы минимальное число записей, указанное для соответствующих приложений, и не поддерживает число записей, превышающее максимальное число записей, указанное для соответствующих приложений.

Максимальное и минимальное числа записей в настоящей главе указываются для различных приложений.
Относительно условий безопасности, применяемых в правилах доступа во всей настоящей главе, см. главу 3.3. В целом, режим доступа Read обозначает команду READ BINARY с чётным и, если поддерживается, нечётным байтом INS, за исключением EF Sensor_Installation_Data на карточке мастерской; см. TCS_156 и TCS_160. Режим доступа Update обозначает команду Update Binary с чётным и, если поддерживается, нечётным байтом INS, а режим доступа Select – команду SELECT.

4.1. Главный файл MF

TCS_142 После персонализации главный файл MF имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

			Правила доступа	
Файл	**ИД файла**	**SFID**	**Read / Select**	**Update**
MF	‘3F00h’			
├─EF ICC	‘0002h’		ALW	NEV
├─EF IC	‘0005h’		ALW	NEV
├─EF DIR	‘2F00h’	30	ALW	NEV
├─EF ATR/INFO (условно)	‘2F01h’	29	ALW	NEV
├─EF Extended_Length (условно)	‘0006h’	28	ALW	NEV
├─DF Tachograph	‘0500h’		SC1	
└─DF Tachograph_G2			SC1	

В настоящей таблице для условия безопасности используется следующее сокращение:
SC1 ALW OR SM-MAC-G2

TCS_143 Все структуры EF транспарентны.

TCS_144 Главный файл MF имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
MF		*63*	*184*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	

├─icSerialNumber	4	4	{00..00}
└─icManufacturingReferences	4	4	{00..00}

EF DIR	*20*	*20*	
См. TCS_145	*20*	*20*	{00..00}
EF ATR/INFO	*7*	*128*	
См. TCS_146	*7*	*128*	{00..00}
EF EXTENDED_LENGTH	*3*	*3*	
См. TCS_147	*3*	*3*	{00..00}
DF Tachograph			
DF Tachograph_G2			

TCS_145 Элементарный файл EF DIR содержи следующие объекты данных, связанные с приложением: ’61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 Элементарный файл EF ATR/INFO присутствует, если карточка тахографа в своей ATR указывает, что поддерживает поля расширенной длины. В данном случае EF ATR/INFO содержит объект данных информации расширенной длины (DO’7F66’), как указано в стандарте ISO/IEC 7816-4:2013, положение 12.7.1.

TCS_147 Элементарный файл EF Extended_Length присутствует, если карточка тахографа в своей ATR указывает, что поддерживает поля расширенной длины. В данном случае EF содержит следующий объект данных: ’02 01 xx’, где значение ‘xx’ показывает, поддерживаются ли поля расширенной длины для протокола T = 1 и/или T = 0.
Значение ‘01’ указывает, что поле расширенной длины поддерживается для протокола T = 1.
Значение ‘10’ указывает, что поле расширенной длины поддерживается для протокола T = 0.
Значение ‘11’ указывает, что поле расширенной длины поддерживается для протоколов T = 1 и T = 0.

4.2. Приложения карточки водителя

4.2.1 Приложение карточки водителя первого поколения

TCS_148 После персонализации приложение карточки водителя первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

		Правила доступа		
Файл	**ИД файла**	**Read**	**Select**	**Update**
DF Tachograph	‘0500h’		SC1	
EF Application_Identification	‘0501h’	SC2	SC1	NEV
EF Card_Certificate	‘C100h’	SC2	SC1	NEV
EF CA_Certificate	‘C108h’	SC2	SC1	NEV
EF Identification	‘0520h’	SC2	SC1	NEV
EF Card_Download	‘050Eh’	SC2	SC1	SC1
EF Driving_Licence_Info	‘0521h’	SC2	SC1	NEV
EF Events_Data	‘0502h’	SC2	SC1	SC3
EF Faults_Data	‘0503h’	SC2	SC1	SC3
EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
EF Places	‘0506h’	SC2	SC1	SC3
EF Current_Usage	‘0507h’	SC2	SC1	SC3
EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW OR SM-MAC-G2
SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2
SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Все структуры EF транспарентны.

TCS_150 Приложение карточки водителя первого поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}

EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}

EF Vehicles_Used		*2606*	*6202*	
└CardVehiclesUsed		*2606*	*6202*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*2604*	*6200*	
└cardVehicleRecords	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
└CardPlaceDailyWorkPeriod		*841*	*1121*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*840*	*1120*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
└SpecificConditionRecord	56	*5*	*5*	
├entryTime		4	4	{00..00}
└SpecificConditionType		1	1	{00}

TCS_151 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки водителя в приложении первого поколения:

		Мин.	**Макс.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5544 байтов (28 дней * 93 изменений вида	13776 байтов (28 дней * 240 изменений вида

		деятельности)	деятельности)

4.2.2 Приложение карточки водителя второго поколения

TCS_152 После персонализации приложение карточки водителя второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

			Правила доступа	
Файл	**ИД файла**	**SFID**	**Read / Select**	**Update**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	‘0501h’	1	SC1	NEV
├─EF CardMA_Certificate	‘C100h’	2	SC1	NEV
├─EF CardSignCertificate	‘C101h’	3	SC1	NEV
├─EF CA_Certificate	‘C108h’	4	SC1	NEV
├─EF Link_Certificate	‘C109h’	5	SC1	NEV
├─EF Identification	‘0520h’	6	SC1	NEV
├─EF Card_Download	‘050Eh’	7	SC1	SC1
├─EF Driving_Licence_Info	‘0521h’	10	SC1	NEV
├─EF Events_Data	‘0502h’	12	SC1	SM-MAC-G2
├─EF Faults_Data	‘0503h’	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	‘0504h’	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	‘0505h’	15	SC1	SM-MAC-G2
├─EF Places	‘0506h’	16	SC1	SM-MAC-G2
├─EF Current_Usage	‘0507h’	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	‘0508h’	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	‘0522h’	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	‘0523h’	20	SC1	SM-MAC-G2
└─EF GNSS_Places	‘0524h’	21	SC1	SM-MAC-G2

В настоящей таблице для условия безопасности используется следующее сокращение:
SC1 ALW OR SM-MAC-G2

TCS_153 Все структуры EF транспарентны.

TCS_154 Приложение карточки водителя второго поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
└DF Tachograph_G2		*19510*	*39306*	
═EF Application_Identification		*15*	*15*	
└DriverCardApplicationIdentification		*15*	*15*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
├noOfEventsPerType		1	1	{00}
├noOfFaultsPerType		1	1	{00}
├activityStructureLength		2	2	{00 00}
├noOfCardVehicleRecords		2	2	{00 00}
├noOfCardPlaceRecords		2	2	{00}
├noOfGNSSCDRecords		2	2	{00 00}
└noOfSpecificConditionRecords		2	2	{00}
═EF CardMA_Certificate		*204*	*341*	
└CardMACertificate		204	341	{00..00}
═EF CardSignCertificate		*204*	*341*	
└CardSignCertificate		204	341	{00..00}
═EF CA_Certificate		*204*	*341*	
└MemberStateCertificate		204	341	{00..00}
═EF Link_Certificate		*204*	*341*	
└LinkCertificate		204	341	{00..00}

EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
└CardVehiclesUsed		*4034*	*9602*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*4032*	*9600*	
└cardVehicleRecords	n_3	*48*	*48*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├vuDataBlockCounter		2	2	{00 00}
└vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*1764*	*2352*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки водителя в приложении второго поколения:

		Мин.	**Макс.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5544 байтов (28 дней * 93 изменений вида деятельности)	13776 байтов (28 дней * 240 изменений вида деятельности)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. Приложения карточки мастерской

4.3.1 Приложение карточки мастерской первого поколения

TCS_156 После персонализации приложение карточки мастерской первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

		Правила доступа		
Файл	**ИД файла**	**Read**	**Select**	**Update**
└DF Tachograph	‘0500h’		SC1	
├EF Application_Identification	‘0501h’	SC2	SC1	NEV
├EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├EF Identification	‘0520h’	SC2	SC1	NEV
├EF Card_Download	‘0509h’	SC2	SC1	**SC1**
├EF Calibration	‘050Ah’	SC2	SC1	SC3
├EF Sensor_Installation_Data	‘050Bh’	**SC4**	SC1	NEV
├EF Events_Data	‘0502h’	SC2	SC1	SC3
├EF Faults_Data	‘0503h’	SC2	SC1	SC3
├EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├EF Places	‘0506h’	SC2	SC1	SC3
├EF Current_Usage	‘0507h’	SC2	SC1	SC3
├EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Для команды READ BINARY с чётным байтом INS:
(PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR (SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)
Для команды READ BINARY с нечётным байтом INS (если поддерживается): NEV

TCS_157 Все структуры EF транспарентны.

TCS_158 Приложение карточки мастерской первого поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
└DF Tachograph		*11055*	*29028*	
├EF Application_Identification		*11*	*11*	
└WorkshopCardApplicationIdentification		*11*	*11*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
├noOfEventsPerType		1	1	{00}
├noOfFaultsPerType		1	1	{00}
├activityStructureLength		2	2	{00 00}
├noOfCardVehicleRecords		2	2	{00 00}
├noOfCardPlaceRecords		1	1	{00}
└noOfCalibrationRecords		1	1	{00}
├EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}

EF Identification	*211*	*211*	
CardIdentification	65	65	
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
cardIssuingAuthorityName	36	36	{00, 20..20}
cardIssueDate	4	4	{00..00}
cardValidityBegin	4	4	{00..00}
cardExpiryDate	4	4	{00..00}
WorkshopCardHolderIdentification	*146*	*146*	
workshopName	36	36	{00, 20..20}
workshopAddress	36	36	{00, 20..20}
cardHolderName			
holderSurname	36	36	{00, 20..20}
holderFirstNames	36	36	{00, 20..20}
cardHolderPreferredLanguage	2	2	{20 20}
EF Card_Download	*2*	*2*	
NoOfCalibrationsSinceDownload	2	2	{00 00}
EF Calibration	*9243*	*26778*	
WorkshopCardCalibrationData	*9243*	*26778*	
calibrationTotalNumber	2	2	{00 00}
calibrationPointerNewestRecord	1	1	{00}
calibrationRecords	*9240*	*26775*	
WorkshopCardCalibrationRecord n_5	*105*	*105*	
calibrationPurpose	1	1	{00}
vehicleIdentificationNumber	17	17	{20..20}
vehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
wVehicleCharacteristicConstan	2	2	{00 00}
kConstantOfRecordingEquipment	2	2	{00 00}
lTyreCircumference	2	2	{00 00}
tyreSize	15	15	{20..20}
authorisedSpeed	1	1	{00}
oldOdometerValue	3	3	{00..00}
newOdometerValue	3	3	{00..00}
oldTimeValue	4	4	{00..00}
newTimeValue	4	4	{00..00}
nextCalibrationDate	4	4	{00..00}
vuPartNumber	16	16	{20..20}
vuSerialNumber	8	8	{00..00}
sensorSerialNumber	8	8	{00..00}
EF Sensor_Installation_Data	*16*	*16*	
SensorInstallationSecData	16	16	{00..00}

EF Events_Data		*432*	*432*	
└CardEventData		*432*	*432*	
└cardEventRecords	6	*72*	*72*	
└CardEventRecord	n_1	*24*	*24*	
├eventType		1	1	{00}
├eventBeginTime		4	4	{00..00}
├eventEndTime		4	4	{00..00}
└eventVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└CardFaultData		*288*	*288*	
└cardFaultRecords	2	*144*	*144*	
└CardFaultRecord	n_2	*24*	*24*	
├faultType		1	1	{00}
├faultBeginTime		4	4	{00..00}
├faultEndTime		4	4	{00..00}
└faultVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└CardDriverActivity		*202*	*496*	
├activityPointerOldestDayRecord		2	2	{00 00}
├activityPointerNewestRecord		2	2	{00 00}
└activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
└CardVehiclesUsed		*126*	*250*	
├vehiclePointerNewestRecord		2	2	{00 00}
└cardVehicleRecords		*124*	*248*	
└cardVehicleRecords	n_3	*31*	*31*	
├vehicleOdometerBegin		3	3	{00..00}
├vehicleOdometerEnd		3	3	{00..00}
├vehicleFirstUse		4	4	{00..00}
├vehicleLastUse		4	4	{00..00}
├vehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
└vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
└CardPlaceDailyWorkPeriod		*61*	*81*	
├placePointerNewestRecord		1	1	{00}
└placeRecords		*60*	*80*	
└PlaceRecord	n_4	*10*	*10*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
└vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	*2*	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки мастерской в приложении первого поколения:

		Мин.	**Макс.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 байтов (1 день * 93 изменения вида деятельности)	492 байта (1 день * 240 изменений вида деятельности)

4.3.2 Приложение карточки мастерской второго поколения

TCS_160 После персонализации приложение карточки мастерской второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

			Правила доступа		
Файл	**ИД файла**	**SFID**	**Read**	**Select**	**Update**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	‘0501h’	1	SC1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	SC1	NEV
EF CardSignCertificate	‘C101h’	3	SC1	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	SC1	NEV
EF Identification	‘0520h’	6	SC1	SC1	NEV
EF Card_Download	‘0509h’	7	SC1	SC1	SC1
EF Calibration	‘050Ah’	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	‘050Bh’	11	**SC5**	SM-MAC-G2	NEV
EF Events_Data	‘0502h’	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	‘0503h’	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	‘0504h’	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	‘0505h’	15	SC1	SC1	SM-MAC-G2
EF Places	‘0506h’	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	‘0507h’	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	‘0508h’	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	‘0522h’	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	‘0523h’	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	‘0524h’	21	SC1	SC1	SM-MAC-G2

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW OR SM-MAC-G2

SC5 Для команды Read Binary с чётным байтом INS: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2
Для команды Read Binary с нечётным байтом INS (если поддерживается): NEV

TCS_161 Все структуры EF транспарентны.

TCS_162 Приложение карточки мастерской второго поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}

EF CA_Certificate	*204*	*341*	
MemberStateCertificate	204	341	{00..00}
EF Link_Certificate	*204*	*341*	
LinkCertificate	204	341	{00..00}
EF Identification	*211*	*211*	
CardIdentification	*65*	*65*	
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
cardIssuingAuthorityName	36	36	{00, 20..20}
cardIssueDate	4	4	{00..00}
cardValidityBegin	4	4	{00..00}
cardExpiryDate	4	4	{00..00}
WorkshopCardHolderIdentification	*146*	*146*	
workshopName	36	36	{00, 20..20}
workshopAddress	36	36	{00, 20..20}
cardHolderName			
holderSurname	36	36	{00, 20..20}
holderFirstNames	36	36	{00, 20..20}
cardHolderPreferredLanguage	2	2	{20 20}
EF Card_Download	*2*	*2*	
NoOfCalibrationsSinceDownload	2	2	{00 00}
EF Calibration	*14788*	*42844*	
WorkshopCardCalibrationData	*14788*	*42844*	
calibrationTotalNumber	2	2	{00 00}
calibrationPointerNewestRecord	2	2	{00}
calibrationRecords	*14784*	*42840*	
WorkshopCardCalibrationRecord n_5	*168*	*168*	
calibrationPurpose	1	1	{00}
vehicleIdentificationNumber	17	17	{20..20}
vehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
wVehicleCharacteristicConstant	2	2	{00 00}
kConstantOfRecordingEquipment	2	2	{00 00}
lTyreCircumference	2	2	{00 00}
tyreSize	15	15	{20..20}
authorisedSpeed	1	1	{00}
oldOdometerValue	3	3	{00..00}
newOdometerValue	3	3	{00..00}
oldTimeValue	4	4	{00..00}
newTimeValue	4	4	{00..00}
nextCalibrationDate	4	4	{00..00}
vuPartNumber	16	16	{20..20}
vuSerialNumber	8	8	{00..00}
sensorSerialNumber	8	8	{00..00}
sensorGNSSSerialNumber	8	8	{00..00}
rcmSerialNumber	8	8	{00..00}
vuAbility	1	1	{00}
sealDataCard	46	46	
noOfSealRecords	1	1	{00}
SealRecords	45	45	
SealRecord 5	9	9	
equipmentType	1	1	{00}
extendedSealIdentifier	8	8	{00..00}

EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
cardVehicleRecords	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	
CardPlaceDailyWorkPeriod		*128*	*170*	
placePointerNewestRecord		2	2	{00 00}
placeRecords		*126*	*168*	
PlaceRecord	n_4	*21*	*21*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
entryGNSSPlaceRecord		11	11	{00..00}
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

EF Current_Usage	*19*	*19*	
CardCurrentUse	*19*	*19*	
sessionOpenTime	4	4	{00..00}
sessionOpenVehicle			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Control_Activity_Data	*46*	*46*	
CardControlActivityDataRecord	*46*	*46*	
controlType	1	1	{00}
controlTime	4	4	{00..00}
controlCardNumber			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
controlVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
controlDownloadPeriodBegin	4	4	{00..00}
controlDownloadPeriodEnd	4	4	{00..00}
EF VehicleUnits_Used	*42*	*42*	
CardVehicleUnitsUsed	*42*	*82*	
vehicleUnitPointerNewestRecord	2	2	{00 00}
cardVehicleUnitRecords	*40*	*80*	
CardVehicleUnitRecord n_7	*10*	*10*	
timeStamp	4	4	{00..00}
manufacturerCode	1	1	{00..00}
deviceID	1	1	{00..00}
vuSoftwareVersion	4	4	{00..00}
EF GNSS_Places	*262*	*362*	
GNSSContinuousDriving	*262*	*362*	
gnssCDPointerNewestRecord	2	2	{00 00}
gnssContinuousDrivingRecords	*260*	*360*	
GNSSContinuousDrivingRecord n_8	*15*	*15*	
timeStamp	4	4	{00..00}
gnssPlaceRecord	11	11	
timeStamp	4	4	{00..00}
gnssAccuracy	1	1	{00}
geoCoordinates	6	6	{00..00}
EF Specific_Conditions	*12*	*22*	
SpecificConditions	*12*	*22*	
conditionPointerNewestRecord	2	2	{00 00}
specificConditionRecords	10	20	
SpecificConditionRecord n_9	*5*	*5*	
entryTime	4	4	{00..00}
specificConditionType	1	1	{00}

TCS_163 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки мастерской в приложении второго поколения:

		Мин.	**Макс.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 байтов (1 день * 93 изменения вида деятельности)	492 байта (1 день * 240 изменений вида деятельности)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Приложения контрольной карточки

4.4.1 Приложение контрольной карточки первого поколения

TCS_164 После персонализации приложение контрольной карточки первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

		Правила доступа		
Файл	**ИД файла**	**Read**	**Select**	**Update**
└DF Tachograph	‘0500h’			
├EF Application_Identification	‘0501h’	SC2	SC1	NEV
├EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├EF Identification	‘0520h’	**SC6**	SC1	NEV
└EF Controller_Activity_Data	‘050Ch’	SC2	SC1	SC3

В настоящей таблице для условий безопасности используются следующие сокращения:
SC1 ALW OR SM-MAC-G2
SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2
SC3 SM-MAC-G1 OR SM-MAC-G2
SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Все структуры EF транспарентны.

TCS_166 Приложение контрольной карточки первого поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	
└DF Tachograph		*11186*	*24526*	
├EF Application_Identification		*5*	*5*	
└ControlCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfControlActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
├EF Identification		*211*	*211*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└ControlCardHolderIdentification		*146*	*146*	
├controlBodyName		36	36	{00, 20..20}
├controlBodyAddress		36	36	{00, 20..20}
├cardHolderName				
├holderSurname		36	36	{00, 20..20}
└holderFirstNames		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}

EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных контрольной карточки в приложении первого поколения:

		Мин.	**Макс.**
n_7	NoOfControlActivityRecords	230	520

4.4.2 Приложение контрольной карточки второго поколения

TCS_168 После персонализации приложение контрольной карточки второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

			Правила доступа	
Файл	**ИД файла**	**SFID**	**Read / Select**	**Update**
DF Tachograph_G2			SC1	
EF Application_Identification	‘0501h’	1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	NEV
EF Identification	‘0520h’	6	SC1	NEV
EF Controller_Activity_Data	‘050Ch’	14	SC1	SM-MAC-G2

В настоящей таблице для условия безопасности используется следующее сокращение:
SC1 ALW OR SM-MAC-G2

TCS_169 Все структуры EF транспарентны.

TCS_170 Приложение контрольной карточки второго поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}

EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных контрольной карточки в приложении второго поколения:

		Мин.	**Макс.**
n_7	NoOfControlActivityRecords	230	520

4.5. Приложения карточки предприятия

4.5.1 Приложение карточки предприятия первого поколения

TCS_172 После персонализации приложение карточки предприятия первого поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

		Правила доступа		
Файл	**ИД файла**	**Read**	**Select**	**Update**
DF Tachograph	‘0500h’		SC1	
EF Application_Identification	‘0501h’	SC2	SC1	NEV
EF Card_Certificate	‘C100h’	SC2	SC1	NEV
EF CA_Certificate	‘C108h’	SC2	SC1	NEV
EF Identification	‘0520h’	**SC6**	SC1	NEV
EF Company_Activity_Data	‘050Dh’	SC2	SC1	SC3

В настоящей таблице для условий безопасности используются следующие сокращения:

SC1 ALW OR SM-MAC-G2
SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2
SC3 SM-MAC-G1 OR SM-MAC-G2
SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Все структуры EF транспарентны.

TCS_174 Приложение карточки предприятия первого поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
DF Tachograph		*11114*	*24454*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}

EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_175 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки предприятия в приложении первого поколения:

		Мин.	**Макс.**
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 Приложение карточки предприятия второго поколения

TCS_176 После персонализации приложение карточки предприятия второго поколения имеет следующую постоянную структуру файла и правила доступа к файлам:

Примечание: Короткий идентификатор SFID файла EF присваивается как десятичное число, например, значение 30 в двоичной системе соответствует величине 11110.

			Правила доступа	
Файл	**ИД файла**	**SFID**	**Read / Select**	**Update**
DF Tachograph_G2			SC1	
EF Application_Identification	‘0501h’	1	SC1	NEV
EF CardMA_Certificate	‘C100h’	2	SC1	NEV
EF CA_Certificate	‘C108h’	4	SC1	NEV
EF Link_Certificate	‘C109h’	5	SC1	NEV
EF Identification	‘0520h’	6	SC1	NEV
EF Company_Activity_Data	‘050Dh’	14	SC1	SM-MAC-G2

В настоящей таблице для условия безопасности используется следующее сокращение:
SC1 ALW OR SM-MAC-G2

TCS_177 Все структуры EF транспарентны.

TCS_178 Приложение карточки предприятия второго поколения имеет следующую структуру данных:

Файл/Элемент данных	**Число записей**	**Размер (байты) Мин.**	**Макс.**	**Значения по умолчанию**
DF Tachograph_G2		*11338*	*25089*	
EF Application_Identification		*5*	*5*	
CompanyCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*139*	*139*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		*74*	*74*	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}

EF Company_Activity_Data		*10582*	*23922*	
CompanyActivityData		*10582*	*23922*	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		*10580*	*23920*	
companyActivityRecord	n_8	*46*	*46*	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
downloadPeriodBegin		4	4	{00..00}
downloadPeriodEnd		4	4	{00..00}

TCS_179 Следующие значения, используемые для указания размера файлов в таблице выше, представляют собой минимальные и максимальные значения числа записей, которые должны использоваться в структуре данных карточки предприятия в приложении второго поколения:

		Мин.	**Макс.**
n_8	NoOfCompanyActivityRecords	230	520