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 11 к приложению IC к регламенту (ЕС) 2016/799.

RU

ПРИЛОЖЕНИЕ 11. ОБЩИЕ МЕХАНИЗМЫ БЕЗОПАСНОСТИ

СОДЕРЖАНИЕ

Преамбула

Настоящее приложение описывает механизмы безопасности, обеспечивающие

- взаимную аутентификацию между различными компонентами системы тахографов.
- конфиденциальность, целостность, подлинность и/или неподдельности данных, передаваемых между различными компонентами системы тахографов или загружаемых на внешние носители.

Приложение состоит из двух частей. Часть А характеризует механизмы безопасности для системы тахографов первого поколения (цифрового тахографа). Часть Б характеризует механизмы безопасности для системы тахографов второго поколения («умного» тахографа).

Механизмы, представленные в части А настоящего приложения, применяются, если хотя бы один из компонентов системы тахографа, участвующий во взаимной аутентификации и/или передаче данных, принадлежит к первому поколению.

Механизмы, представленные в части Б настоящего приложения, применяются, если оба компонента системы тахографа, участвующие во взаимной аутентификации и/или передаче данных, принадлежат ко второму поколению.

В приложении 15 представлена более подробная информация об использовании компонентов первого поколения в сочетании с компонентами второго поколения.

ЧАСТЬ А. СИСТЕМА ТАХОГРАФОВ ПЕРВОГО ПОКОЛЕНИЯ

1. Введение

1.1. Ссылки

В настоящем приложении используются следующие источники:

SHA-1	Национальный институт стандартов и технологий (NIST). *Публикация FIPS 180-1: стандарт безопасного хеширования*. Апрель 1995 г.
PKCS1	Лаборатории RSA. PKCS # 1: *стандарт шифрования RSA*. Версия 2.0. Октябрь 1998 г.
TDES	Национальный институт стандартов и технологий (NIST). *Публикация FIPS 46-3: стандарт шифрования данных*. Проект 1999 г.
TDES-OP	ANSI X9.52, Рабочие режимы алгоритма тройного шифрования данных. 1998.
ISO/IEC 7816-4	Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами– Часть 4: межсекторные команды обмена данными. 1-е издание: 1995 + поправка 1: 1997.
ISO/IEC 7816-6	Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами– Часть 6: межсекторные элементы данных. 1-е издание: 1996 + поправка 1: 1998.
ISO/IEC 7816-8	Информационные технологии. Идентификационные карточки – карточки с интегральными микросхемами с контактами – Часть 8: Межсекторные команды, связанные с безопасностью. 1-е издание, 1999.
ISO/IEC 9796-2	Информационные технологии. Техника обеспечения безопасности. Схемы цифровой подписи с восстановлением сообщений. Часть 2: механизмы с использованием хэш-функции. 1-е издание: 1997.
ISO/IEC 9798-3	Информационные технологии. Техника обеспечения безопасности. Механизмы аутентификации субъектов. Часть 3: аутентификация субъектов с применением алгоритма открытого ключа. 2-е издание, 1998.
ISO 16844-3	Дорожные транспортные средства. Системы тахографов. Часть 3: интерфейс датчика движения.

1.2. Условные обозначения и сокращённые термины

В настоящем приложении используются следующие условные обозначения и сокращённые термины:

(K_a, K_b, K_c)	набор ключей, используемый в рамках алгоритма тройного шифрования данных,
CA	Сертифицирующий орган,
CAR	Указатель сертифицирующего органа,
CC	Криптографическая контрольная сумма,
CG	Криптограмма,
CH	Заголовок команды,
CHA	Полномочия держателя сертификата,
CHR	Указатель держателя сертификата,
D()	Расшифровка при помощи DES,
DE	Элемент данных,
DO (ОД)	Объект данных,
d	Закрытый ключ в криптосистеме RSA, закрытая экспонента,
e	Открытый ключ в криптосистеме RSA, открытая экспонента,
E()	Шифрование при помощи DES,
EQT	Аппаратура,
Hash()	Значение хеш-функции, выходные данные *хеширования*,
Hash	Хеш-функция,
KID	Ключевой идентификатор,
Km	Ключ TDES. Ключ верхнего уровня, определение которого содержится в ISO 16844-3.
Km_{VU}	Ключ TDES, вводимый в бортовые устройства.
Km_{WC}	Ключ TDES, вводимый в карточки мастерской.
m	Репрезентативный параметр сообщения, целое число от 0 до *n*-1,
n	ключ криптосистемы RSA, модуль,
PB	Байты заполнения,
PI	Байт индикации заполнения (используется в криптограммах для обеспечения конфиденциальности объектов данных),
PV	Простое значение,
s	Репрезентативный параметр подписи, целое число от 0 до *n*-1,
SSC	Счётчик исходящих сообщений,
SM	Защищённый обмен сообщениями,
TCBC	Режим сцепления криптоблоков при тройном шифровании данных TDEA
TDEA	Алгоритм тройного шифрования данных,
TLV	Значение длины метки,
VU (БУ)	Бортовое устройство,
X.C	Сертификат пользователя X, выданный сертификационным органом,
X.CA	Сертификационный орган пользователя X,
$X.CA.PK \circ X.C$	Операция по расшифровке сертификата с целью извлечения открытого ключа. Используется двухкомпонентный оператор, левым компонентом которого является открытый ключ сертификационного органа, а правым компонентом выданный этим сертификационный органом сертификат. Результатом операции является открытый ключ пользователя X, сертификат которого использовался в качестве правого компонента;
X.PK	Открытый ключ пользователя X в криптосистеме RSA,
X.PK[I]	Шифрование информации I по системе RSA с использованием открытого ключа пользователя X,
X.SK	Закрытый ключ пользователя X в криптосистеме RSA,

X.SK[I]	Шифрование информации I по системе RSA с использованием закрытого ключа пользователя X,
‘xx’	Шестнадцатеричное значение,
||	оператор конкатенации.

2. Криптографические системы и алгоритмы

2.1. Криптографические системы

CSM_001 В бортовых устройствах и карточках тахографа применяется классический вариант криптосистемы RSA с открытым ключом для решения следующих задач защиты:

- взаимная аутентификация бортовых устройств и карточек,
- передача между бортовыми устройствами и карточками тахографа сеансовых ключей тройного шифрования по системе DES,
- цифровая подпись данных, загружаемых с бортовых устройств или карточек тахографа и сохраняемых на внешних носителях.

CSM_002 В бортовых устройствах и карточках тахографа используется симметричная криптосистема DES с тройным шифрованием информации для её защиты от искажений при пользовательских операциях обмена данными между бортовыми устройствами и карточками тахографа и для обеспечения в необходимых случаях конфиденциальности данных, передаваемых между бортовым устройством и карточкой тахографа.

2.2. Криптографические алгоритмы

2.2.1 Алгоритм RSA

CSM_003 Алгоритм RSA полностью выражается следующими соотношениями:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Более полное описание функции RSA можно найти в источниках [PKCS1]. Открытая экспонента, e, для расчётов RSA это целое число в диапазоне от 3 до n-1, удовлетворяющее условию gcd(e, lcm(p-1, q-1))=1.

2.2.2 Алгоритм хеширования

CSM_004 В схемах цифровой подписи используется хеш-алгоритм SHA-1, описание которого приведено в источниках [SHA-1].

2.2.3 Алгоритм шифрования данных

CSM_005 Алгоритмы на базе DES применяются в режиме сцепления криптоблоков.

3. Ключи и сертификаты

3.1. Генерация и рассылка ключей

3.1.1 Генерация и рассылка ключей RSA

CSM_006 Ключи RSA генерируются на трёх функциональных уровнях, которые образуют следующую иерархию:

- европейский уровень,
- уровень государства-члена,
- аппаратный уровень.

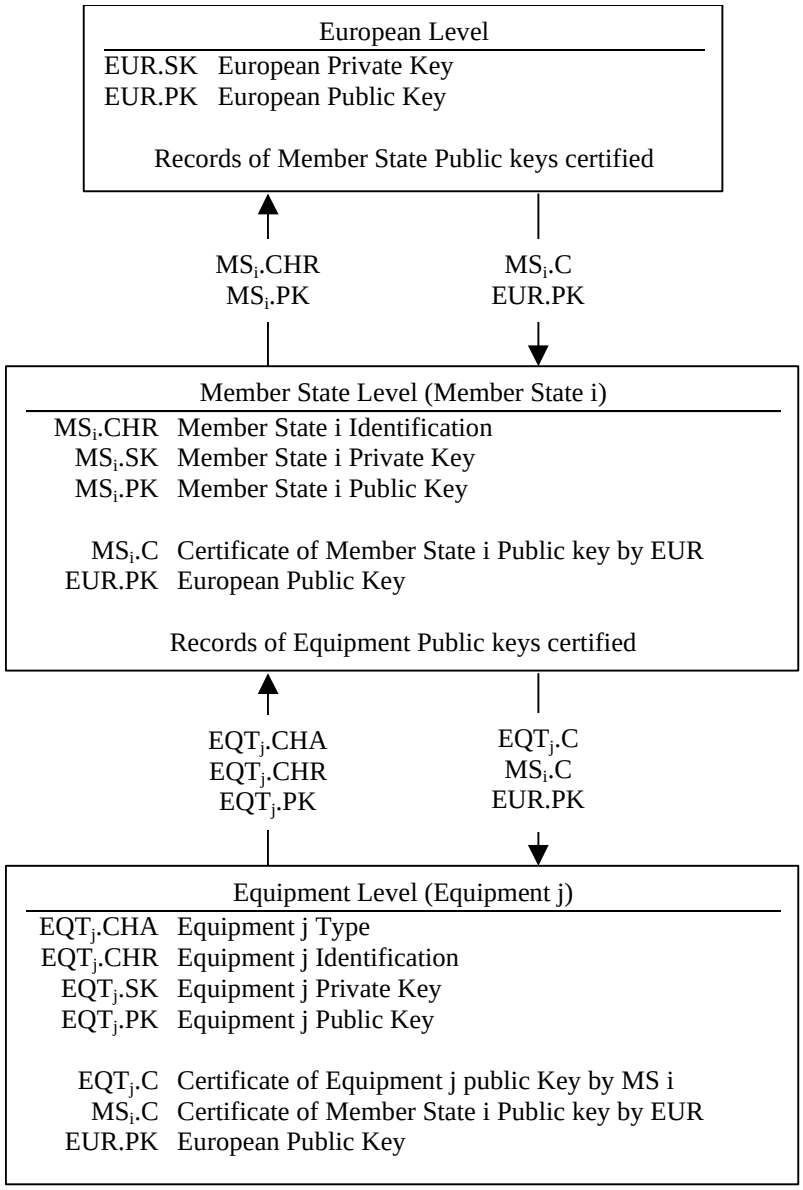
CSM_007 На европейском уровне генерируется единая пара общеевропейских ключей (EUR.SK и EUR.PK). Закрытый европейский ключ служит для сертификации открытых ключей государств-членов. Все сертифицируемые ключи подлежат регистрации. Эти задачи выполняет европейский сертификационный орган под руководством и при ответственности Европейской комиссии.

CSM_008 На уровне государств-членов генерируется пара ключей государств-членов (MS.SK и MS.PK). Открытые ключи государств-членов сертифицируются европейским сертификационным органом. Закрытый ключ государства-члена используется для сертификации открытых ключей, вводимых в соответствующие аппаратные средства (бортовые устройства или карточки тахографа). Все сертифицируемые открытые ключи подлежат регистрации с указанием аппаратуры, для которой они предназначены. Эти функции выполняет сертификационный орган государства-члена. Государство-член может регулярно менять свою пару ключей.

CSM_009 На аппаратном уровне генерируется единая пара ключей (EQT.SK и EQT.PK), вводимых в каждое устройство. Открытые ключи аппаратного уровня сертифицирует сертификационный орган государства-члена. Эти функции могут также выполнять производители аппаратуры, предприятия, персонализирующие аппаратуру, или соответствующие органы государств-членов. Данная пара ключей служит для аутентификации, создания цифровых подписей и шифрования данных.

CSM_010 При генерации, транспортировке (если она необходима) и хранении закрытых ключей соблюдается режим конфиденциальности.

Поток данных в ходе этого процесса схематически представлен на рисунке ниже.



3.1.2 Испытательные ключи RSA

CSM_011 В целях испытания аппаратуры (включая испытания на эксплуатационную совместимость) европейский сертификационный орган генерирует отдельную единую пару общеевропейских испытательных ключей и не менее двух пар испытательных ключей для государств-членов, открытые ключи которых сертифицируются закрытым испытательным ключом общеевропейского уровня. При испытаниях, проводимых с целью официального утверждения типовых образцов, в испытываемую аппаратуру производителями вводятся испытательные ключи, сертифицированные одним из вышеупомянутых испытательных ключей государств-членов.

3.1.3 Ключи датчика движения

При генерации, транспортировке (если она необходима) и хранении трёх ключей TDES, о которых говорится ниже, соблюдается надлежащий режим конфиденциальности.

В целях обеспечения совместимости с компонентами тахографов, соответствующими стандарту ISO 16844, европейский сертификационный орган и сертификационные органы государств-членов предпринимают нижеследующие дополнительные меры:

CSM_036 Европейский сертификационный орган генерирует Km_{VU} и Km_{WC}, два независимых уникальных ключа для тройного шифрования по системе DES, после чего вычисляет Km по формуле: $Km = Km_{VU}$ XOR Km_{WC}. По запросам сертификационных органов государств-членов европейский сертификационный орган высылает им эти ключи с соблюдением надлежащих процедур защиты.

CSM_037 Сертификационные органы государств-членов:

- используют ключ Km для шифрования показаний датчиков движения в соответствии с указаниями производителей этих датчиков (определение данных, подлежащих шифрованию ключом Km, даётся в стандарте ISO 16844-3),
- с соблюдением надлежащих процедур защиты высылают Km_{VU} производителям бортовых устройств для ввода в эти устройства,
- обеспечивают ввод Km_{WC} во все карточки мастерских (запись `SensorInstallationSecData` в элементарном файле `Sensor_Installation_Data`) при персонализации карточек.

3.1.4 Генерация и рассылка ключей сеанса T-DES

CSM_012 Бортовые устройства и карточки тахографа в рамках процесса взаимной аутентификации генерируют необходимые данные и обмениваются ими в целях составления единого сеансового ключа для тройного шифрования по системе DES. Для сохранения конфиденциальности этого обмена данными используется криптографическая защита RSA.

CSM_013 Данный ключ используется при всех последующих операциях криптозащищённого обмена сообщениями. Он перестаёт действовать по окончании текущего сеанса (извлечение или перезагрузка карточки) и/или после 240-го использования (однократное использование ключа = передача на карточку одного защищённого сообщения-команды и получение соответствующего ответа).

3.2. Ключи

CSM_014 Ключи RSA (независимо от уровня) имеют следующую длину: модуль *n* 1024 бита, открытая экспонента *e* до 64 бит, закрытая экспонента *d* 1024 бита.

CSM_015 Ключи DES для тройного шифрования имеют вид (K_a, K_b, K_a), где K_a и K_b – независимые ключи длиной 64 бита. Биты контроля по чётности не задаются.

3.3. Сертификаты

CSM_016 Сертификаты открытых ключей RSA – «не самодокументирующие» сертификаты, поддающиеся проверке (источник: ISO/IEC 7816-8)

3.3.1 Содержание сертификатов

CSM_017 Сертификаты открытых ключей RSA создаются на основе следующих данных в указанной последовательности:

Данные	**Формат**	**Байты**	**Наблюдения**
CPI	INTEGER	1	Идентификатор профиля сертификата (в данной версии – ‘01’)
CAR	OCTET STRING	8	Указатель сертифицирующего органа
CHA	OCTET STRING	**7**	Полномочия держателя сертификата
EOV	TimeReal	4	Дата истечения срока действия сертификата. Может не указываться; в этом случае поле заполняется байтами “FF”.
CHR	OCTET STRING	8	Указатель держателя сертификата
n	OCTET STRING	128	Открытый ключ (модуль)
e	OCTET STRING	8	Открытый ключ (открытая экспонента)
		164	

Примечания:

1. 1. Идентификатор профиля сертификата (CPI) определяет конкретную структуру сертификата, используемого в целях аутентификации. Он может применяться аппаратурой в качестве внутреннего идентификатора для вызова соответствующего списка заголовков, заключающего в себе описание конкатенации элементов данных, из которых состоит сертификат.

   Данному сертификату соответствует следующий список заголовков:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	’81 80’	‘82’	‘08’

2. 2. Указатель сертификационного органа (CAR) служит для обозначения сертификационного органа, выдавшего сертификат; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа сертификационного органа для указания на принадлежащий данному органу открытый ключ (информацию о соответствующих кодах см. ниже в пункте, посвящённом идентификаторам ключей).
3. 3. Полномочия держателя сертификата (CHA) – указание на объём прав, предоставляемых сертификатом. Они включают в себя идентификатор приложения тахографа и типа аппаратуры, для которой предназначен сертификат (соответствует элементу данных EquipmentType; для государства-члена используется значение ‘00’).
4. 2. Указатель держателя сертификата (CHR) служит для уникального обозначения держателя сертификата; таким образом, этот элемент данных может использоваться одновременно с идентификатором ключа субъекта для указания на принадлежащий данному держателю сертификата открытый ключ.
5. Идентификаторы ключей позволяют однозначно идентифицировать держателя сертификата или сертификационный орган. Они кодируются следующим образом:

   5.1 Аппаратура (БУ или карточка):

Данные	Серийный номер оборудования	Дата	Тип	Производитель
Длина	4 байта	2 байта	1 байт	1 байт
Значение	Целое число	мм гг BCD-код	Относится к конкретному производителю	Код производителя

   Когда речь идёт о БУ, его производитель, запрашивая сертификаты, не обязательно должен знать идентификационные данные аппаратуры, в которую будут вводиться соответствующие ключи.

   Если эти идентификационные данные производителю известны, он направляет их вместе с открытым ключом на сертификацию в сертификационный орган своего государства-члена. Выданный в результате сертификат будет содержать идентификационные данные аппаратуры, и производителю необходимо будет принять меры к тому, чтобы ключи и сертификат вводились именно в ту аппаратуру, для которой они предназначены. Идентификатор ключа при этом имеет вид, показанный выше.

   Если идентификационные данные производителю неизвестны, он должен однозначно идентифицировать каждый запрос на сертификат и направляет такие идентификационные данные вместе с открытым ключом на сертификацию в сертификационный орган своего государства-члена. В выданном сертификате будет указано индивидуальное обозначение заявки. После ввода ключа в аппаратуру производитель должен информировать сертификационный орган своего государства-члена о закреплении этого ключа за соответствующей аппаратурой (т.е. сообщить индивидуальное обозначение заявки на сертификат и идентификационные данные аппаратуры). При этом идентификатор ключа выглядит следующим образом:

Данные	Серийный номер заявки на выдачу сертификата	Дата	Тип	Производитель
Длина	4 байта	2 байта	1 байт	1 байт

Значение	Целое число	мм гг BCD-код	‘FF’	Код производителя

5.2 Сертифицирующий орган:

Данные	Идентификационные данные органа	Серийный номер ключа	Дополнительная информация	Идентификатор
Длина	4 байта	1 байт	2 байта	1 байт
Значение	Цифровой код государства 1 байт Буквенно-цифровой код государства 3 байта	Целое число	Дополнительное кодирование (относится к конкретному CA) ‘FF FF’, если не используется	‘01’

Серийный номер ключа позволяет отличать друг от друга различные ключи государства-члена в случае смены им своего ключа.

6. Сторона, проверяющая сертификат, по косвенным признакам распознаёт сертифицируемый открытый ключ как ключ криптосистемы RSA, предназначенный для аутентификации, проверки цифровых подписей и шифрования конфиденциальной информации (сам сертификат не содержит прямо указывающих на это идентификаторов объектов).

3.3.2 Выдаваемые сертификаты

CSM_018 Выдаваемый сертификат представляет собой цифровую подпись с возможностью частичного восстановления содержания сертификата, соответствующую стандарту ISO/IEC 9796-2 (за исключением дополнения A4) и сопровождаемую указателем сертификационного органа.

$$X.C = X.CA.SK[‘6A’ \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, ‘BC’] \,||\, C_n \,||\, X.CAR$$

С содержанием сертификата = Cc = C_r || C_n
106 байтов 58 байтов

Примечания:

1. Длина данного сертификата составляет 194 байта.
2. К подписи также приобщается скрытый ею CAR, что позволяет использовать для проверки сертификата открытый ключ соответствующего сертификационного органа.
3. Сторона, проверяющая сертификат, по косвенным признакам определяет алгоритм, использованный сертификационным органом для подписания сертификата.
4. Данному сертификату соответствует следующий список заголовков:

‘7F 21’	‘09’	‘5F 37’	’81 80’	‘5F 38’	‘3A’	‘42’	‘08’
Метка сертификата CV (генерируется)	Длина последующих объектов данных	Метка подписи	Длина подписи	Метка остатка	Длина остатка	Метка CAR	Длина CAR

3.3.3 Проверка и расшифровка сертификатов

Процесс проверки и расшифровки сертификатов заключается в проверке подписи согласно стандарту ISO/IEC 9796-2, извлечении содержания сертификата и получении из него соответствующего открытого ключа: $X.PK = X.CA.PK \circ X.C$ и проверке действительности сертификата.

CSM_019 Этот процесс состоит из следующих этапов:

Проверка подписи и извлечение содержания:
– из X.C извлекаются Sign, C_n’ и CAR’: X.C = Sign || C_n’ || CAR’

128 байтов 58 байтов 8 байтов

- из CAR’ выбирается открытый ключ соответствующего сертификационного органа (если он не выбран до этого иным способом)
- функция Sign открывается при помощи открытого ключа CA: Sr’= X.CA.PK [Sign],
- проверяется Sr’ (начальными символами должны быть ‘6A’, конечными – ‘BC’);
- вычисляются C_r’ и H’ по формуле: Sr’ = ‘6A’|| C_r’ || H’ || ‘BC’

106 байтов 20 байтов

- Восстанавливается содержание сертификата C’ = C_r’ || C_n’,
- проверяется *Hash*(C’) = H’

Положительный результат проверки указывает на подлинность сертификата, содержание которого соответствует C’.

Подтверждение действительности. Из C’:

- если применимо, проверяется дата истечения срока действия сертификата.

Извлечение из C’ и сохранение открытого ключа, идентификатора ключа, полномочий держателя сертификата и даты истечения срока его действия:

- X.PK = *n* || *e*
- X.KID = CHR
- X.CHA = CHA
- X.EOV = EOV

4. Механизм взаимной аутентификации

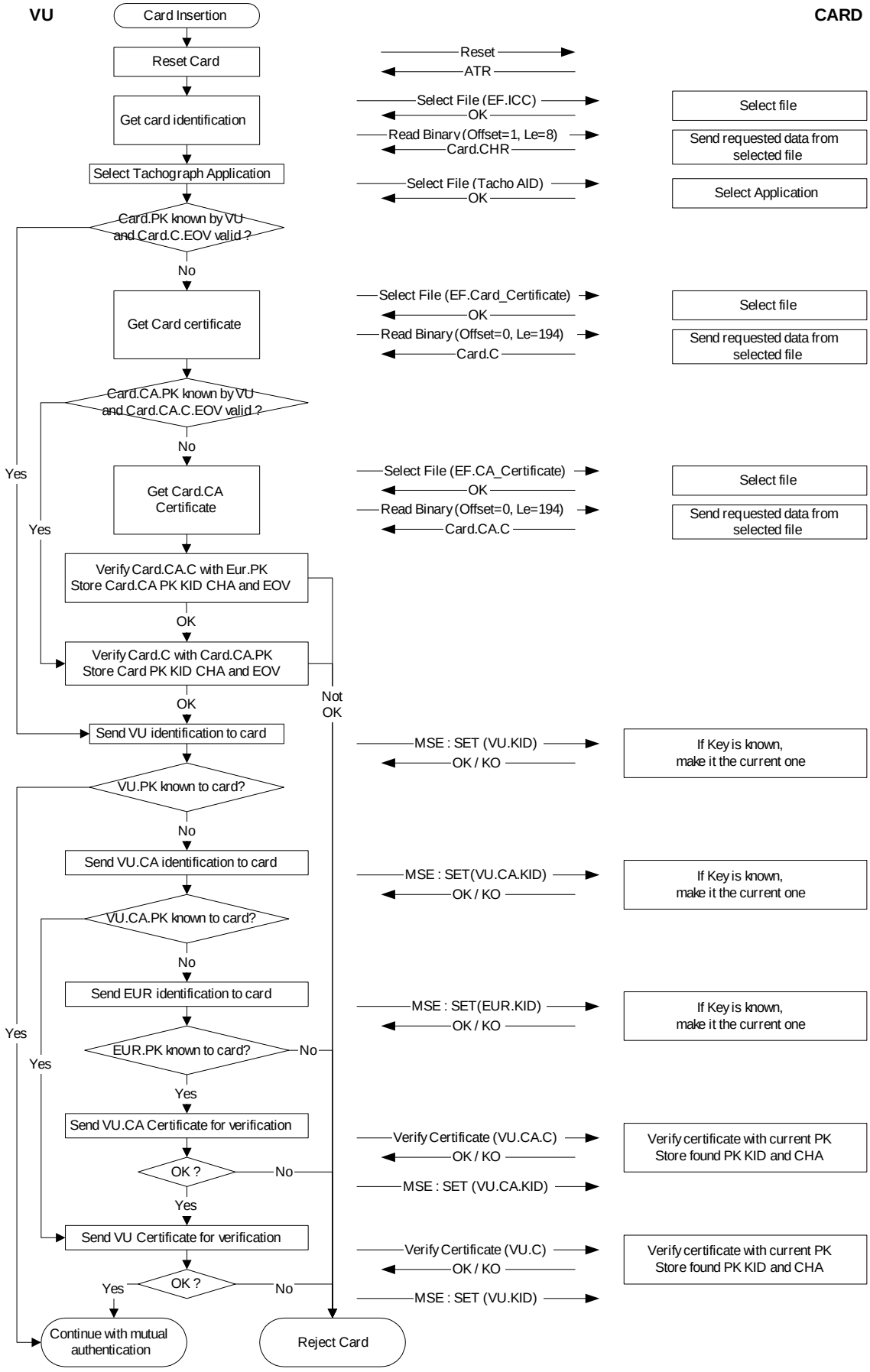
В основу механизма взаимной аутентификации карточек и БУ положен следующий принцип:

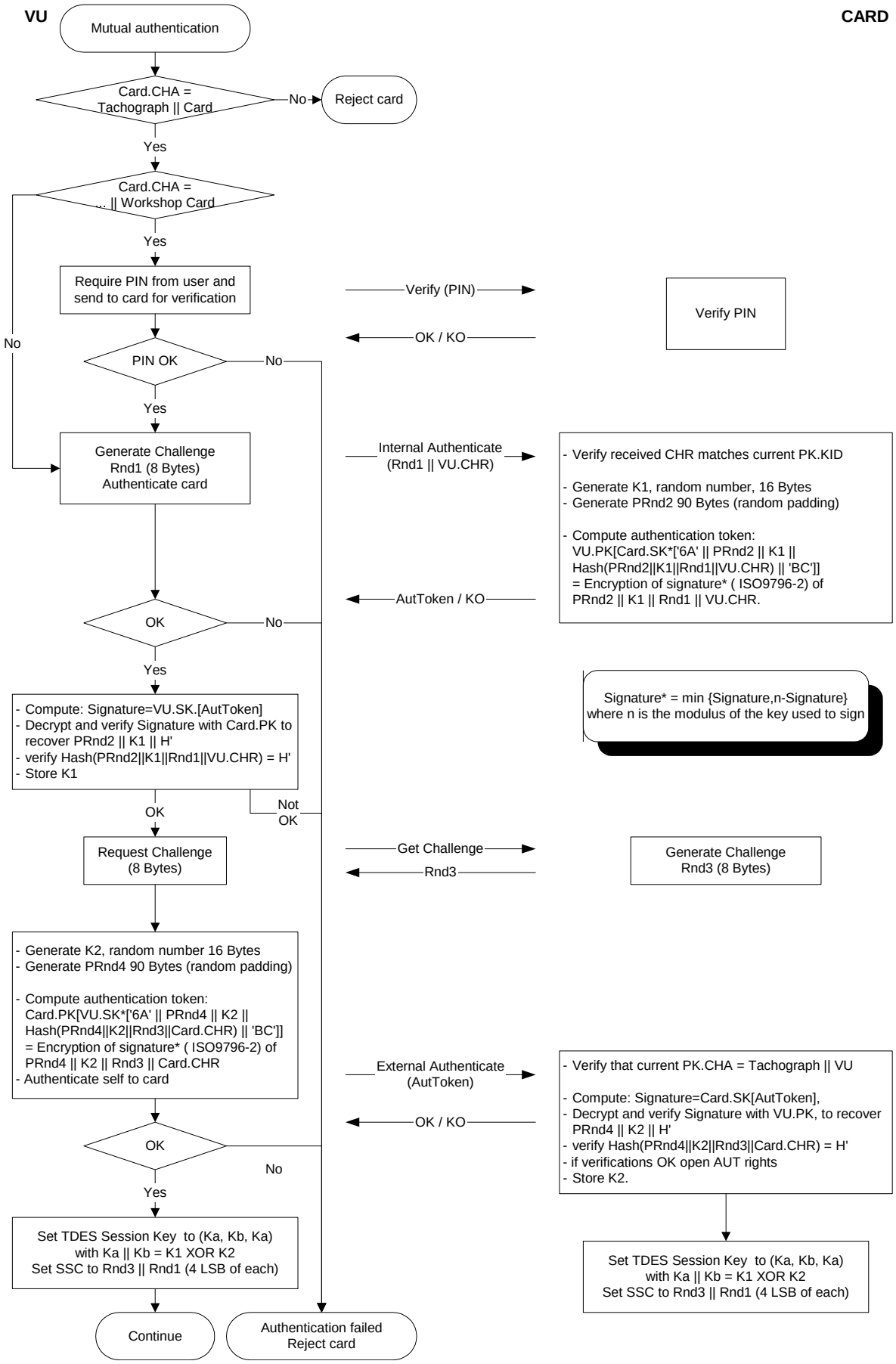
Каждая сторона должна доказать другой наличие у неё действительной пары ключей, открытый ключ которой сертифицирован сертификационным органом государства-члена, имеющим в свою очередь сертификат, выданный европейским сертификационным органом.

Доказательством служит подписание закрытым ключом случайной последовательности цифр, полученной от другой стороны, которая при проверке подписи должна восстановить из неё ту же последовательность цифр.

Данный механизм запускается со стороны БУ при вводе карточки. Процесс начинается с обмена сертификатами и извлечения открытых ключей и завершается созданием сеансового ключа.

CSM_020 При этом используется протокол, представленный ниже (стрелками показаны команды и передаваемые данные (см. Приложение 2)):


VU
CARD
Card Insertion
Reset Card
Reset
ATR
Get card identification
Select File (EF.ICC)
OK
Select file
Read Binary (Offset=1, Le=8)
Card.CHR
Send requested data from selected file
Select Tachograph Application
Select File (Tacho AID)
OK
Select Application
Card.PK known by VU and Card.C.EOV valid ?
No
Get Card certificate
Select File (EF.Card_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.C
Send requested data from selected file
Card.CA.PK known by VU and Card.CA.C.EOV valid ?
No
Yes
Get Card.CA Certificate
Select File (EF.CA_Certificate)
OK
Select file
Read Binary (Offset=0, Le=194)
Card.CA.C
Send requested data from selected file
Yes
Verify Card.CA.C with Eur.PK
Store Card.CA PK KID CHA and EOV
OK
Verify Card.C with Card.CA.PK
Store Card PK KID CHA and EOV
OK
Not OK
Send VU identification to card
MSE : SET (VU.KID)
OK / KO
If Key is known, make it the current one
VU.PK known to card?
No
Send VU.CA identification to card
MSE : SET(VU.CA.KID)
OK / KO
If Key is known, make it the current one
VU.CA.PK known to card?
No
Send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
Yes
EUR.PK known to card?
No
Yes
Yes
Send VU.CA Certificate for verification
Verify Certificate (VU.CA.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
OK ?
No
MSE : SET (VU.CA.KID)
Yes
Send VU Certificate for verification
Verify Certificate (VU.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
Yes
OK ?
No
MSE : SET (VU.KID)
Continue with mutual authentication
Reject Card


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
OK
Not OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. Механизмы обеспечения конфиденциальности, целостности и аутентификации данных при их передаче между БУ и карточками

5.1. Защищённый обмен сообщениями

CSM_021 Целостность данных, передаваемых между БУ и карточками, обеспечивается благодаря криптозащите сообщений в соответствии с цитируемыми источниками [ISO/IEC 7816-4] и [ISO/IEC 7816-8].

CSM_022 При передаче данных, которые нуждаются в защите, к высылаемым в виде команды или ответа объектам данных добавляется объект, представляющий собой криптографическую контрольную сумму. Эта криптографическая контрольная сумма проверяется принимающим устройством.

CSM_023 В криптографической контрольной сумме данных, высылаемых в виде команды, учитываются заголовок команды и все содержащиеся в ней объекты данных (=>CLA = ‘0C’, причём все эти объекты данных при их формировании снабжаются метками, где b1=1).

CSM_024 Байты ответа, несущие информацию о состоянии, защищаются с помощью криптографической контрольной суммы в тех случаях, когда ответ не содержит полей данных.

CSM_025 Криптографические контрольные суммы имеют длину 4 байта.

Таким образом, при защищённом обмене сообщениями команды и ответы имеют структуру, показанную ниже.

Используемые здесь объекты данных представляют собой часть набора ОД для защищённого обмена сообщениями, описание которого приводится в ISO/IEC 7816-4:

Метка	Мнемоника	Значение
‘81’	T_{PV}	Простое значение: данные без кодировки BER-TLV (защищаются с помощью CC)
‘97’	**T_{LE}**	Значение Le в незащищённой команде (защищается с помощью CC)
‘99’	T_{SW}	Информация о статусе (защищается с помощью CC)
‘8E’	T_{CC}	Криптографическая контрольная сумма
‘87’	$T_{PI\,CG}$	Байт индикации заполнения || Криптограмма (Простое значение без кодировки BER-TLV)

Если незащищённая пара команды и ответа выглядит следующим образом:

Заголовок команды	**Основная часть команды**
CLA INS P1 P2 четыре байта	[поле L_c] [Поле данных] [поле L_e] Байты L, обозначаемые как B_1-B_L

Основная часть ответа	**Концевая метка ответа**
[Поле данных] Байты данных L_r	SW1 SW2 два байта

соответствующая ей защищённая пара команды и ответа имеет следующий вид:

Защищённая команда:

Заголовок команды (CH)	**Основная часть команды**										
CLA INS P1 P2	[Новое поле L_c]	[Новое поле данных]									[Новое поле L_e]
‘OC’	Длина Новое поле данных	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
		‘81’	L_c	Поле данных	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Данные, которые должны быть включены в контрольную сумму = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = байты заполнения (80 .. 00) согласно стандартам ISO-IEC 7816-4 и ISO 9797 (метод 2).

Объекты данных PV и LE присутствуют лишь в случаях, когда незащищённая команда содержит соответствующие данные.

Защищённый ответ:

1. Если поле данных ответа не является пустым, но не нуждается в защите конфиденциальности:

Основная часть ответа						**Концевая метка ответа**
[Новое поле данных]						Новые SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Поле данных	‘8E’	‘04’	CC	

Данные, которые должны быть включены в контрольную сумму = T_{PV} || L_{PV} || PV || PB

2. Если поле данных ответа не является пустым и нуждается в защите конфиденциальности:

Основная часть ответа						**Концевая метка ответа**
[Новое поле данных]						Новые SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI || CG	‘8E’	‘04’	CC	

Информация, передаваемая в виде криптограммы: данные без кодировки BER-TLV и заполняющие байты.
Данные, которые должны быть включены в контрольную сумму = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Если поле данных ответа пустое:

Основная часть ответа						**Концевая метка ответа**
[Новое поле данных]						Новые SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
‘99’	‘02’	Новые SW1 SW2	‘8E’	‘04’	CC	

Данные, которые должны быть включены в контрольную сумму = T_{SW} || L_{SW} || SW || PB

5.2. Обработка ошибок при защищённом обмене сообщениями

CSM_026 Когда карточка тахографа обнаруживает ошибку SM при расшифровке команды, она возвращает соответствующие байты статуса, не используя SM. В соответствии со стандартом ISO/IEC 7816-4 для указания на ошибки SM предусматриваются следующие байты статуса:
’66 88’: Несоответствие криптографической контрольной суммы,
’69 87’: Отсутствие предусмотренных объектов данных SM,
’69 88’: Неверные объекты данных SM.

CSM_027 Если карточкой тахографа возвращены байты статуса без ОД SM или с неверным ОД SM, БУ должно прервать сеанс обмена данными.

5.3. Алгоритм расчёта криптографических контрольных сумм

CSM_028 Криптографические контрольные суммы вычисляются на основе алгоритма аутентификации сообщений retail-MAC в соответствии с ANSI X9.19 и системой DES:
- Начальный этап: в качестве первого контрольного блока y0 используется E(Ka, SSC).
- Последующий этап: контрольные блоки y1, .. , yn рассчитываются при помощи Ka.
- Заключительный этап: по последнему контрольному блоку yn рассчитывается криптографическая контрольная сумма: E(Ka, D(Kb, yn)).

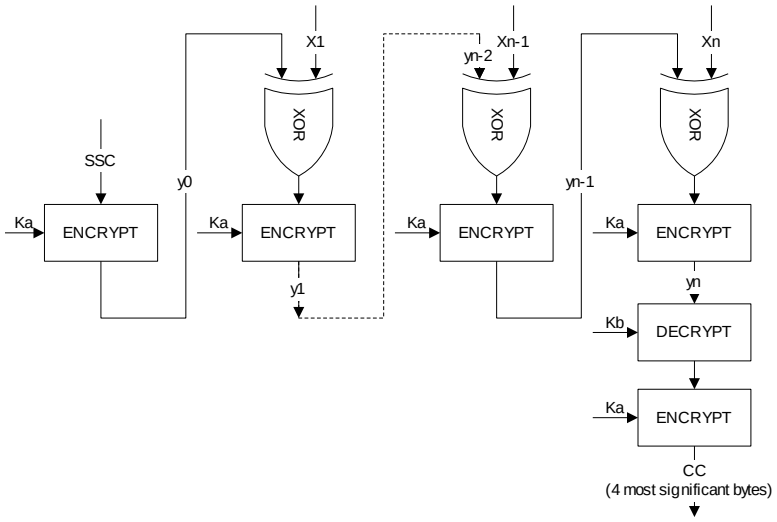
где E() означает шифрование по системе DES, а D() – расшифровку по системе DES.

Передаче подлежат четыре старших байта криптографической контрольной суммы.

CSM_029 Счётчик исходящих сообщений (SSC) запускается во время процедуры согласования ключа:
Исходный SSC : Rnd3 (4 наименее значимых байта) || Rnd1 (4 наименее значимых байта).

CSM_030 Счётчик исходящих сообщений увеличивается на 1 единицу перед каждым вычислением MAC (т.е. для первой команды значение SSC составляет исходный SSC + 1, а для первого ответа – исходный SSC + 2).

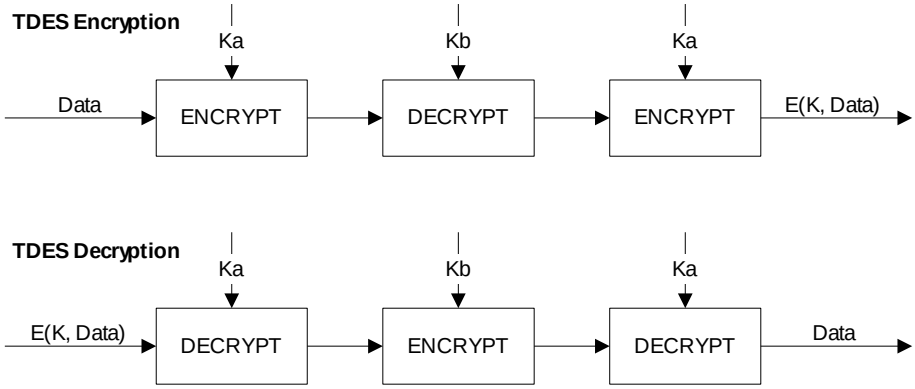
Способ вычисления retail-MAC изображен на диаграмме ниже:



5.4. Алгоритм расчёта криптограмм для защиты конфиденциальности ОД

CSM_031 Криптограммы рассчитываются с помощью алгоритма TDEA в режиме TCBC, как указано в цитируемых источниках [TDES] и [TDES-OP], причём в качестве блока начальной величины используется нуль-вектор.

Применение ключей TDES изображён на диаграмме ниже:



6. Механизмы цифровой подписи при загрузке данных

CSM_032 Данные, полученные из того или иного аппаратного источника (БУ или карточки) за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Данный файл должен содержать сертификаты MS_i.C и EQT.C. Файл содержит цифровые подписи блоков данных в соответствии с указанными в приложении 7 (Протоколы загрузки данных).

CSM_033 Цифровые подписи загружаемых данных создаются по схеме, предполагающей добавление информации, которая позволяет при желании производить считывание загруженных данных в нерасшифрованном виде.

6.1. Генерация подписей

CSM_034 Подписи данных генерируются аппаратурой согласно схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1:

Подпись = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(данные))]

PS = заполняющая октетная строка со значением ‘FF’ до общей длины 128.

DER(SHA-1(*M*)) – кодированное представление идентификатора алгоритма хеш-функции и значения хеш-функции в виде величины стандарта ASN.1 типа DigestInfo (правила однозначного шифрования):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||значение хеш-функции.

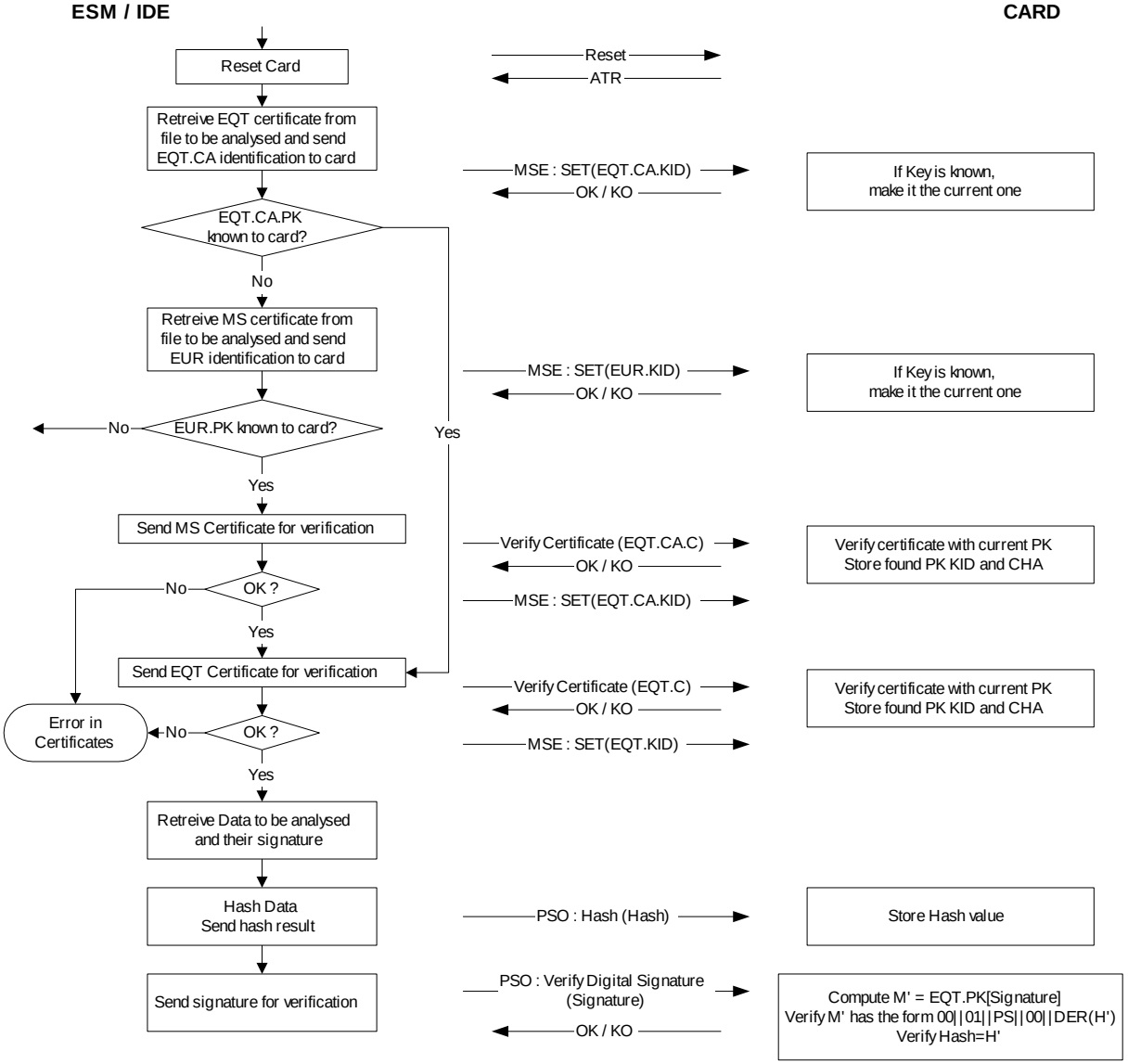
6.2. Проверка подписей

CSM_035 Подписи загружаемых данных проверяются по схеме подписи с соответствующим добавлением, которая определена в цитируемом источнике [PKCS1], при помощи хеш-функции SHA-1.

Проверяющей стороне должен быть известен европейский открытый ключ EUR.PK, который она должна получить из независимого (и пользующегося доверием) источника.

В нижеследующей таблице представлен протокол, в соответствии с которым СПА после ввода в неё карточки контролёра может проверять целостность загруженных данных, сохранённых на ВН (внешнем носителе). Для расшифровки цифровых подписей используется карточка контролёра. В этом случае данная функция не обязательно должна быть предусмотрена в СПА.

Аппаратура, с помощью которой были загружены и подписаны подлежащие анализу данные, обозначена буквами EQT.



ЧАСТЬ Б. СИСТЕМА ТАХОГРАФОВ ВТОРОГО ПОКОЛЕНИЯ

7. Введение

7.1. Ссылки

В этой части настоящего приложения используются следующие источники:

AES	Национальный институт стандартов и технологий (NIST), FIPS PUB 197: Расширенный стандарт шифрования (AES), 26 ноября 2001 г.
DSS	Национальный институт стандартов и технологий (NIST), FIPS PUB 186-4: Стандарт цифровой подписи (DSS), июль 2013 г.
ISO 7816-4	ISO/IEC 7816-4, Идентификационные карточки – карточки с интегральными микросхемами. Часть 4: организация, безопасность и команды обмена. 3-е издание. 15 апреля 2013 г.
ISO 7816-4	ISO/IEC 7816-4, Идентификационные карточки – карточки с интегральными микросхемами. Часть 8: команды операций по обеспечению безопасности. 2-е издание. 1 июня 2004 г.
ISO 8825-1	ISO/IEC 8825-1, Информационные технологии. Правила кодирования ASN.1: Спецификация базовых правил кодирования (BER), канонических правил кодирования (CER) и особых правил кодирования (DER). 4-е издание, 15 декабря 2008 г.
ISO 9797-1	ISO/IEC 9797-1, Информационные технологии. Техники обеспечения безопасности. Коды аутентификации сообщений (MAC). Часть 1: механизмы шифрования блоками. 2-е издание, 1 марта 2011 г.
ISO 10116	ISO/IEC 10116, Информационные технологии. Техника обеспечения безопасности. Режимы работы блока шифрования *n*-бит. 3-е издание, 1 февраля 2006 г.
ISO 16844-3	ISO/IEC 16844-3, Дорожные транспортные средства. Системы тахографов. Часть 3: интерфейс датчика движения. 1-е издание, 2004 г., включая техническую поправку 1 2006.
RFC 5480	Эллиптическая криптография. Информация об открытом ключе субъекта, март 2009 г.
RFC 5639	Эллиптическая криптография (ECC). Стандартные кривые Brainpool и генерирование кривых, 2010
RFC 5869	Функция формирования ключа извлечения и расширения на базе HMAC (HKDF), май 2010 г.
SHS	Национальный институт стандартов и технологий (NIST), FIPS PUB 180-4: стандарт безопасного хеширования, март 2012 г.
SP 800-38B	Национальный институт стандартов и технологий (NIST), специальный выпуск 800-38B: Рекомендация по режимам работы с шифрованием блоками: режим аутентификации CMAC, 2005
TR-03111	Технические рекомендации BSI TR-03111, эллиптическая криптография, версия 2.00, 28 июня 2012 г.

7.2. Условные обозначения и сокращения

В настоящем приложении используются следующие условные обозначения и сокращённые термины:

AES	Расширенный стандарт шифрования
CA	Сертификационный орган
CAR	Указатель сертификационного органа
CBC	Сцепление криптоблоков (режим работы)

CH Заголовок команды
CHA Полномочия держателя сертификата
CHR Указатель держателя сертификата
CV Постоянный вектор
DER Особые правила кодирования
DO (ОД) Объект данных
DSRC Выделенная связь ближнего действия
ECC Эллиптическая криптография
ECDSA Алгоритм цифровой подписи эллиптической кривой
ECDH Эллиптическая кривая Диффи-Хеллмана (алгоритм согласования ключей)
EGF Внешнее устройство ГНСС
EQT Аппаратура
IDE (СПА) Специализированная программируемая аппаратура
K_M Ключ старшего разряда датчика движения, позволяющий осуществлять соединение бортового устройства с датчиком движения
$K_{M\text{-}VU}$ Ключ, вводимый в бортовые устройства, позволяющий БУ генерировать ключ старшего разряда датчика движения, если в БУ вставлена карточка мастерской
$K_{M\text{-}WC}$ Ключ, вводимый в карточки мастерской, позволяющий БУ генерировать ключ старшего разряда датчика движения, если в БУ вставлена карточка мастерской
MAC Код аутентификации сообщений
MoS Датчик движения
MSB Самый значимый бит
PKI Инфраструктура открытых ключей
RCF Средство удалённой связи
SSC Счётчик исходящих сообщений
SM Защищённый обмен сообщениями
TDES Стандарт тройного шифрования данных
TLV Значение длины метки
VU (БУ) Бортовое устройство
X.C Сертификат открытого ключа пользователя X
X.CA Сертификационный орган, выдавший сертификат пользователю X
X.CAR Указатель сертификационного органа, указанного в сертификате пользователя X
X.CHR Указатель держателя сертификата, указанного в сертификате пользователя X
X.PK Открытый ключ пользователя X
X.SK Закрытый ключ пользователя X
$X.PK_{eph}$ Кратковременный открытый ключ пользователя X
$X.SK_{eph}$ Кратковременный закрытый ключ пользователя X
‘xx’ Шестнадцатеричное значение
|| оператор конкатенации

7.3. Определения

Определения терминов, употребляемых в настоящем приложении, даны в разделе I дополнения 1C.

8. Криптографические системы и алгоритмы

8.1. Криптографические системы

CSM_38 В бортовых устройствах и карточках тахографа применяется вариант криптосистемы на основе эллиптической кривой с открытым ключом для решения следующих задач защиты:
- взаимная аутентификация бортовых устройств и карточек,
- согласование сеансовых ключей AES между бортовыми устройствами и карточками,
- обеспечение подлинности, целостности и неподдельности данных, загружаемых с бортовых устройств или карточек тахографа на внешние носители.

CSM_39 В бортовых устройствах и внешних устройствах ГНСС применяется вариант криптосистемы на основе эллиптической кривой с открытым ключом для решения следующих задач защиты:
- соединение бортового устройства и внешнего устройства ГНСС,
- взаимная аутентификация бортового устройства и внешнего устройства ГНСС,
- согласование сеансовых ключей AES между бортовыми устройствами и внешними устройствами ГНСС.

CSM_40 В бортовых устройствах и карточках тахографа применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты:
- обеспечение подлинности и целостности данных, которыми обмениваются бортовое устройство и карточка тахографа,
- если применимо, обеспечение конфиденциальности данных, которыми обмениваются бортовое устройство и карточка тахографа.

CSM_41 В бортовых устройствах и внешних устройствах ГНСС применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты:
- обеспечение подлинности и целостности данных, которыми обмениваются бортовое устройство и внешнее устройство ГНСС.

CSM_42 В бортовых устройствах и датчиках движения применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты:
- соединение бортового устройства и датчика движения,
- взаимная аутентификация бортовых устройств и датчиков движения,
- обеспечение конфиденциальности данных, которыми обмениваются бортовое устройство и датчик движения.

CSM_43 В бортовых устройствах и контрольных карточках применяется вариант симметричной криптосистемы на основе AES для решения следующих задач защиты, связанных с интерфейсом удалённой связи:
- обеспечение конфиденциальности, подлинности и целостности данных, которые бортовое устройство передаёт на контрольную карточку.

Примечания:
- Строго говоря, данные передаются из бортового устройства на удалённое средство контроля под руководством контролёра при помощи средства удалённой связи, которое может внутренним или внешним относительно БУ; см. приложение 14. Однако удалённое средство контроля передаёт данные на контрольную карточку для расшифровки и подтверждения подлинности. С точки зрения защиты средство удалённой связи и удалённое средство контроля полностью транспарентны.
- Карточка мастерской предлагает те же самые функции интерфейса DSRC, что и контрольная карточка. Это позволяет мастерской проверять надлежащее функционирование интерфейса удалённой связи БУ, включая характеристики безопасности. Более подробно см. в разделе 9.2.2.

8.2. Криптографические алгоритмы

8.2.1 Симметричные алгоритмы

CSM_44 Бортовые устройства, карточки тахографов, датчики движения и внешние устройства ГНСС поддерживают алгоритм AES, определённый в источнике [AES], с длиной ключей 128, 192 и 256 бит.

8.2.2 Асимметричные алгоритмы и стандартизированные параметры области

CSM_45 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают эллиптическую криптографию с размером ключей 256, 384 и 512/521 бит.

CSM_46 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживать алгоритм подписи ECDSA, как описано в источнике [DSS].

CSM_47 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают алгоритм согласования ключей ECKA-EG, как указано в источнике [TR 03111].

CSM_48 Бортовые устройства, карточки тахографов и внешние устройства ГНСС поддерживают все стандартизированные параметры области, указанные ниже в Таблица 1 в отношении эллиптической криптографии.

Название	**Размер (биты)**	**Указатель**	**Идентификатор объекта**
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

Таблица 1 Стандартизированные параметры области

Примечание: идентификаторы объектов, перечисленные в последнем столбце Таблица 1, указаны в источнике [RFC 5639] по кривым Brainpool и в источнике [RFC 5480] по кривым NIST.

Пример 1: идентификатор объекта кривой BrainpoolP256r1 – `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}.`
Или в точечной нотации: `1.3.36.3.3.2.8.1.1.7.`

Пример 2: идентификатор объекта кривой NIST P-384 –
`{iso(1) identified-organization(3) certicom(132) curve(0) 34}.`
Или в точечной нотации: `1.3.132.0.34.`

8.2.3 Алгоритмы хеширования

CSM_49 Бортовые устройства и карточки тахографов поддерживают алгоритмы SHA-256, SHA-384 и SHA-512, описанные в [SHS].

8.2.4 Последовательности шифров

CSM_50 Если симметричный алгоритм, несимметричный алгоритм и/или алгоритм хеширования используются вместе для формирования протокола безопасности, длина их соответствующих ключей и размеры хеш-параметров (примерно) равны. Таблица 2 отображает допустимые последовательности шифров:

ИД последовательности шифров	**Размер ключа ECC (биты)**	**Длина ключа AES (биты)**	**Алгоритм хеширования**	**Длина MAC (в байтах)**
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Таблица 2 Допустимые последовательности шифров

Примечание: Размеры ключей ECC, составляющие 512 бит и 521 бит, считаются равными по силе для выполнения всех задач в рамках настоящего приложения.

9. Ключи и сертификаты

9.1. Асимметричные пары ключей и сертификаты открытых ключей

9.1.1 Общие положения

Примечание: ключи, описанные в настоящем разделе, используются для взаимной аутентификации и защищённого обмена сообщениями между бортовыми устройствами и карточками тахографов и между бортовыми устройствами и внешними устройствами ГНСС. Данные процессы подробно освещены в главах 10 и 11 настоящего приложения.

CSM_51 В рамках европейской системы «умных» тахографов пары ключей ECC и соответствующие сертификаты генерируются и управляются на трёх функциональных уровнях, образующих иерархию:

- европейский уровень,
- уровень государства-члена,
- аппаратный уровень.

CSM_52 Во всей европейской системе «умных» тахографов открытые и закрытые ключи и сертификаты генерируются, управляются и передаются при помощи стандартизированных защищённых средств.

9.1.2 Европейский уровень

CSM_53 На европейском уровне генерируется единая пара общеевропейских ключей ECC, обозначаемых как EUR. В неё входят закрытый ключ (EUR.SK) и открытый ключ (EUR.PK). Данная пара ключей формирует пару корневых ключей для PKI всей европейской системы «умных» тахографов. Эту задачу выполняет европейский сертификационный орган (ERCA) под руководством и при ответственности Европейской комиссии.

CSM_54 ERCA использует европейский закрытый ключ для подписания (самоподписывающегося) корневого сертификата европейского открытого ключа и передаёт этот европейский корневой сертификат всем государствам-членам.

CSM_55 ERCA использует европейский закрытый ключ для подписания сертификатов открытых ключей государств-членов по запросу. ERCA ведёт записи всех подписанных сертификатов открытых ключей государств-членов.

CSM_56 Как показано на Рисунок 1 в разделе 9.1.7, ERCA генерирует новую пару европейских корневых ключей каждые 17 лет. Когда ERCA генерирует новую пару европейских корневых ключей, он создаёт новый самоподписывающийся корневой сертификат для нового европейского открытого ключа. Срок действия европейского корневого сертификата составляет 34 года и 3 месяца.

Примечание: Введение новой пары корневых ключей также означает, что ERCA создаст новый ключ старшего разряда для датчика движения и новый ключ старшего разряда DSRC; см. разделы 9.2.1.2 и 9.2.2.2.

CSM_57 До генерирования новой пары европейских корневых ключей ERCA проводит анализ криптографической силы, необходимой для новой пары ключей, учитывая, что она должна быть защищена на протяжении следующих 34 лет. При необходимости ERCA переходит на последовательность шифров мощнее текущей, как указано в CSM_50.

CSM_58 Когда ERCA генерирует новую пару европейских корневых ключей, он создаёт связующий сертификат для нового европейского открытого ключа и подписывает его старым европейским закрытым ключом. Срок действия такого сертификата составляет 17 лет. Данный процесс также показан на Рисунок 1 в разделе 9.1.7.

Примечание: Поскольку связующий сертификат включает в себя открытый ключ ERCA поколения *X* и подписан закрытым ключом ERCA поколения *X-1*, такой сертификат предлагает аппаратуре поколения *X-1* средство доверия аппаратуре поколения *X*.

CSM_59 С момента вступления в силу нового сертификата корневого ключа ERCA больше не использует закрытый ключ пары корневых ключей ни для каких целей.

CSM_60 В любой момент времени ERCA располагает следующими криптографическими ключами и сертификатами:

- Текущая пара ключей EUR и соответствующий сертификат
- Все прежние сертификаты EUR для проверки сертификатов MSCA, которые всё ещё действительны
- Связующие сертификаты для всех поколений сертификатов EUR, кроме первого

9.1.3 Уровень государства-члена

CSM_61 На уровне государств-членов все государства, необходимы для подписания сертификатов карточек тахографов, генерируют одну или несколько уникальных пар ключей ECC, обозначаемых как MSCA_Card. Все государства-члены, необходимые для подписания сертификатов для бортовых устройств или внешних устройств ГНСС, также генерируют одну или несколько уникальных пар ключей ECC, обозначаемых как MSCA_VU-EGF.

CSM_62 Задачу генерирования пар ключей государств-членов выполняет сертификационный орган государства-члена (MSCA). Когда MSCA генерирует пару ключей государства-члена, он передаёт открытый ключ ERCA, чтобы получить соответствующий сертификат государства-члена, подписанный ERCA.

CSM_63 MSCA выбирает силу пары ключей государства-члена, которая была бы равна силе пары европейских корневых ключей, используемых для подписания соответствующего сертификата государства-члена.

CSM_64 Пара ключей MSCA_VU-EGF, если она есть, состоит из закрытого ключа MSCA_VU-EGF.SK и открытого ключа MSCA_VU-EGF.PK. MSCA использует закрытый ключ MSCA_VU-EGF.SK исключительно для подписания сертификатов открытых ключей бортовых устройств и внешних устройств ГНСС.

CSM_65 Пара ключей MSCA_Card состоит из закрытого ключа MSCA_Card.SK и открытого ключа MSCA_Card.PK. MSCA использует закрытый ключ MSCA_Card.SK исключительно для подписания сертификатов открытых ключей карточек тахографов.

CSM_66 MSCA ведёт учёт всех подписанных сертификатов БУ, внешних устройств ГНСС и карточек вместе с идентификационными данными оборудования, для которого предназначен каждый сертификат.

CSM_67 Срок действия сертификата MSCA_VU-EGF составляет 17 лет и 3 месяца. Срок действия сертификата MSCA_Card составляет 7 лет и 1 месяц.

CSM_68 Как показано на Рисунок 1 в разделе 9.1.7, закрытый ключ пары ключей MSCA_VU-EGF и закрытый ключ пары ключей MSCA_Card используются в течение двух лет.

CSM_69 С момента окончания периода применения MSCA больше не использует закрытый ключ пары ключей MSCA_VU-EGF ни для каких целей. С момента окончания периода применения MSCA также больше ни для каких целей не использует закрытый ключ пары ключей MSCA_Card.

CSM_70 В любой момент времени MSCA располагает следующими криптографическими ключами и сертификатами:

- Текущая пара ключей MSCA_Card и соответствующий сертификат
- Все прежние сертификаты MSCA_Card для проверки сертификатов карточек тахографа, которые всё ещё действительны
- Текущий сертификат EUR, необходимый для проверки текущего сертификата MSCA
- Все прежние сертификаты EUR, необходимые для проверки сертификатов MSCA, которые всё ещё действительны

CSM_71 Если MSCA должен подписывать сертификаты бортовых устройств или внешних устройств ГНСС, он дополнительно располагает следующими ключами и сертификатами:

- Текущая пара ключей MSCA_VU-EGF и соответствующий сертификат
- Все прежние сертификаты MSCA_VU-EGF для проверки сертификатов БУ или внешних устройств ГНСС, которые всё ещё действительны

9.1.4 Аппаратный уровень: бортовые устройства

CSM_72 Для каждого бортового устройства генерируются две уникальные пары ключей ECC, обозначаемые как VU_MA и VU_Sign. Эту задачу выполняют производители БУ. При генерировании пары ключей БУ сторона, генерирующая ключ, передаёт открытый ключ MSCA страны, в которой она проживает, чтобы получить соответствующий сертификат БУ, подписанный MSCA. Закрытый ключ использует только бортовое устройство.

CSM_73 У сертификатов VU_MA и VU_Sign определённого бортового устройства одна и та же дата срока действия сертификата.

CSM_74 Производитель БУ выбирает силу пары ключей БУ, которая была бы равна силе пары ключей MSCA, используемых для подписания соответствующего сертификата БУ.

CSM_75 Бортовое устройство использует свою пару ключей VU_MA, состоящую из закрытого ключа VU_MA.SK и открытого ключа VU_MA.PK, исключительно для аутентификации БУ относительно карточек тахографов и внешних устройств ГНСС, как указано в разделах 10.3 и 11.4 настоящего приложения.

CSM_76 Бортовое устройство способно генерировать кратковременные пары ключей ECC и использует такую пару ключей исключительно для согласования сеансовых ключей с карточкой тахографа или внешним устройством ГНСС, как указано в разделах 10.4 и 11.4 настоящего приложения.

CSM_77 Бортовое устройство использует закрытый ключ VU_Sign.SK своей пары ключей VU_Sign исключительно для загрузки файлов данных, как указано в главе 14 настоящего приложения. Соответствующий открытый ключ VU_Sign.PK используется исключительно для проверки подписей, созданных бортовым устройством.

CSM_78 Как показано на Рисунок 1 в разделе 9.1.7, срок действия сертификата VU_MA составляет 15 лет и 3 месяца. Срок действия сертификата VU_Sign также составляет 15 лет и 3 месяцаThe validity period of a VU_Sign certificate shall also be 15 years and 3 months.

Примечания:

- Продлённый срок действия сертификата VU_Sign позволяет бортовому устройству создавать действительные подписи через загружаемые данные в течение первых трёх месяцев после его истечения, как требуется в Регламенте (ЕС) № 581/2010.
- Продлённый срок действия сертификата VU_MA нужен для аутентификации БУ относительно контрольной карточки или карточки предприятия в течение первых трёх месяцев после его истечения, чтобы можно было загрузить данные.

CSM_79 С момент истечения срока действия соответствующего сертификата бортовое устройство не использует закрытый ключ пары ключей БУ ни для каких целей.

CSM_80 После начала эксплуатации бортового устройства пары ключей БУ (кроме кратковременных пар ключей) и соответствующие сертификаты данного бортового устройства на месте не заменяются.

Примечания:

- Данное требование не касается кратковременных пар ключей, так как новая кратковременная пара ключей генерируется БУ всякий раз, когда проводится аутентификация микросхемы и согласуются сеансовые ключи; см. раздел 10.4. Следует отметить, что у кратковременных пар ключей соответствующих сертификатов нет.
- Данное требование не исключает возможности замены статичных пар ключей БУ во время реконструкции или ремонта в защищённой среде, контролируемой производителем БУ.

CSM_81 После ввода в эксплуатацию бортовые устройства содержат следующие криптографические ключи и сертификаты:

- Закрытый ключ VU_MA и соответствующий сертификат
- Закрытый ключ VU_Sign и соответствующий сертификат
- Сертификат MSCA_VU-EGF, содержащий открытый ключ MSCA_VU-EGF.PK для проверки сертификата VU_MA и сертификата VU_Sign
- Сертификат EUR, содержащий открытый ключ EUR.PK, для проверки сертификата MSCA_VU-EGF

- Сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_VU-EGF, если таковой существует
- Связующий сертификат, соединяющий эти два сертификата EUR, если таковые существуют

CSM_82 Помимо криптографических ключей и сертификатов, перечисленных в CSM_81, в бортовых устройствах также есть ключи и сертификаты, указанные в части A настоящего приложения, позволяющие бортовому устройству вступать во взаимодействие с карточками тахографов первого поколения.

9.1.5 Аппаратный уровень: карточки тахографа

CSM_83 Для каждой карточки тахографа генерируется одна уникальная пара ключей ECC, обозначаемая как Card_MA. Для каждой карточки водителя и каждой карточки мастерской также дополнительно генерируется пара ключей ECC, обозначаемая как Card_Sign. Эту задачу могут выполнять производители или персонализаторы карточек. При генерировании пары ключей карточки сторона, генерирующая ключ, передаёт открытый ключ MSCA страны, в которой она проживает, чтобы получить соответствующий сертификат карточки, подписанный MSCA. Закрытый ключ использует только карточка тахографа.

CSM_84 У сертификатов Card_MA и Card_Sign определённой карточки водителя или мастерской одна и та же дата срока действия сертификата.

CSM_85 Производитель или персонализатор карточки выбирает силу пары ключей карточки, которая была бы равна силе пары ключей MSCA, используемых для подписания соответствующего сертификата карточки.

CSM_86 Карточка тахографа использует свою пару ключей Card_MA, состоящую из закрытого ключа Card_MA.SK и открытого ключа Card_MA.PK, исключительно для взаимной аутентификации и согласования сеансовых ключей относительно бортовых устройств, как указано в разделах 10.3 и 10.4 настоящего приложения.

CSM_87 Карточка водителя или мастерской использует закрытый ключ Card_Sign.SK своей пары ключей Card_Sign исключительно для загрузки файлов данных, как указано в главе 14 настоящего приложения. Соответствующий открытый ключ Card_Sign.PK используется исключительно для проверки подписей, созданных карточкой.

CSM_88 Срок действия сертификата Card_MA таков:
- Карточки водителя: 5 лет
- Карточки предприятия: 2 года
- Контрольные карточки: 2 года
- Карточки мастерской: 1 год

CSM_89 Срок действия сертификата Card_Sign таков:
- Карточки водителя: 5 лет и 1 месяц
- Карточки мастерской: 1 год и 1 месяц

Примечание: продлённый срок действия сертификата Card_Sign позволяет карточке водителя создавать действительные подписи через загружаемые данные в течение первого месяца после его истечения. Это необходимо в соответствии с Регламентом (ЕС) № 581/2010, который требует, чтобы загрузку данных с карточки водителя можно было произвести в течение периода до 28 дней после записи последних данных.

CSM_90 После выпуска карточки пары ключей и соответствующие сертификаты данной карточки тахографа не меняются или не возобновляются.

CSM_91 После выпуска карточки тахографа содержат следующие криптографические ключи и сертификаты:
- Закрытый ключ Card_MA и соответствующий сертификат
- Дополнительно для карточек водителя и мастерской: закрытый ключ Card_Sign и соответствующий сертификат
- Сертификат MSCA_Card, содержащий открытый ключ MSCA_Card.PK для проверки сертификата Card_MA и сертификата Card_Sign
- Сертификат EUR, содержащий открытый ключ EUR.PK, для проверки сертификата MSCA_Card

- Сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_Card, если таковой существует
- Связующий сертификат, соединяющий эти два сертификата EUR, если таковые существуют

CSM_92 Помимо криптографических ключей и сертификатов, перечисленных в CSM_91, на карточках тахографа также есть ключи и сертификаты, указанные в части A настоящего приложения, позволяющие таким карточкам вступать во взаимодействие с бортовыми устройствами первого поколения.

9.1.6 Аппаратный уровень: внешние устройства ГНСС

CSM_93 Для каждого внешнего устройства ГНСС генерируется одна уникальная пара ключей ECC, обозначаемая как EGF_MA. Эту задачу выполняют производители внешних устройств ГНСС. При генерировании пары ключей EGF_MA открытый ключ передаётся MSCA страны проживания, чтобы получить соответствующий сертификат EGF_MA, подписанный MSCA. Закрытый ключ использует только внешнее устройство ГНСС.

CSM_94 Производитель EGF выбирает силу пары ключей EGF_MA, которая была бы равна силе пары ключей MSCA, используемых для подписания соответствующего сертификата EGF_MA.

CSM_95 Внешнее устройство ГНСС использует свою пару ключей EGF_MA, состоящую из закрытого ключа EGF_MA.SK и открытого ключа EGF_MA.PK, исключительно для взаимной аутентификации и согласования сеансовых ключей относительно бортовых устройств, как указано в разделах 11.4 и 11.4 настоящего приложения.

CSM_96 Срок действия сертификата EGF_MA составляет 15 лет.

CSM_97 С момент истечения срока действия соответствующего сертификата внешнее устройство ГНСС не использует закрытый ключ пары ключей EGF_MA для соединения с бортовым устройством.

Примечание: как поясняется в разделе 11.3.3, EGF может использовать свой закрытый ключ для взаимной аутентификации относительно БУ, с которым оно уже соединено, даже после истечения срока действия соответствующего сертификата.

CSM_98 После начала эксплуатации EGF пара ключей EGF_MA и соответствующий сертификат данного внешнего устройства ГНСС на месте не заменяются или не возобновляются.

Примечание: Данное требование не исключает возможности замены статичных пар ключей EGF во время реконструкции или ремонта в защищённой среде, контролируемой производителем EGF.

CSM_99 После ввода в эксплуатацию внешнее устройство ГНСС содержит следующие криптографические ключи и сертификаты:
- Закрытый ключ EGF_MA и соответствующий сертификат
- Сертификат MSCA_VU-EGF, содержащий открытый ключ MSCA_VU-EGF.PK для проверки сертификата EGF_MA
- Сертификат EUR, содержащий открытый ключ EUR.PK, для проверки сертификата MSCA_VU-EGF
- Сертификат EUR, срок действия которого непосредственно предшествует сроку действия сертификата EUR, используемого для проверки сертификата MSCA_VU-EGF, если таковой существует
- Связующий сертификат, соединяющий эти два сертификата EUR, если таковые существуют

9.1.7 Обзор: замена сертификата

На Рисунок 1 ниже показано, как выпускаются и с течением времени используются корневые сертификаты ERCA различных поколений, связующие сертификаты ERCA, сертификаты MSCA и сертификаты оборудования (БУ и карточки):

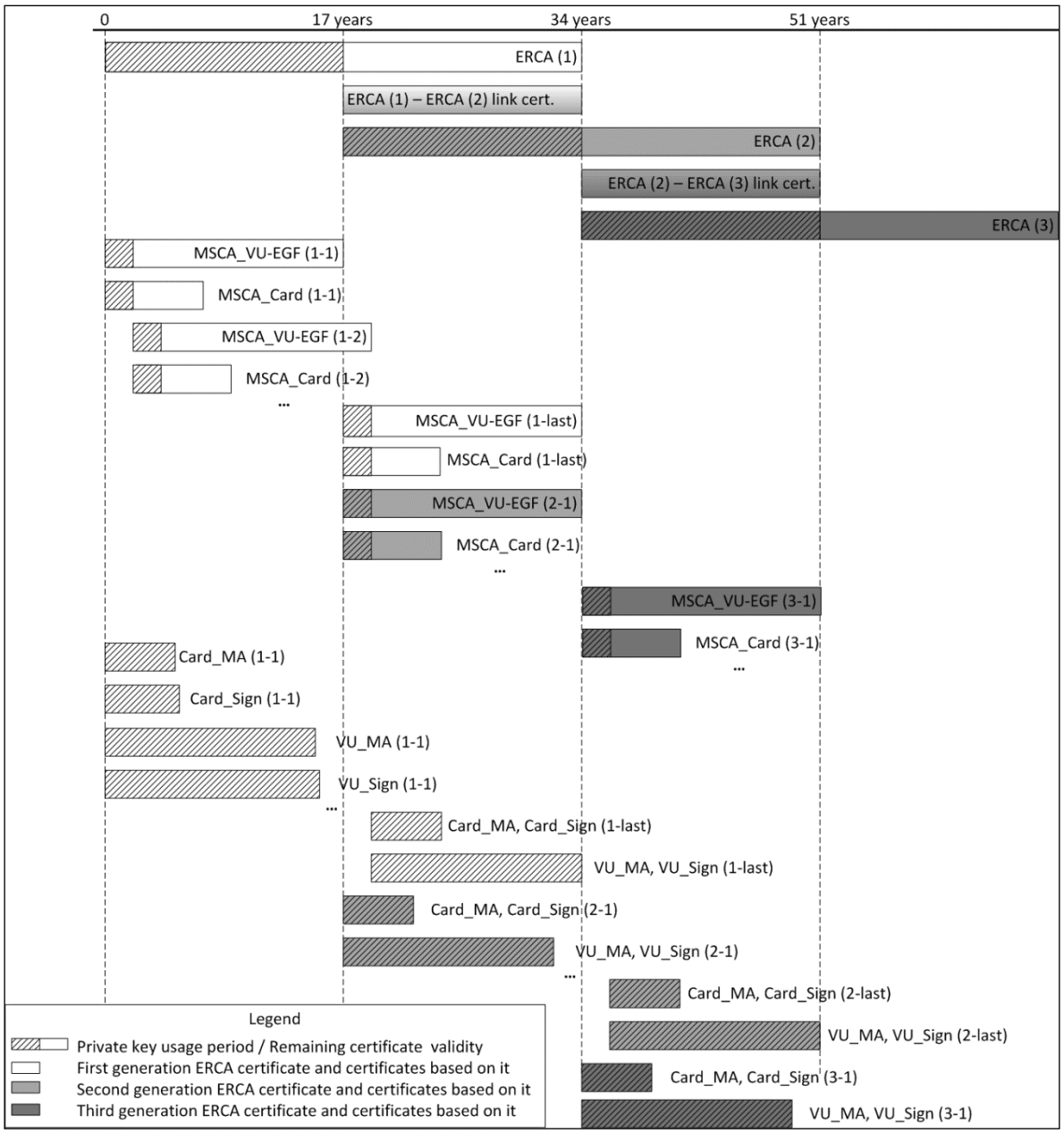


Рисунок 1 Выпуск и использование корневых сертификатов ERCA различных поколений, связующих сертификатов ERCA, сертификатов MSCA и сертификатов оборудования

Примечания к Рисунок 1:

1. Разные поколения корневого сертификата обозначены цифрой в скобках. Например, ERCA (1) означает корневой сертификат ERCA первого поколения; ERCA (2) – сертификат второго поколения и т.д.
2. Другие сертификаты помечаются двумя цифрами в скобках, первая из которых указывает на поколение выпуска корневого сертификата, а вторая – на поколение самого сертификата. Например, MSCA_Card (1-1) – это первый сертификат MSCA_Card, выпущенный в рамках ERCA (1); MSCA_Card (2-1) – первый сертификат MSCA_Card, выпущенный в рамках ERCA (2); MSCA_Card (2-last) – последний сертификат MSCA_Card, выпущенный в рамках ERCA (2); Card_MA(2-1) – первый сертификат карточки для взаимной аутентификации, выпущенный в рамках ERCA (2), и т.д.
3. Сертификаты MSCA_Card (2-1) и MSCA_Card (1-last) выпускаются почти в тот же день, но не совсем. MSCA_Card (2-1) – первый сертификат MSCA_Card, выпускаемый в рамках ERCA (2), будет выпущен немного позднее, чем MSCA_Card (1-last), последний сертификат MSCA_Card, выпускаемый в рамках ERCA (1).

4. Как показано на рисунке, первые сертификаты БУ и карточки, выпускаемые в рамках ERCA (2), появятся почти за два года до последних сертификатов БУ и карточки, выпускаемых в рамках ERCA (1). Это связано с тем, что сертификаты БУ и карточки выпускаются по сертификату MSCA, а не непосредственно по сертификату ERCA. Сертификат MSCA (2-1) выдаётся непосредственно после вступления в силу ERCA (2), а сертификат MSCA (1-last) выдаётся лишь незадолго до того времени, в последний момент, когда сертификат ERCA (1) ещё действителен. Таким образом, срок действия этих двух сертификатов MSCA почти одинаковый, несмотря на то, что они принадлежат к разным поколениям.
5. Срок действия, указываемый в отношении карточек, – это срок действия карточек водителей (5 лет).
6. Ради экономии места разница в сроках действия между сертификатами Card_MA и Card_Sign и между сертификатами VU_MA и VU_Sign отображается только в отношении первого поколения.

9.2. Симметричные ключи

9.2.1 Ключи для обеспечения связи между БУ и датчиком движения

9.2.1.1 Общие положения

Примечание: предполагается, что читатели данного раздела знакомы с содержанием [ISO 16844-3], описывающего интерфейс между бортовым устройством и датчиком движения. Процесс соединения между БУ и датчиком движения подробно описан в главе 12 настоящего приложения.

CSM_100 Для соединения бортовых устройств и датчиков движения, для взаимной аутентификации между бортовыми устройствами и датчиками движения и для шифрования связи между бортовыми устройствами и датчиками движения необходим ряд симметричных ключей, как показано в Таблица 3. Все эти ключи – ключи AES, длина которых равна длине ключа старшего порядка датчиков движения, связанного с длиной (планируемой) пары европейских корневых ключей, как описано в CSM_50.

Ключ	**Символ**	**Кем/чем генерируется**	**Метод генерирования**	**Где хранится**
Ключ старшего порядка датчика движения – часть БУ	$K_{M\text{-}VU}$	ERCA	Случайный	ERCA, MSCA, участвующие в выпуске сертификатов БУ, производители БУ, бортовые устройства
Ключ старшего порядка датчика движения – часть мастерской	$K_{M\text{-}WC}$	ERCA	Случайный	ERCA, MSCA, производители карточек, карточки мастерской
Ключ старшего порядка датчика движения	K_M	Самостоятельно не генерируется	Вычисляется как $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA, MSCA, участвующие в выдаче ключей датчиков движения (факультативно)*
Идентификационный ключ	K_{ID}	Самостоятельно не генерируется	Вычисляется как $K_{ID} = K_M$ XOR CV (CV описывается в CSM_106)	ERCA, MSCA, участвующие в выдаче ключей датчиков движения (факультативно)*
Ключ соединения	K_P	Производитель датчика движения	Случайный	Один датчик движения
Сеансовый ключ	K_S	БУ (во время соединения БУ и датчика движения)	Случайный	Одно БУ и один датчик движения

Таблица 3 Ключи для обеспечения связи бортового устройства и датчика движения

*Хранение K_M и K_{ID} факультативно, так как эти ключи можно извлечь из K_{M-VU}, K_{M-WC} и CV.

CSM_101 Европейский сертификационный орган (ERCA) генерирует K_{M-VU} и K_{M-WC}, два случайных и уникальных ключей AES, по которым ключ старшего порядка датчика движения K_M можно вычислить как K_{M-VU} XOR K_{M-WC}. ERCA передаёт K_M, K_{M-VU} и K_{M-WC} сертификационным органам государств-членов по их просьбе.

CSM_102 Каждому ключу старшего порядка датчика движения K_M ERCA присваивает уникальный номер версии, который также используется для составления ключей K_{M-VU} и K_{M-WC} и для связанного с ними идентификационного ключа K_{ID}. ERCA сообщает MSCA о номере версии, когда отправляет им K_{M-VU} и K_{M-WC}.

Примечание: Номер версии используется для различения разных поколений этих ключей, как подробно поясняется в разделе 9.2.1.2.

CSM_103 Сертификационный орган государства-члена передаёт K_{M-VU} вместе с номером его версии производителям бортового устройства по их просьбе. Производители БУ включают K_{M-VU} и номер его версии во все изготавливаемые БУ.

CSM_104 Сертификационный орган государства-члена заботится о том, чтобы K_{M-WC} вместе с номером его версии был включён в каждую карточку мастерской, выдаваемую в сфере его ответственности.

Примечания:
- См. описание типа данных `SensorInstallationSecData` в приложении 2.
- Как поясняется в разделе 9.2.1.2, на одну карточку мастерской фактически может быть необходимо поместить несколько поколений K_{M-WC}.

CSM_105 Помимо ключа AES, указанного в CSM_104, MSCA заботится о том, чтобы ключ TDES Km_{WC}, указанный в требовании CSM_037 в части A настоящего приложения, был помещён на каждую карточку мастерской, выдаваемую в сфере его ответственности.

Примечания:
- Это позволяет использовать карточку мастерской второго поколения для соединения БУ первого поколения.
- На карточке мастерской второго поколения содержатся два разных приложения, одно из которых соответствует части Б настоящего приложения, а второе – части А. Последнее хранит в себе ключ TDES Km_{WC}.

CSM_106 MSCA, участвующий в выпуске датчиков движения, извлекает идентификационный ключ из ключа старшего порядка датчика движения при помощи XOR и постоянного вектора CV. Значение CV:
- В случае 128-битных ключей старшего порядка датчика движения: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’
- В случае 192-битных ключей старшего порядка датчика движения: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’
- В случае 256-битных ключей старшего порядка датчика движения: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Примечание: постоянные векторы генерируются следующим образом:
Pi_10 = первые 10 байтов десятичной доли математической константы π = ‘24 3F 6A 88 85 A3 08 D3 13 19’
CV_128-bits = первые 16 байтов SHA-256(Pi_10)
CV_192-bits = первые 24 байта SHA-384(Pi_10)
CV_256-bits = первые 32 байта SHA-512(Pi_10)

CSM_107 Производители датчиков движения генерируют случайный и уникальный ключ соединения K_P для каждого датчика движения и передают все ключи соединения сертификационному органу государства-члена. MSCA шифрует каждый ключ соединения отдельно с ключом старшего порядка датчика движения K_M и возвращает зашифрованный ключ производителю датчика движения. В отношении каждого зашифрованного ключа MSCA сообщает производителю датчиков движения номер версии соответствующего K_M.

Примечание: как поясняется в разделе 9.2.1.2, производитель датчиков движения фактически может быть вынужден генерировать множество уникальных ключей соединения для одного датчика движения.

CSM_108 Производители датчиков движения генерируют уникальный серийный номер для каждого датчика движения и передают все серийные номера сертификационному органу государства-члена. MSCA шифрует каждый серийный номер отдельно с идентификационным ключом K_{ID} и возвращает зашифрованный серийный номер производителю датчика движения. В отношении каждого зашифрованного серийного номера MSCA сообщает производителю датчиков движения номер версии соответствующего K_{ID}.

CSM_109 Что касается требований CSM_107 и CSM_108, MSCA использует алгоритм AES в режиме сцепления криптоблоков, как описано [ISO 10116], с параметром чередования $m = 1$ и вектором инициализации SV = ‘00’ {16}, т.е. шестнадцать байтов с двоичным значением, равным 0. При необходимости MSCA использует метод заполнения 2, описанный в [ISO 9797-1].

CSM_110 Производитель датчиков движения хранит зашифрованный ключ соединения и зашифрованный серийный номер на соответствующем датчике движения, вместе с соответствующими значениями в формате простого текста и номером версии K_M и K_{ID}, используемых для шифрования.

Примечание: как поясняется в разделе 9.2.1.2, производитель датчиков движения фактически может быть вынужден включить множество зашифрованных ключей соединения и множество зашифрованных серийных номеров в один датчик движения.

CSM_111 Помимо криптографического материала на базе AES, как описано в CSM_110, производитель датчиков движения в каждом датчике движения может также хранить криптографический материал на базе TDES, как указано в требовании CSM_037 в части A настоящего приложения.

Примечание: таким образом датчик движения второго поколения можно будет соединить с БУ первого поколения.

CSM_112 Длина сеансового ключа K_S, генерируемого БУ во время подсоединения к датчику движения, связана с длиной его $K_{M\text{-}VU}$, как описано в CSM_50.

9.2.1.2 Замена ключа старшего порядка датчика движения в оборудовании второго поколения

CSM_113 Каждый ключ старшего порядка датчика движения и все соответствующие ключи (см. Таблица 3) связаны с определённым поколением пары корневых ключей ERCA. Так, эти ключи заменяются каждые 17 лет. Срок действия каждого поколения ключей старшего порядка датчиков движения начинается за год до вступления в силу соответствующей пары корневых ключей ERCA и кончается, когда истекает срок действия соответствующей пары корневых ключей ERCA. Это показано на Рисунок 2.

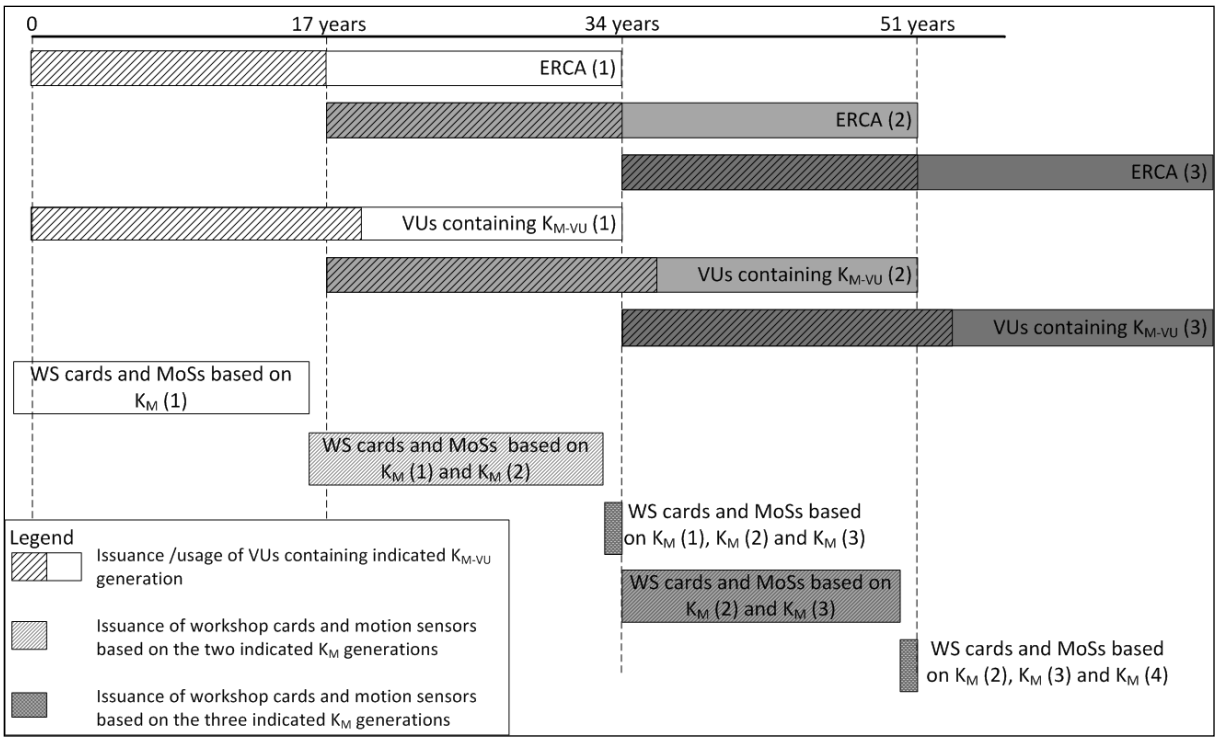


Рисунок 2 Выпуск и использование разных поколений ключей старшего порядка датчиков движения в бортовых устройствах, датчиках движения и на карточках мастерской

CSM_114 По крайней мере, за один год до генерирования новой пары европейских корневых ключей, как описано в CSM_56, ERCA генерирует новый ключ старшего порядка датчика движения K_M посредством генерирования новых $K_{M\text{-}VU}$ и $K_{M\text{-}WC}$. Длина ключа старшего порядка датчика движения связана с установленным уровнем силы новой пары европейских корневых ключей, в соответствии с CSM_50. ERCA передаёт новые K_M, $K_{M\text{-}VU}$ и $K_{M\text{-}WC}$ MSCA по его просьбе вместе с номером версии.

CSM_115 MSCA заботится о том, чтобы все действительные поколения $K_{M\text{-}WC}$ хранились на каждой карточке мастерской, выпущенной в сфере его ответственности, вместе с номерами их версий, как показано на Рисунок 2.

Примечание: это значит, что в последний год срока действия сертификата ERCA карточки мастерской выдаются с $K_{M\text{-}WC}$ трёх разных поколений, как показано на Рисунок 2.

CSM_116 Что касается процесса, описанного выше в CSM_107 и CSM_108: MSCA шифрует каждый ключ соединения K_P, который он получает от производителя датчиков движения, отдельно для каждого действительного поколения ключа старшего порядка датчика движения K_M. MSCA также шифрует каждый серийный номер, который он получает от производителя датчиков движения, отдельно для каждого действительного поколения идентификационного ключа K_{ID}. Производитель датчиков движения хранит все версии зашифрованного ключа соединения и все версии зашифрованного серийного номера на соответствующем датчике движения, вместе с соответствующими значениями в формате простого текста и номером (-ами) версии K_M и K_{ID}, используемых для шифрования.

Примечание: это значит, что в последний год срока действия сертификата ERCA датчики движения выдаются с зашифрованными данными на основе K_M трёх разных поколений, как показано на Рисунок 2.

CSM_117 Что касается процесса, описанного выше в CSM_107: Поскольку длина ключа соединения K_P связана с длиной K_M (см. CSM_100), производитель датчика движения может быть вынужден генерировать до трёх различных ключей соединения (различной длины) для одного датчика движения в случае, если у последующих поколений K_M разная длина. В подобном случае производитель передаёт MSCA каждый ключ соединения. MSCA заботится о том, чтобы каждый ключ соединения был зашифрован при правильном генерировании ключа старшего порядка датчика движения, т.е. ключа такой же длины.

Примечание: Если производитель датчика движения решает генерировать ключ соединения на базе TDES для датчика движения второго поколения (см. CSM_111), производитель указывает MSCA, что ключ старшего порядка датчика движения на базе TDES должен использоваться для шифрования данного ключа соединения. Это связано с тем, что длина ключа TDES может быть равна длине ключа AES, так что MSCA не может ориентироваться лишь на длину ключа.

CSM_118 Производители бортовых устройств в каждое бортовое устройство включают лишь одно поколение K_{M-VU} вместе с номером версии. Такое генерирование K_{M-VU} связано с сертификатом ERCA, на который опираются сертификаты БУ.

Примечания:

- В бортовое устройство, основанное на сертификате ERCA поколения *X*, вводится только K_{M-VU} поколения *X*, даже если оно выпускается после начала срока действия сертификата ERCA поколения *X+1*. Это показано на Рисунок 2.
- БУ поколения *X* нельзя подсоединять к датчику движения поколения *X-1*.
- Поскольку карточки мастерской действительны в течение года, согласно CSM_113-CSM_118 все карточки мастерской будут содержать новый K_{M-WC} в момент выпуска первого БУ, содержащего новый K_{M-VU}. Таким образом, такой БУ всегда сможет вычислить новый $K_{M.}$ Кроме того, к тому времени большинство новых датчиков движения также будут содержать зашифрованные данные на основе нового K_M.

9.2.2 Ключи для обеспечения связи DSRC

9.2.2.1 Общие положения

CSM_119 Подлинность и конфиденциальность данных, передающихся из бортового устройства контрольному органу через канал удалённой связи DSRC, обеспечиваются при помощи ряда ключей AES, конкретно связанных с БУ, полученных на основе единого ключа старшего порядка DSRC KM_{DSRC}.

CSM_120 Ключ старшего порядка DSRC KM_{DSRC} – это ключ AES, который в защищённом виде генерирует, хранит и распространяет ERCA. Длина ключа может быть 128, 192 или 256 бит и связана с длиной пары европейских корневых ключей, как описано в CSM_50.

CSM_121 ERCA передаёт ключ старшего порядка DSRC сертификационным органам государства-члена по их просьбе в защищённом виде, чтобы они могли извлечь ключи DSRC, конкретно связанные с БУ, и позаботиться о том, чтобы ключ старшего порядка DSRC был помещён на все контрольные карточки и карточки мастерской, выданные в сфере их ответственности.

CSM_122 Каждому ключу старшего порядка DSRC ERCA присваивает уникальный номер версии. ERCA сообщает MSCA о номере версии, когда отправляет им ключ старшего порядка DSRC.

Примечание: Номер версии используется для различения разных поколений ключей старшего порядка DSRC, как подробно поясняется в разделе 9.2.2.2.

CSM_123 Для каждого бортового устройства производитель бортовых устройств создаёт уникальный серийный номер БУ и передаёт его сертификационному органу своего государства-члена с заявкой на получение набора из двух ключей DSRC, связанных с конкретным БУ. Серийный номер БУ содержит тип данных `VuSerialNumber`, а для кодирования применяются особые правила кодирования (DER) в соответствии с [ISO 8825-1].

CSM_124 По получении заявки на ключи DSRC, связанные с конкретным БУ, MSCA производит два ключа AES для бортового устройства, обозначаемые как K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC. Длина этих ключей для конкретного БУ такая же, как длина ключа старшего порядка DSRC. MSCA использует функцию создания ключей, описанную в [RFC 5869]. Хеш-функция, необходимая для обработки хеш-функции HMAC, связана с длиной ключа старшего порядка DSRC, как описано в CSM_50. Функция создания ключей в [RFC 5869] используется следующим образом:
Этап 1 (извлечение):

- *PRK* = HMAC-Hash (*salt, IKM*), где *salt* – это пустая строка ‘’, а *IKM* – это KM_{DSRC}.

Этап 2 (расширение):

- *OKM* = *T(1)*, где
  T(1) = HMAC-Hash (*PRK, T(0)* || *info* || ‘01’) с
    - *T(0)* = пустая строка (‘’)
    - *info* = серийный номер БУ, как указано в CSM_123
- K_VU_{DSRC}_ENC = первые *L* октеты *OKM* и
  K_VU_{DSRC}_MAC = последние *L* октеты *OKM,*
  где *L* – это требуемая длина K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC в октетах.

CSM_125 MSCA распределяет K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC в защищённом виде производителю БУ для ввода в соответствующее бортовое устройство.

CSM_126 При выпуске на бортовом устройстве в защищённом блоке памяти уже есть K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC, чтобы оно было в состоянии обеспечить целостность, подлинность и конфиденциальность данных, передаваемых через канал удалённой связи. Бортовое устройство также хранит номер версии ключа старшего порядка DSRC, используемого для выведения этих ключей для конкретного БУ.

CSM_127 При выпуске на контрольных карточках и карточках мастерской в защищённом блоке памяти уже есть KM_{DSRC}, чтобы они были в состоянии обеспечить целостность и подлинность данных, передаваемых БУ через канал удалённой связи, и расшифровать эти данные. На контрольных карточках и карточках мастерской также хранится номер версии ключа старшего порядка DSRC.

Примечание: как поясняется в разделе 9.2.2.2, на одну карточку мастерской или контрольную карточку фактически может быть необходимо поместить несколько поколений K_{DSRC}.

CSM_128 MSCA хранит записи обо всех составленных им ключах DSRC конкретных БУ, номере их версий и идентификационных данных БУ, для которого предназначен каждый набор ключей.

9.2.2.2 Замена ключа старшего порядка DSRC

CSM_129 Каждый ключ старшего порядка DSRC связан с определённым поколением пары корневых ключей ERCA. Таким образом, ERCA заменяет ключ старшего порядка DSRC каждые 17 лет. Срок действия каждого поколения ключей старшего порядка DSRC начинается за два года до вступления в силу соответствующей пары корневых ключей ERCA и кончается, когда истекает срок действия соответствующей пары корневых ключей ERCA. Это показано на Рисунок 3.

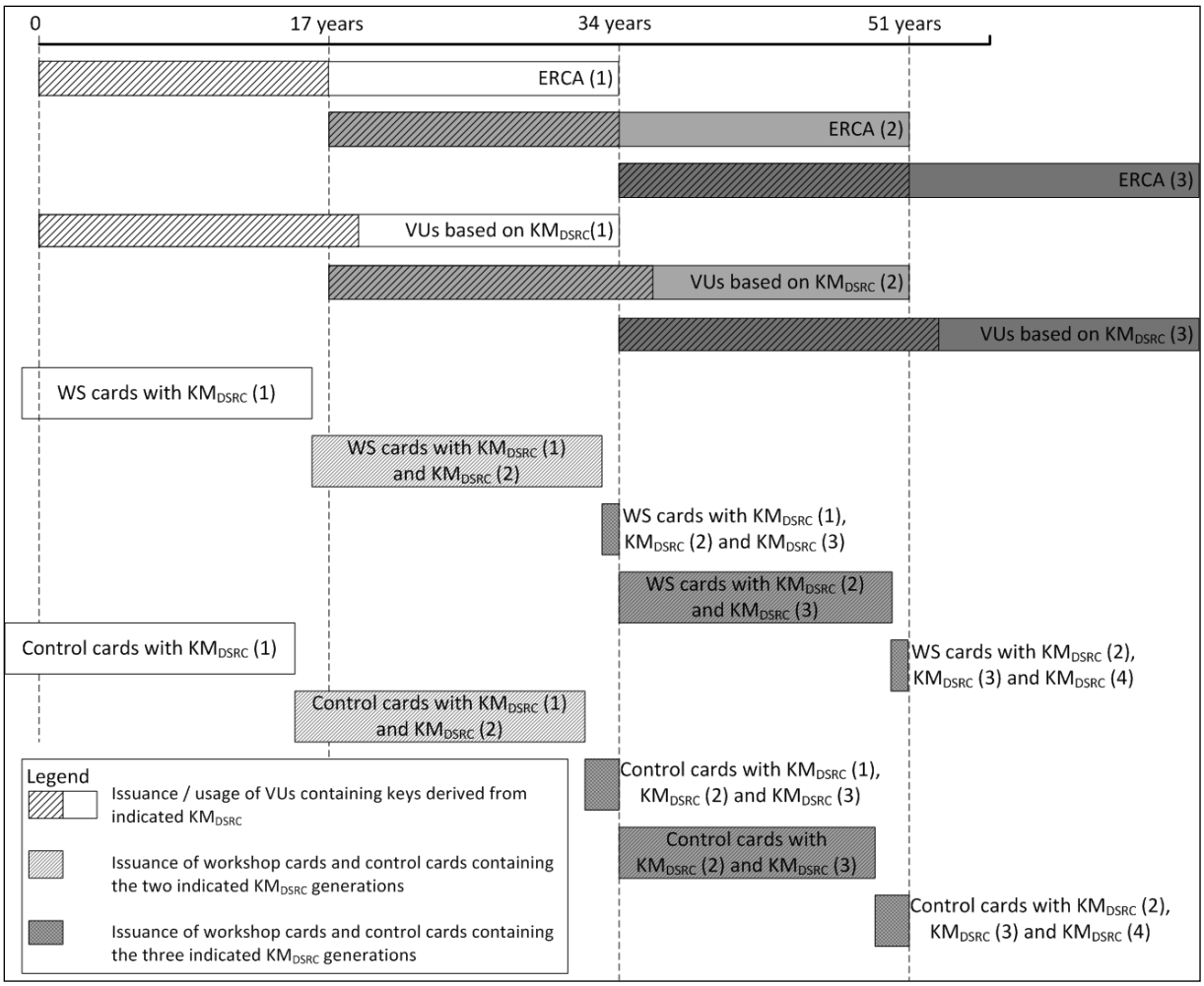


Рисунок 3 Выпуск и использование разных поколений ключей старшего порядка DSRC в бортовых устройствах, на карточках мастерской и на контрольных карточках

CSM_130 По крайней мере, за два года до генерирования новой пары европейских корневых ключей, как описано в CSM_56, ERCA генерирует новый ключ старшего порядка DSRC. Длина ключа DSRC связана с установленным уровнем силы новой пары европейских корневых ключей, в соответствии с CSM_50. ERCA передаёт новые ключ старшего порядка DSRC MSCA по его просьбе вместе с номером версии.

CSM_131 MSCA заботится о том, чтобы все действительные поколения KM_{DSRC} хранились на каждой контрольной карточке, выпущенной в сфере его ответственности, вместе с номерами их версий, как показано на Рисунок 3.

Примечание: это значит, что в последние два года срока действия сертификата ERCA карточки мастерской выдаются с KM_{DSRC} трёх разных поколений, как показано на Рисунок 3.

CSM_132 MSCA заботится о том, чтобы все поколения KM_{DSRC}, действительные хотя бы в течение года и всё ещё действительные, хранились на каждой карточке мастерской, выпущенной в сфере его ответственности, вместе с номерами их версий, как показано на Рисунок 3.

Примечание: это значит, что в последний год срока действия сертификата ERCA карточки мастерской выдаются с KM_{DSRC} трёх разных поколений, как показано на Рисунок 3.

CSM_133 Производители бортовых устройств в каждое бортовое устройство включают лишь один набор ключей DSRC, связанных с конкретным БУ, вместе с номером версии. Такой набор ключей выводится на основе поколения KM_{DSRC}, связанного с сертификатом ERCA, на основании которого выдаются сертификаты БУ.

Примечания:

- Это значит, что в бортовое устройство, основанное на сертификате ERCA поколения *X*, вводится только K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC поколения *X*, даже если БУ выпускается после начала срока действия сертификата ERCA поколения X+1. Это показано на Рисунок 3.
- Поскольку карточки мастерской действительны в течение года, а контрольные карточки – двух лет, согласно CSM_131-CSM_133 все карточки мастерской и контрольные карточки будут содержать новый ключ старшего порядка DSRC в момент выпуска первого БУ, содержащего конкретно с ним связанные ключи, основанные на том ключе старшего порядка.

9.3. Сертификаты

9.3.1 Общие положения

CSM_134 Все сертификаты европейской системы «умных» тахографов являются самодокументирующимися сертификатами, поддающимися проверке по карточке (CV), в соответствии с [ISO 7816-4] и [ISO 7816-8].

CSM_135 Для кодирования структур данных ASN.1 и (связанных с конкретным приложением) объектов данных в сертификатах применяются особые правила кодирования (DER) в соответствии с [ISO 8825-1].

Примечание: такое кодирование приводит к следующей структуре значения длины метки (TLV):

- Метка: Метка кодируется одним или двумя октетами и указывает на содержание.
- Длина: Длина кодируется как неподписанное целое число одним, двумя или тремя октетами, что приводит к максимальной длине 65535 октетов. Используется минимальное число октетов.
- Значение: Значение кодируется в виде нуля или более октетов.

9.3.2 Содержание сертификатов

CSM_136 Структура всех сертификатов такова, как показано в описании сертификата в Таблица 4.

Поле	**ИД поля**	**Метка**	**Длина (байты)**	**Тип данных ASN.1 (см. приложение 1)**
Сертификат ECC	C	‘7F 21’	var	
Сертификационный орган ECC	B	‘7F 4E’	var	
Идентификатор описания сертификата	CPI	‘5F 29’	‘01’	INTEGER(0..255)
Указатель сертифицирующего органа	CAR	‘42’	‘08’	KeyIdentifier
Полномочия держателя сертификата	CHA	‘5F 4C’	‘07’	CertificateHolder Authorisation
Открытый ключ	PK	‘7F 49’	var	
Параметры области	DP	‘06’	var	OBJECT IDENTIFIER
Открытая точка	PP	‘86’	var	OCTET STRING
Указатель держателя сертификата	CHR	‘5F 20’	‘08’	KeyIdentifier
Дата вступления сертификата в силу	CEfD	‘5F 25’	‘04’	TimeReal
Дата истечения срока действия сертификата	CExD	‘5F 24’	‘04’	TimeReal
Подпись сертификата ECC	S	‘5F 37’	var	OCTET STRING

Таблица 4 Описание сертификата, версия 1

Примечание: ИД поля применяется в последующих разделах настоящего приложения, чтобы указать на отдельные поля сертификата, например, X.CAR – это указатель сертифицирующего органа, отмеченного в сертификате пользователя X.

9.3.2.1 Идентификатор описания сертификата

CSM_137 В сертификатах идентификатор описания сертификата используется для указания на описание сертификата, взятое за основу. Версия 1, как указано в Таблица 4, обозначается значением ‘00’.

9.3.2.2 Указатель сертифицирующего органа

CSM_138 Указатель сертифицирующего органа используется для обозначения открытого ключа, который должен применяться для проверки подписи сертификата. Таким образом, указатель сертифицирующего органа в сертификате соответствующего сертификационного органа равен указателю держателя сертификата.

CSM_139 Корневой сертификат ERCA самоподписывающийся, т.е. указатель сертифицирующего органа и указатель держателя сертификата в сертификате равны.

CSM_140 Что касается связующего сертификата ERCA, указатель держателя сертификата равен CHR нового корневого сертификата ERCA. Указатель сертифицирующего органа в связующем сертификате равен CHR прежнего корневого сертификата ERCA.

9.3.2.3 Полномочия держателя сертификата

CSM_141 Полномочия держателя сертификата используются для определения типа сертификата. Они состоят из шести наиболее значимых байтов ИД приложения тахографа в конкатенации с типом оборудования, для которого предназначен сертификат.

9.3.2.4 Открытый ключ

Открытый ключ включает в себя два элемента данных: стандартизированные параметры области, используемые с открытым ключом в сертификате, и значение открытой точки.

CSM_142 Элемент данных параметров области содержит один из идентификаторов объектов, указанных в Таблица 1, чтобы указать на набор стандартизированных параметров области.

CSM_143 Элемент данных открытой точки содержит в себе открытую точку. Открытые точки эллиптической кривой конвертируются в октетные строки, как указано в [TR-03111]. Используется несжатый формат кодирования. При восстановлении точки эллиптической кривой из кодированного формата всегда проводятся проверки, описанные в [TR-03111].

9.3.2.5 Указатель держателя сертификата

CSM_144 Указатель держателя сертификата – это идентификатор открытого ключа, представленного в сертификате. Он используется для указания этого открытого ключа на других сертификатах.

CSM_145 В случае сертификатов карточек и сертификатов внешних устройств ГНСС указатель держателя сертификата содержит тип данных `ExtendedSerialNumber`, указанный в приложении 1.

CSM_146 В отношении бортовых устройств производитель, подавая заявку на сертификат, необязательно знает серийный номер БУ производителя, для которого предназначен сертификат и связанный с ним закрытый ключ. Если номер производителю известен, указатель держателя сертификата содержит тип данных `ExtendedSerialNumber`, указанный в приложении 1. Если номер производителю известен, указатель держателя сертификата содержит тип данных `CertificateRequestID`, указанный в приложении 1.

CSM_147 В случае сертификатов ERCA и MSCA указатель держателя сертификата содержит тип данных `CertificationAuthorityKID`, указанный в приложении 1.

9.3.2.6 Дата вступления сертификата в силу

CSM_148 Дата вступления сертификата в силу указывает на дату и время начала периода действительности сертификата. Это дата поколения сертификата.

9.3.2.7 Дата истечения срока действия сертификата

CSM_149 Дата истечения срока действия сертификата указывает на дату и время конца периода действительности сертификата.

9.3.2.8 Подпись сертификата

CSM_150 Подпись на сертификате создаётся через закодированную основную часть сертификата, включая метку и длину основной части сертификата. Алгоритм подписи – ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа подписывающего органа, как указано в CSM_50. Формат подписи простой, как указано в [TR-03111].

9.3.3 Заявки на сертификаты

CSM_151 При подаче заявки на сертификат заявитель передаёт своему сертификационному органу следующие данные:

- Идентификатор описания соответствующего сертификата
- Указатель сертифицирующего органа, в который планируется обратиться за подписью сертификата.
- Открытый ключ, подлежащий подписи

CSM_152 Помимо данных в CSM_151, MSCA передаёт следующие данные в заявке на сертификат ERCA, что позволяет ERCA сформировать указатель держателя сертификата для нового сертификата MSCA:

- Цифровой код государства сертификационного органа (тип данных `NationNumeric`, определённый в приложении 1)
- Буквенно-цифровой код государства сертификационного органа (тип данных `NationAlpha`, определённый в приложении 1)
- 1-байтовый серийный номер, позволяющий проводить различие между различными ключами сертификационного органа в случае изменения ключей
- Двухбайтовое поле, содержащее конкретную дополнительную информацию о сертификационном органе

CSM_153 Помимо данных в CSM_151, производитель оборудования передаёт следующие данные в заявке на сертификат MSCA, что позволяет MSCA сформировать указатель держателя сертификата для нового сертификата оборудования:

- Идентификатор типа оборудования конкретного производителя
- Если известен (см. CSM_154), серийный номер оборудования, уникальный для данного производителя, типа оборудования и месяц изготовления. В противном случае, уникальный идентификатор заявки на сертификат.
- Месяц и год изготовления оборудования или заявки на сертификат.

Производитель заботится о том, чтобы эта дата была правильной и чтобы выданный MSCA сертификат был введён в оборудование, для которого он предназначен.

CSM_154 В отношении БУ производитель, подавая заявку на сертификат, необязательно знает серийный номер БУ производителя, для которого предназначен сертификат и связанный с ним закрытый ключ. Если серийный номер известен, производитель БУ передаёт его MSCA. Если он неизвестен, производитель присваивает уникальный идентификатор каждой заявке на сертификат и передаёт этот серийный номер заявки MSCA. Выданный впоследствии сертификат будет содержать серийный номер заявки на сертификат. После ввода сертификата в соответствующее БУ производитель передаёт MSCA связь между серийным номером заявки на сертификат и идентификационными данными БУ.

10. Взаимная аутентификация БУ и карточки и защищённый обмен сообщениями

10.1. Общие положения

CSM_155 На высоком уровне защищённая связь между бортовым устройством и карточкой тахографа осуществляется следующими этапами:

- Во-первых, каждая сторона доказывает другой наличие у неё действительного сертификата открытого ключа, подписанного сертификационным органом государства-члена. Сертификат открытого ключа MSCA в свою очередь должен быть подписан европейским сертификационным органом. Данный этап называется проверкой цепочки сертификата и подробно рассматривается в разделе 10.2
- Во-вторых, бортовое устройство доказывает карточке наличие у него закрытого ключа, соответствующего открытому ключу в представленном сертификате. Это происходит путём подписания случайного числа, отправленного карточкой. Карточка проверяет подпись случайного числа. Если проверка выполнена успешно, происходит аутентификация БУ. Данный этап называется аутентификацией БУ и подробно рассматривается в разделе 10.3.
- В-третьих, обе стороны самостоятельно вычисляют два сеансовых ключа AES при помощи алгоритма согласования асимметричного ключа. При помощи одного из этих сеансовых ключей карточка создаёт код аутентификации сообщения (MAC), связанный с некоторыми данными, переданными из БУ. БУ проверяет MAC. Если проверка выполнена успешно, происходит аутентификация карточки. Данный этап называется аутентификацией карточки и подробно рассматривается в разделе 10.4.
- В-четвёртых, БУ и карточка используют согласованные сеансовые ключи для обеспечения конфиденциальности, целостности и подлинности всех передаваемых сообщений. Данный этап называется защищённым обменом сообщениями и подробно рассматривается в разделе 10.5.

CSM_156 Механизм, описанный в CSM_155, запускается бортовым устройством всякий раз, когда в одно из его считывающих устройств вводится карточка.

10.2. Взаимная проверка цепочки сертификата

10.2.1 Проверка цепочки сертификата карточки, проводимая БУ

CSM_157 Для проверки цепочки сертификата карточки тахографа бортовые устройства используют протокол, изображённый на Рисунок 4.

Примечания к Рисунок 4:

- Сертификаты карточки и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В разделе 9.1.5 они обозначаются как Card_MA.
- Сертификаты Card.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов карточек, и это отмечено в CAR сертификата карточки. В разделе 9.1.3 они обозначаются как MSCA_Card.
- Сертификат Card.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата Card.CA.
- Сертификат Card.Link, указанный на рисунке, – это связующий сертификат карточки, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат Card.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата Card.Link.

CSM_158 Как показано на Рисунок 4, проверка цепочки сертификата карточки начинается с ввода карточки. Бортовое устройство считывает указатель владельца карточки (`cardExtendedSerialNumber`) из EF ICC. БУ проверяет, известна ли ему карточка, т.е. была ли в прошлом проведена успешная проверка цепочки сертификата карточки, которая была сохранена на будущее. Если да и если сертификат карточки всё ещё действителен, процесс продолжается, и проводится проверка цепочки сертификата БУ. В противном случае БУ последовательно считывает с карточки сертификат MSCA_Card, используемый для проверки сертификата карточки Card.CA. Сертификат EUR, используемого для проверки сертификата MSCA_Card и, возможно, связующего сертификата, пока не будет найден известный ему сертификат или сертификат, который он может проверить. Если такой сертификат найден, БУ использует его для проверки базовых сертификатов карточки, которые он считал с карточки. Если проверка прошла успешно, процесс продолжается, и проводится проверка цепочки сертификата БУ. Если нет, БУ игнорирует карточку.

Примечание: Есть три способа, по которым БУ узнаёт сертификат Card.CA.EUR:

- сертификат Card.CA.EUR – это тот же самый сертификат, что и собственный сертификат EUR БУ;
- сертификат Card.CA.EUR предшествует собственному сертификату EUR БУ, и этот сертификат уже содержался в БУ при его выпуске (см. CSM_81);
- сертификат Card.CA.EUR выдан позднее собственного сертификата EUR БУ, и БУ в прошлом получил связующий сертификат с другой карточки тахографа, проверил его и сохранил на будущее.

CSM_159 Как показано на Рисунок 4, как только БУ проверит подлинность и действительность ранее неизвестного сертификата, он может сохранить этот сертификат на будущее, чтобы не надо было снова проверять подлинность этого сертификата, если он будет опять представлен БУ. Вместо хранения всего сертификата БУ может принять решение хранить только содержание основной части сертификата, как указано в разделе 9.3.2.

CSM_160 БУ проверяет временную действительность любого сертификата, считываемого с карточки или хранящегося в его памяти, и отклоняет просроченные сертификаты. Для проверки временной действительности представленного карточкой сертификата БУ использует внутренние часы.

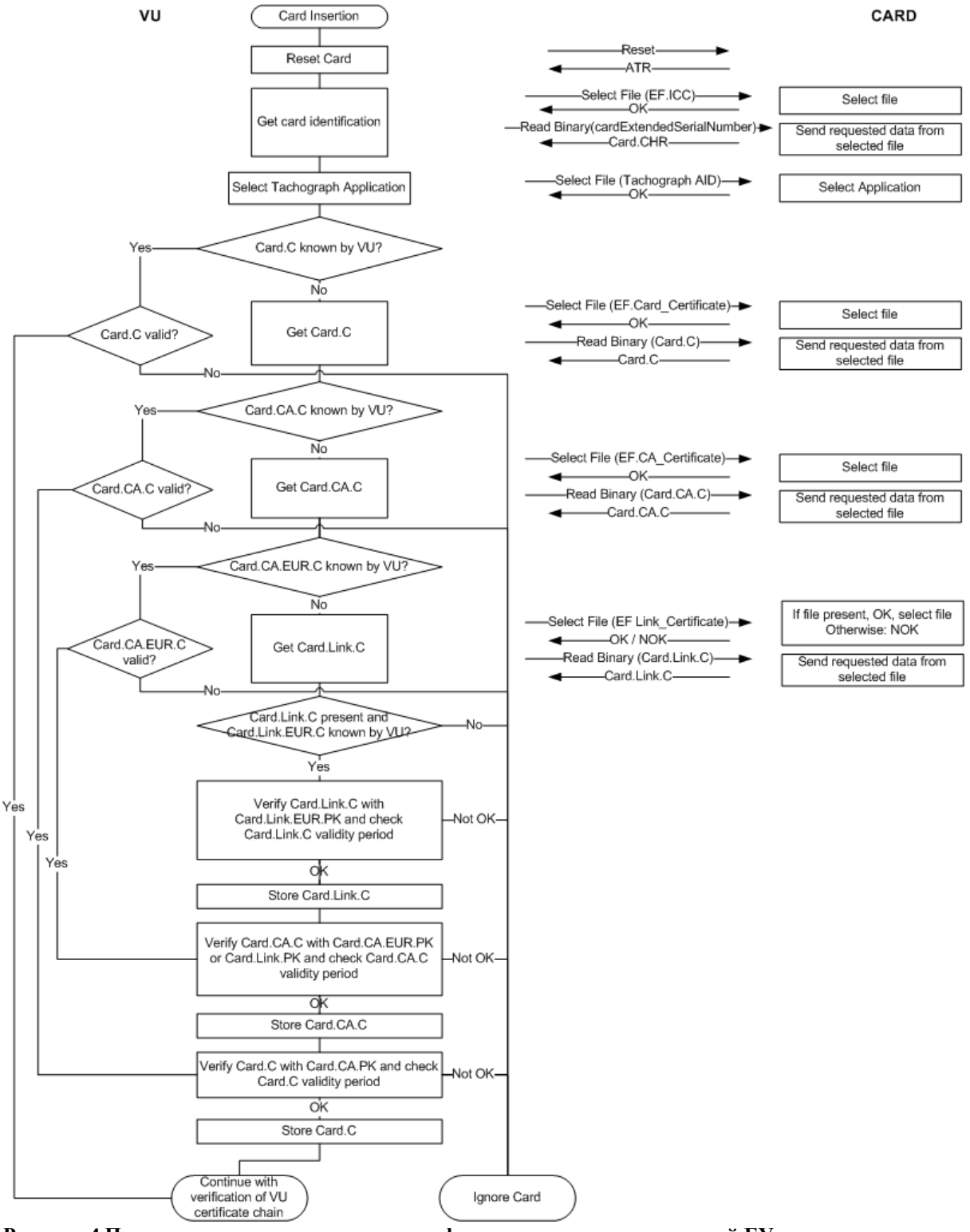


Рисунок 4 Протокол проверки цепочки сертификата карточки, проводимой БУ

10.2.2 Проверка цепочки сертификата БУ, проводимая карточкой

CSM_161 Для проверки цепочки сертификата БУ карточки тахографа используют протокол, изображённый на Рисунок 5.

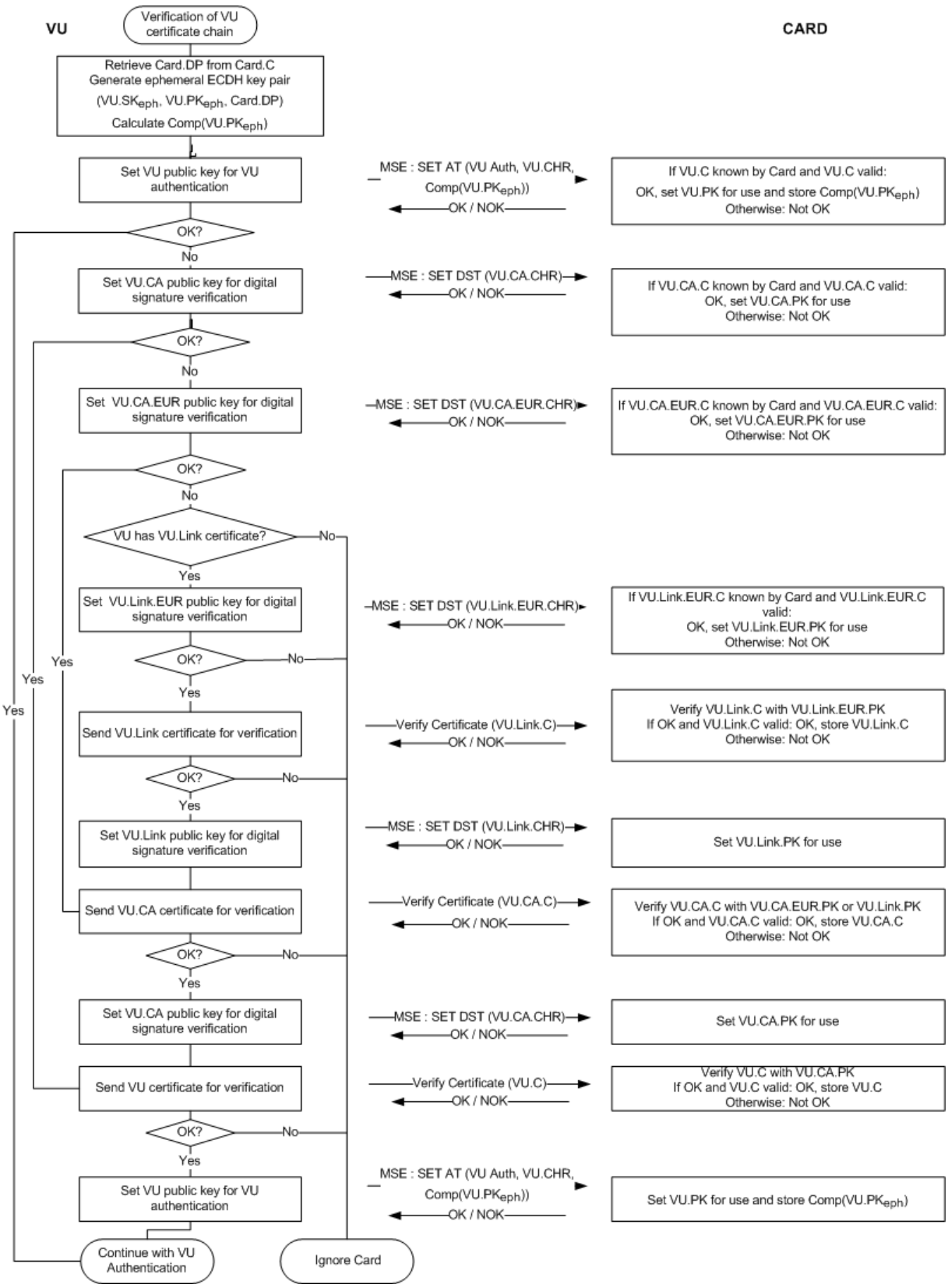


Рисунок 5 Протокол проверки цепочки сертификата БУ, проводимой карточкой

Примечания к Рисунок 5:

- Сертификаты БУ и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В разделе 9.1.4 они обозначаются как VU_MA.
- Сертификаты VU.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов БУ и внешних устройств ГНСС. В разделе 9.1.3 они обозначаются как MSCA_VU-EGF.
- Сертификат VU.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата VU.CA.
- Сертификат VU.Link, указанный на рисунке, – это связующий сертификат БУ, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат VU.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата VU.Link.

CSM_162 Как показано на Рисунок 5, проверка цепочки сертификата бортового устройства начинается с того, что бортовое устройство пытается установить свой собственный открытый ключ для использования на карточке тахографа. Если эта попытка удалась, это значит, что карточка успешно проверяла цепочку сертификата БУ ранее и сохранила сертификат БУ на будущее. В таком случае сертификат БУ можно использовать, и процесс продолжается с проведением аутентификации БУ. Если сертификат БУ карточке неизвестен, БУ последовательно представляет сертификат VU.CA для проверки его сертификата БУ, сертификат VU.CA.EUR для проверки сертификата VU.CA и, возможно, связующий сертификат для обнаружения известного сертификата или сертификата, который карточка может проверить. Если такой сертификат найден, карточка использует его для проверки базовых сертификатов БУ, которые были ей представлены. Если получилось, БУ наконец устанавливает свой собственный открытый ключ для использования на карточке тахографа. Если нет, БУ игнорирует карточку.

Примечание: Есть три способа, по которым карточка узнаёт сертификат VU.CA.EUR:

- сертификат VU.CA.EUR – это тот же самый сертификат, что и собственный сертификат EUR карточки;
- сертификат VU.CA.EUR предшествует собственному сертификату EUR карточки, и этот сертификат уже содержался на карточке при её выпуске (см. CSM_91);
- сертификат VU.CA.EUR выдан позднее собственного сертификата EUR карточки, и карточка в прошлом получила связующий сертификат из другого бортового устройства, проверила его и сохранила на будущее.

CSM_163 БУ использует MSE: Set AT, чтобы установить свой собственный открытый ключ для использования на карточке тахографа. Как указано в приложении 2, эта команда содержит указание криптографического механизма, который используется с установленным ключом. Этот механизм – аутентификация БУ с применением алгоритма ECDSA в сочетании с алгоритмом хеширования, связанным с размером ключа пары ключей VU_MA БУ, как указано в CSM_50.

CSM_164 Команда MSE: Set AT также содержит указание на кратковременную пару ключей, которую БУ использует во время согласования сеансовых ключей (см. раздел 10.4). Таким образом, перед передачей команды MSE: Set AT БУ генерирует кратковременную пару ключей ECC. Для генерирования кратковременной пары ключей БУ использует стандартизированные параметры области, указанные в сертификате карточки. Кратковременная пара ключей обозначается как ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). БУ принимает координату x кратковременной открытой точки ECDH как идентификационные данные ключа; это называется сжатым выражением открытого ключа и обозначается как $Comp(VU.PK_{eph})$.

CSM_165 Если команда MSE: Set AT выполнена успешно, карточка устанавливает указанный VU.PK для последующего использования во время аутентификации транспортного средства и временно хранит $Comp(VU.PK_{eph})$. Если до согласования сеансовых ключей передаются две или несколько команд MSE: Set AT, карточка сохраняет только последнюю полученную команду $Comp(VU.PK_{eph})$.

CSM_166 Карточка проверяет временную действительность любого сертификата, представляемого БУ или указанного БУ и при этом хранящегося в памяти карточки, и отклоняет просроченные сертификаты.

CSM_167 Для проверки временной действительности представленного БУ сертификата, каждая карточка тахографа внутри сохраняет некоторые данные, представляющие текущий момент времени. БУ эти данные напрямую не обновляет. При выпуске текущее время карточки устанавливается как равно фактической дате сертификата Card_MA карточки. Карточка обновляет своё текущее время, если фактическая дата подлинного действительного источника времени, представленная БУ, более поздняя, чем текущее время карточки. В подобном случае карточка устанавливает своё текущее время по фактической дате этого сертификата. В качестве действительного источника времени карточка принимает только следующие сертификаты:

- Связующие сертификаты ERCA второго поколения
- Сертификаты MSCA второго поколения
- Сертификаты БУ второго поколения, выданные той же страной, что и собственный сертификат (-ы) карточки.

Примечание: последнее требование значит, что карточка способна распознавать CAR сертификата БУ, т.е. сертификата MSCA_VU-EGF. Он будет отличаться от CAR её собственного сертификата, т.е. сертификата MSCA_Card.

CSM_168 Как показано на Рисунок 5, как только карточка проверит подлинность и действительность ранее неизвестного сертификата, она может сохранить этот сертификат на будущее, чтобы не надо было снова проверять подлинность этого сертификата, если он будет опять представлен карточке. Вместо хранения всего сертификата карточка может принять решение хранить только содержание основной части сертификата, как указано в разделе 9.3.2.

10.3. Аутентификация БУ

CSM_169 Бортовые устройства и карточки используют протокол аутентификации БУ, представленный на Рисунок 6 для аутентификации БУ относительно карточки. Аутентификация БУ позволяет карточке тахографа достоверно проверить подлинность БУ. Для этого БУ использует закрытый ключ для подписания запросы, сгенерированного карточкой.

CSM_170 Помимо запроса карточки, БУ включает в подпись указатель владельца карточки, взятый из сертификата карточки.

Примечание: Таким образом обеспечивается, что карточка, относительно которой происходит аутентификация БУ, является той же самой карточкой, цепочку сертификата которой БУ уже проверял.

CSM_171 БУ также включает в подпись идентификатор кратковременного открытого ключа Comp(VU.PK_{eph}), который БУ использует для установки защищённого обмена сообщениями во время процесса аутентификации микросхемы, указанного в разделе 10.4.

Примечание: Тем самым обеспечивается, чтобы БУ, с которым карточка установила связь во время сеанса защищённого обмена сообщениями, был тот же самый БУ, который был аутентифицирован карточкой.

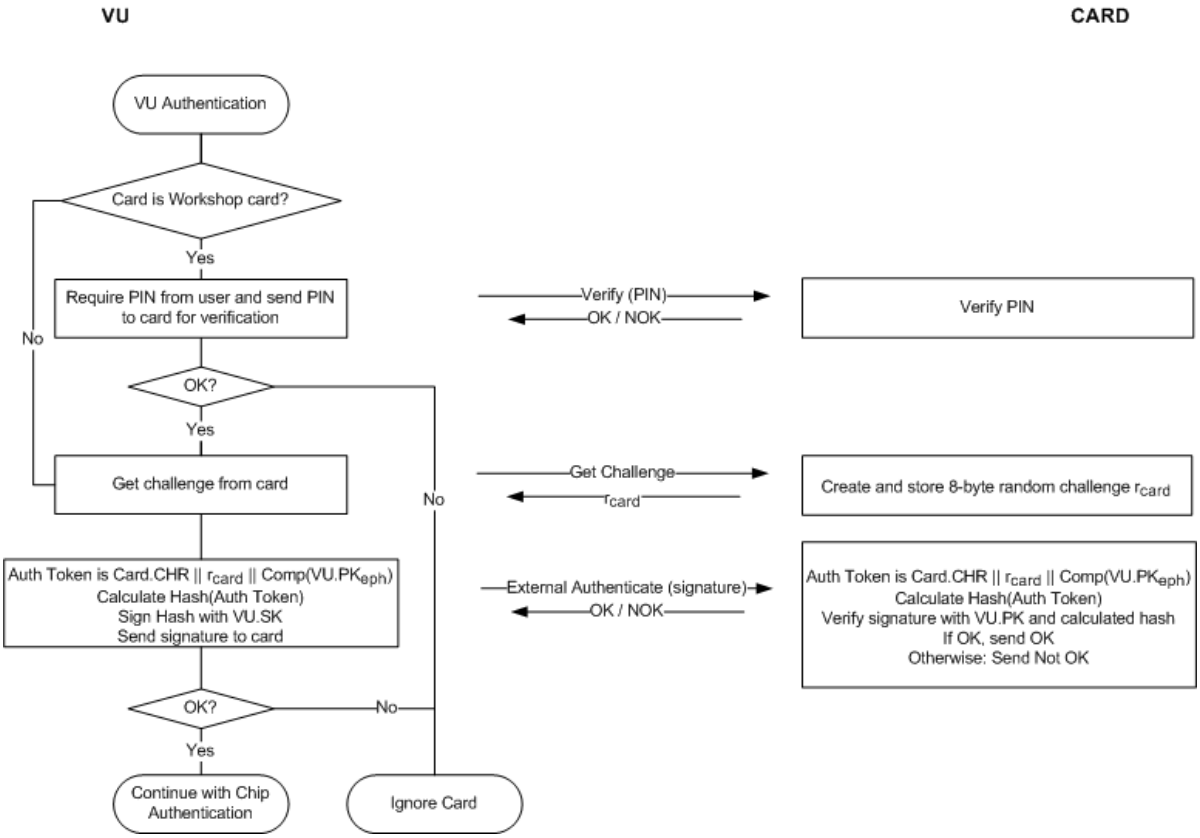


Рисунок 6 Протокол аутентификации БУ

CSM_172 Если во время аутентификации БУ передаёт несколько команд GET CHALLENGE, карточка каждый раз возвращает новый 8-байтовый случайный запрос, а сохраняет только последний из них.

CSM_173 Алгоритм подписи, который БУ использует для аутентификации БУ, – ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа пары ключей VU_MA БУ, как указано в CSM_50. Формат подписи простой, как указано в [TR-03111]. БУ передаёт полученную подпись на карточку.

CSM_174 По получении подписи БУ в команде EXTERNAL AUTHENTICATE карточка

- Вычисляет маркер аутентификации путём конкатенации Card.CHR, запроса карточки r_{card} и идентификатора кратковременного открытого ключа БУ Comp($VU.PK_{eph}$),
- Вычисляет хеш-функцию, связанную с маркером аутентификации, с применением алгоритма хеширования, связанного с размером ключа пары ключей VU_MA БУ, как указано в CSM_50,
- Проверяет подпись БУ с применением алгоритма ECDSA в сочетании с VU.PK и вычисленной хеш-функцией.

10.4. Аутентификация микросхемы и согласование сеансовых ключей

CSM_175 Бортовые устройства и карточки используют протокол аутентификации микросхемы, представленный на **Рисунок 7** для аутентификации карточки относительно БУ. Аутентификация микросхемы позволяет бортовому устройству достоверно проверить подлинность карточки.

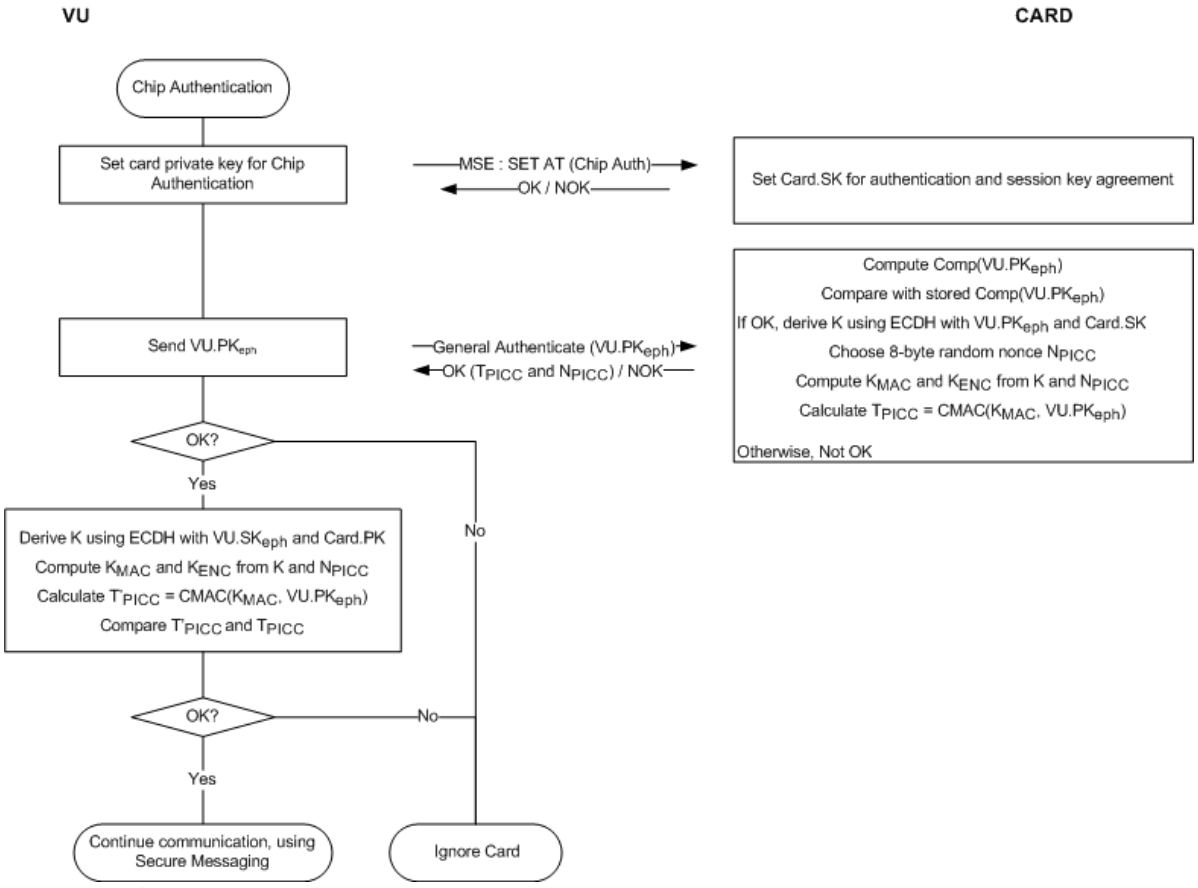


Рисунок 7 Аутентификация микросхемы и согласование сеансовых ключей

CSM_176 БУ и карточка предпринимают следующие действия:

1. Бортовое устройство инициирует процесс аутентификации микросхемы, передавая команду MSE: Set AT с указанием аутентификации микросхемы с применением алгоритма ECDSA, в результате чего получается длина сеансового ключа AES, связанная с размером ключа пары ключей Card_MA карточки, как указано в CSM_50. БУ определяет размер ключа пары ключей карточки по сертификату карточки.
2. БУ передаёт открытую точку $VU.PK_{eph}$ своей кратковременной пары ключей на карточку. Как поясняется в CSM_164, БУ сгенерировал эту кратковременную пару ключей до проверки цепочки сертификата БУ. БУ передало идентификатор кратковременного открытого ключа $Comp(VU.PK_{eph})$ на карточку, и карточка его сохранила.
3. Карточка вычисляет $Comp(VU.PK_{eph})$ по $VU.PK_{eph}$ и сравнивает полученное значение с сохранённым значением $Comp(VU.PK_{eph})$.
4. Используя алгоритм ECDH в сочетании со статичным закрытым ключом карточки и кратковременным открытым ключом БУ, карточка вычисляет тайный K.
5. Карточка выбирает случайный временный 8-байтовый код N_{PICC} и использует его для получения двух сеансовых ключей AES K_{MAC} и K_{ENC} из K. См. CSM_179.
6. Используя K_{MAC}, карточка вычисляет маркер аутентификации по идентификатору кратковременного открытого ключа БУ: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Карточка передаёт N_{PICC} и T_{PICC} в бортовое устройство.
7. Используя алгоритм ECDH в сочетании со статичным открытым ключом карточки и кратковременным закрытым ключом БУ, БУ вычисляет тот же самый тайный K, что и карточка на этапе 4.
8. БУ получает сеансовые ключи K_{MAC} и K_{ENC} из K и N_{PICC}; см. CSM_179.
9. БУ проверяет маркер аутентификации T_{PICC}.

CSM_177 На указанном выше этапе 3 карточка вычисляет Comp(VU.PKeph) как координату x открытой точки в VU.PKeph.

CSM_178 На указанных выше этапах 4 и 7 карточка и бортовое устройство используют алгоритм ECKA-EG, как описано в [TR-03111].

CSM_179 На указанных выше этапах 5 и 8 карточка и бортовое устройство используют функцию составления ключей для сеансовых ключей AES, как описано в [TR-03111], с учётом следующих уточнений и изменений:

- Значение счётчика – ’00 00 00 01’ для K_{ENC} и ’00 00 00 02’ для $K_{MAC.}$
- Используется факультативное временное значение *r*, равное $N_{PICC.}$
- Для получения 128-битовых ключей AES используется алгоритм хеширования SHA-256.
- Для получения 192-битовых ключей AES используется алгоритм хеширования SHA-384.
- Для получения 256-битовых ключей AES используется алгоритм хеширования SHA-512.

Длина сеансовых ключей (т.е. длина, на которой усекается хеш) связана с размером пары ключей Card_MA, как указано в CSM_50.

CSM_180 На указанных выше этапах 6 и 9 карточка и бортовое устройство используют алгоритм AES в режиме CMAC, как описано в [SP 800-38B]. Длина T_{PICC} связана с длиной сеансовых ключей AES, как описано в CSM_50.

10.5. Защищённый обмен сообщениями

10.5.1 Общие положения

CSM_181 Все команды и ответы, которыми обмениваются бортовое устройство и карточка тахографа после успешной аутентификации микросхемы и до конца сеанса, защищены механизмом защищённого обмена сообщениями.

CSM_182 За исключением случаев считывания из файла с условием доступа SM-R-ENC-MAC-G2 (см. приложение 2, раздел 4), защищённый обмен сообщениями используется только в режиме аутентификации. В этом режиме ко всем командам и ответам добавляется криптографическая контрольная сумма (MAC), чтобы обеспечить подлинность и целостность сообщения.

CSM_183 При считывании данных из файла с условием доступа SM-R-ENC-MAC-G2 защищённый обмен сообщениями используется в режиме шифрования с последующей аутентификацией, т.е. данные ответа сначала шифруются, чтобы обеспечить конфиденциальность сообщения, а затем вычисляется MAC, связанная с отформатированными зашифрованными данными, для обеспечения подлинности и целостности.

CSM_184 Защищённый обмен сообщениями использует AES, как описано в [AES], с сеансовыми ключами K_{MAC} и K_{ENC}, согласованными в процессе аутентификации микросхемы.

CSM_185 В качестве счётчика исходящих сообщений (SSC) для предотвращения повторных атак используется неподписанное целое число. Размер SSC равен размеру блока AES, т.е. 128 битам. SSC представлен в формате изначальных MSB. Счётчик исходящих сообщений выставляется на ноль (т.е. ‘00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’), когда начинается защищённый обмен сообщениями. SSC увеличивается всякий раз перед генерированием команды или ответа APDU, т.к. поскольку стартовое значение SSC в сеансе SM равно 0, в первой команде значение SSC будет 1. Значение SSC в первом ответе будет 2.

CSM_186 Для шифрования сообщения используется K_{ENC} с AES в режиме сцепления криптоблоков (CBC), как описано в [ISO 10116], с параметром чередования $m = 1$ и вектором инициализации $SV = E(K_{ENC}, SSC)$, т.е. текущее значение счётчика исходящих сообщений, зашифрованного при помощи K_{ENC}.

CSM_187 Для аутентификации сообщений используется K_{MAC} с AES в режиме CMAC, как описано в [SP 800-38B]. Длина MAC связана с длиной сеансовых ключей AES, как описано в CSM_50. Счётчик исходящих сообщений включается в MAC путём его добавления перед аутентификацией датаграммы.

10.5.2 Структура защищённого сообщения

CSM_188 Защищённый обмен сообщениями использует только объекты данных защищённого обмена сообщениями (см. [ISO 7816-4]), перечисленные в Таблица 5. В любом сообщении эти объекты данных используются в очерёдности, указанной в данной таблице

Название объекта данных	Метка	Присутствие обязательно (M), условно (C) или запрещено (F)	
		Команды	Ответы
Простое значение, не закодированное в BER-TLV	‘81’	C	C
Простое значение, закодированное в BER-TLV , но не включающее в себя объекты данных SM	‘B3’	C	C
Показатель заполняющего содержания с последующей пиктограммой, простое значение, не закодированное в BER-TLV	‘87’	C	C
Защищённое значение Le	‘97’	C	F
Статус обработки	‘99’	F	M
Криптографическая контрольная сумма	‘8E’	M	M

Таблица 5 Объекты данных защищённого обмена сообщениями

Примечание: Как указано в приложении 2, карточки тахографа могут поддерживать команды READ BINARY и UPDATE BINARY с нечётным байтом INS (‘B1’ resp. ‘D7’). Эти варианты команд необходимы для считывания и обновления файлов, содержащих более чем 32768 байтов или более. В случае использования такого варианта вместо объекта с меткой ‘81’ используется объект данных с меткой ‘B3’. Более подробно см. приложение 2.

CSM_189 Все объекты данных SM кодируются в DER TLV, как указано в [ISO 8825-1]. Такое кодирование приводит к следующей структуре значения длины метки (TLV):

- Метка: Метка кодируется одним или двумя октетами и указывает на содержание.
- Длина: Длина кодируется как неподписанное целое число одним, двумя или тремя октетами, что приводит к максимальной длине 65535 октетов. Используется минимальное число октетов.
- Значение: Значение кодируется в виде нуля или более октетов.

CSM_190 APDU, защищённые механизмом защищённого обмена сообщениями, создаются следующим образом:

- Заголовок команды включается в вычисление MAC, так что значение ‘0C’ используется для классового байта CLA.
- Как указано в приложении 2, все байты INS чётные, с возможным исключением нечётных байтов INS для команд READ BINARY и UPDATE BINARY.
- Фактическое значение Lc будет изменено на Lc’ после применения механизма защищённого обмена сообщениями.
- Поле данных состоит из объектов данных SM.
- В защищённой команде APDU новый байт Le устанавливается на ‘00’. При необходимости объект данных ‘97’ включается в поле данных, чтобы передать исходное значение Le.

CSM_191 Любой объект данных, подлежащий шифрованию, заполняется в соответствии с [ISO 7816-4] при помощи показателя заполнения ‘01’. Для вычисления MAC каждый объект данных в APDU также отдельно заполняется в соответствии с [ISO 7816-4].

Примечание: Заполнение в механизме защищённого обмена сообщениями всегда происходит на уровне защищённого обмена сообщениями, а не через алгоритмы CMAC или CBC.

Резюме и примеры

У команды APDU с применяемым механизмом защищённого обмена сообщениями будет следующая структура, в зависимости от соответствующей незащищённой команды (DO – объект данных):

Пример 1: CLA INS P1 P2 || Lc’ || DO ‘8E’ || Le
Пример 2: CLA INS P1 P2 || Lc’ || DO ‘97’ || DO’8E’ || Le
Пример 3 (чётный байт INS): CLA INS P1 P2 || Lc’ || DO ‘81’ || DO’8E’ || Le
Пример 3 (нечётный байт INS): CLA INS P1 P2 || Lc’ || DO ‘B3’ || DO’8E’ || Le
Пример 4 (чётный байт INS): CLA INS P1 P2 || Lc’ || DO ‘81’ || DO’97’ || DO’8E’ || Le
Пример 4 (нечётный байт INS): CLA INS P1 P2 || Lc’ || DO ‘B3’ || DO’97’ || DO’8E’ || Le

где Le = ‘00’ или ’00 00’ в зависимости от того, используются ли поля короткой длины или поля расширенной длины; см. [ISO 7816-4].

У ответа APDU с применяемым механизмом защищённого обмена сообщениями будет следующая структура, в зависимости от соответствующего незащищённого ответа:

Пример 1 или 3:	DO ‘99’ || DO ‘8E’ || SW1SW2
Пример 2 или 4 (чётный байт INS) с шифрованием:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Пример 2 или 4 (чётный байт INS) без шифрования:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Пример 2 или 4 (нечётный байт INS) без шифрования:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

Примечание: Пример 2 или 4 (нечётный байт INS) с шифрованием никогда не используется при связи между БУ и карточкой.

Далее приводятся три примера трансформаций APDU для команд с чётным кодом INS. Рисунок 8 показывает аутентифицированную команду APDU в примере 4, Рисунок 9 показывает аутентифицированный ответ APDU в примерах 2/4, и Рисунок 10 показывает зашифрованный и аутентифицированный ответ APDU в примерах 2/4.

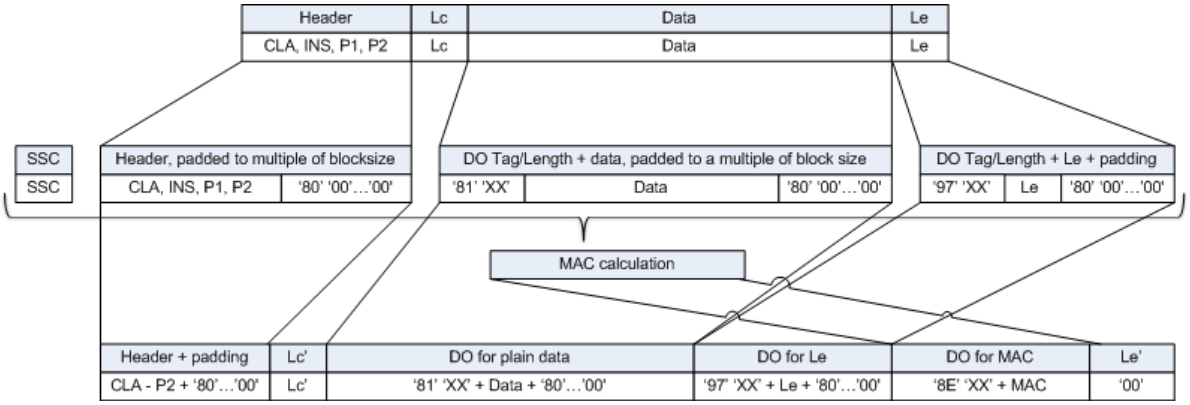


Рисунок 8 Трансформация аутентифицированной команды APDU в примере 4

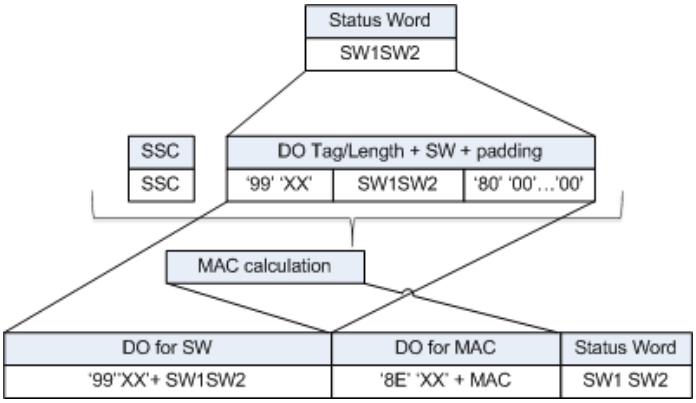


Рисунок 9 Трансформация аутентифицированного ответа APDU в примерах 1/3

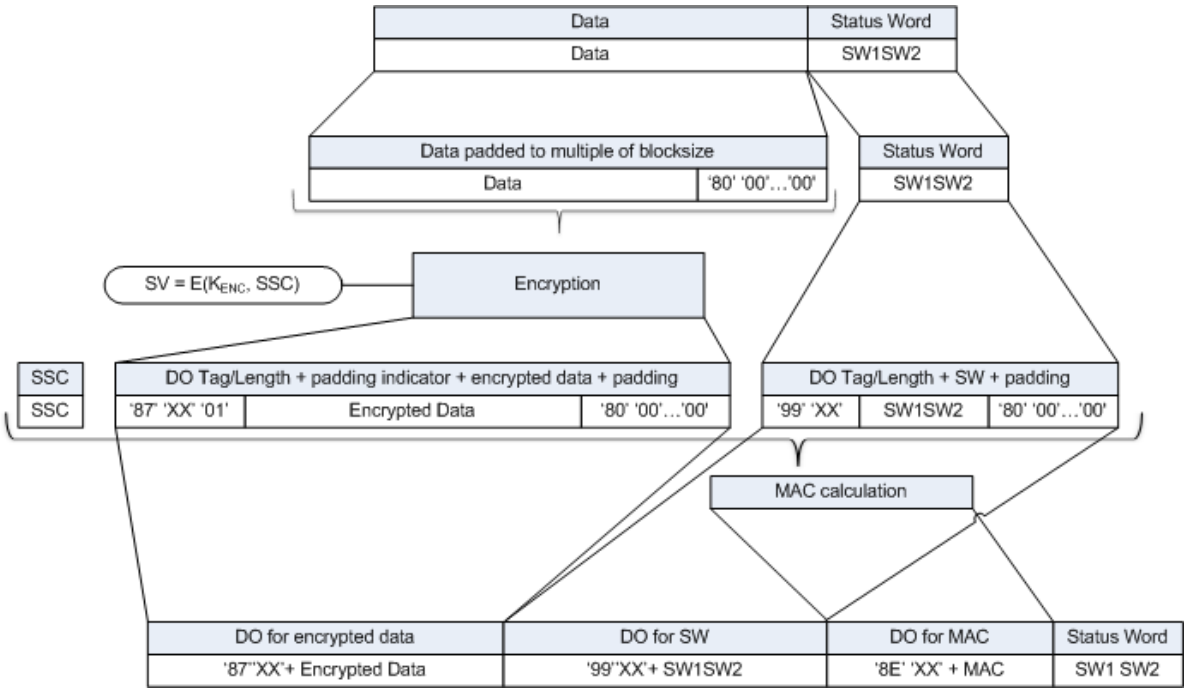


Рисунок 10 Трансформация зашифрованного и аутентифицированного ответа APDU в примерах 2/4

10.5.3 Отмена сеанса защищённого обмена сообщениями

CSM_192 Бортовое устройство прерывает текущий сеанс защищённого обмена сообщениями, только если возникает одно из следующих условий:

- оно получает простой ответ APDU,
- оно обнаруживает ошибку защищённого обмена сообщениями в ответе APDU:
  - Отсутствие ожидаемого объекта данных защищённого обмена сообщениями, неверная последовательность объектов данных или присутствие неизвестного объекта данных.
  - Объект данных защищённого обмена сообщениями неверный, например, неверное значение MAC, неверная структура TLV или показатель заполнения с меткой ‘87’ не равен ‘01’.
- карточка передаёт байт статуса, указывающий на то, что обнаружена ошибка SM (см. CSM_194),
- достигнуто предельное число команд и соответствующих ответов в рамках текущего сеанса. В отношении данного БУ такой предел устанавливает производитель, учитывающий требования безопасности к используемому аппаратному обеспечению, с максимальным значением 240 команд и ответов SM за сеанс.

CSM_193 Карточка тахографа прерывает текущий сеанс защищённого обмена сообщениями, только если возникает одно из следующих условий:

- она получает простую команду APDU,
- она обнаруживает ошибку защищённого обмена сообщениями в команде APDU:
  - Отсутствие ожидаемого объекта данных защищённого обмена сообщениями, неверная последовательность объектов данных или присутствие неизвестного объекта данных.
  - Объект данных защищённого обмена сообщениями неверный, например, неверное значение MAC или неверная структура TLV.
- прекращено питание или она перезагрузилась,
- БУ выбирает приложение на карточке,
- БУ начинает процесс аутентификации БУ,
- достигнуто предельное число команд и соответствующих ответов в рамках текущего сеанса. В отношении данной карточки такой предел устанавливает производитель, учитывающий требования безопасности к используемому аппаратному обеспечению, с максимальным значением 240 команд и ответов SM за сеанс.

CSM_194 Касательно ошибки обработки SM на карточке тахографа:

- Если в команде APDU отсутствуют некоторые ожидаемые объекты данных защищённого обмена сообщениями, неверный порядок объектов данных или присутствуют неизвестные объекты данных, карточка тахографа отвечает байтами статуса ’69 87’.
- Если в команде APDU неверный объект данных защищённого обмена сообщениями, карточка тахографа отвечает байтами статуса ’69 88’.

В таком случае байты статуса возвращаются без использования SM.

CSM_195 Если сеанс защищённого обмена сообщениями между БУ и карточкой тахографа прерван, БУ и карточка тахографа

- в безопасной манере уничтожают сохранённые сеансовые ключи
- немедленно запускают новый сеанс защищённого обмена сообщениями, как описано в разделах 10.2-10.5.

CSM_196 Если по какой-либо причине БУ решает перезапустить взаимную аутентификацию в отношении введённой карточки, процесс снова начинается с проверки цепочки сертификата карточки, как описано в разделе 10.2, и продолжается, как описано в разделах 10.2-10.5.

11. Соединение, взаимная аутентификация и защищённый обмен сообщениями между БУ и внешним устройством ГНСС

11.1. Общие положения

CSM_197 Устройство ГНСС, которое БУ использует для установления местоположения, может быть внутренним (т.е. встроенным в корпус БУ и не съёмным), или это может быть внешний модуль. В первом случае нет необходимости стандартизировать внутреннюю связь между устройством ГНСС и БУ, и требования настоящей главы не применяются. В последнем случае связь между БУ и внешним устройством ГНСС стандартизируется и защищается, как описано в настоящей главе.

CSM_198 Защищённая связь между бортовым устройством и внешним устройством ГНСС происходит так же, как защищённая связь между бортовым устройством и карточкой тахографа, где внешнее устройство ГНСС (EGF) играет роль карточки. EGF удовлетворяет всем требованиям главы 10 к карточкам тахографа с учётом отклонений, пояснений и дополнений, представленных в настоящей главе. В частности, взаимная проверка цепочки сертификата, аутентификация БУ и аутентификация микросхемы проводятся так, как описано в разделах 11.3 и 11.4.

CSM_199 Связь между бортовым устройством и EGF отличается от связи между бортовым устройством и карточкой тем, что бортовое устройство и EGF должны быть однажды соединены в мастерской, чтобы впоследствии в режиме нормальной эксплуатации они могли обмениваться данными ГНСС. Процесс соединения описан в разделе 11.2.

CSM_200 Для обеспечения связи между бортовым устройством и EGF используются команды и ответы APDU согласно [ISO 7816-4] и [ISO 7816-8]. Точная структура таких APDU описана в приложении 2 к настоящему дополнению.

11.2. Соединение БУ и внешнего устройства ГНСС

CSM_201 Бортовое устройство и EGF транспортного средства соединяются в мастерской. В режиме нормальной эксплуатации связь могут держать только соединённые между собой бортовое устройство и EGF.

CSM_202 Соединение бортового устройства и EGF возможно только в том случае, если бортовое устройство находится в режиме калибровки. Соединение инициирует бортовое устройство.

CSM_203 Мастерская может в любой момент пересоединить бортовое устройство с другим или тем же самым EGF. В время повторного соединения БУ в безопасной манере уничтожает сохранившийся в памяти сертификат EGF_MA и сохраняет сертификат EGF_MA EGF, с которым оно соединяется.

CSM_204 Мастерская может в любой момент пересоединить внешнее устройство ГНСС с другим или тем же самым БУ. В время повторного соединения EGF в безопасной манере уничтожает сохранившийся в памяти сертификат VU_MA и сохраняет сертификат VU_MA БУ, с которым оно соединяется.

11.3. Взаимная проверка цепочки сертификата

11.3.1 Общие положения

CSM_205 Взаимная проверка цепочки сертификата между БУ и EGF проводится только во время соединения БУ и EGF в мастерской. Во время нормальной эксплуатации соединённых БУ и EGF проверка сертификатов не проводится. Вместо этого БУ и EGF доверяют сертификатам, которые они сохранили во время соединения, после проверки временной действительности таких сертификатов. Для защиты связи БУ и EGF во время нормальной эксплуатации БУ и EGF не доверяют никаким другим сертификатам.

11.3.2 Во время соединения БУ и EGF

CSM_206 Во время соединения с EGF для проверки цепочки сертификата внешнего устройства ГНСС бортовое устройство использует протокол, отображённый на Рисунок 4 (раздел 10.2.1).

Связанные с этим примечания по Рисунок 4:

- Контроль связи не входит в область применения настоящего приложения. Однако EGF не является «умной» карточкой, и потому БУ, скорее всего, не передаст команду Reset для запуска связи и не получит ATR.
- Сертификаты карточки и открытые ключи, указанные на рисунке, интерпретируются как сертификаты и открытые ключи EGF для взаимной аутентификации. В разделе 9.1.6 они обозначаются как EGF_MA.
- Сертификаты Card.CA и открытые ключи, указанные на рисунке, интерпретируются как сертификаты и открытые ключи MSCA для подписания сертификатов EGF. В разделе 9.1.3 они обозначаются как MSCA_VU-EGF.
- Сертификат Card.CA.EUR, указанный на рисунке, интерпретируется как европейский корневой сертификат, отмеченный в CAR сертификата MSCA_VU-EGF.
- Сертификат Card.Link, указанный на рисунке, интерпретируется как связующий сертификат EGF, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат Card.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата Card.Link.
- Вместо `cardExtendedSerialNumber` БУ считывает `sensorGNSSserialNumber` из EF ICC.
- Вместо выбора AID тахографа БУ выбирает AID EGF.
- ‘Ignore Card’ интерпретируется как ‘Ignore EGF’.

CSM_207 После проверки сертификата EGF_MA бортовое устройство хранит этот сертификат для использования во время нормальной эксплуатации; см. раздел 11.3.3.

CSM_208 Во время соединения с БУ для проверки цепочки сертификата БУ внешнее устройство ГНСС использует протокол, отображённый на Рисунок 5 (раздел 10.2.2).

Связанные с этим примечания по Рисунок 5:

- БУ генерирует новую кратковременную пару ключей с параметрами области в сертификате EGF.
- Сертификаты БУ и открытые ключи, указанные на рисунке, предназначены для взаимной аутентификации. В разделе 9.1.4 они обозначаются как VU_MA.
- Сертификаты VU.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов БУ и внешних устройств ГНСС. В разделе 9.1.3 они обозначаются как MSCA_VU-EGF.
- Сертификат VU.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата VU.CA.
- Сертификат VU.Link, указанный на рисунке, – это связующий сертификат БУ, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат VU.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата VU.Link.

CSM_209 Отклоняясь от требования CSM_167, EGF использует время ГНСС для проверки временной действительности любого представленного сертификата.

CSM_210 После проверки сертификата VU_MA внешнее устройство ГНСС хранит этот сертификат для использования во время нормальной эксплуатации; см. раздел 11.3.3.

11.3.3 Во время нормальной эксплуатации

CSM_211 Во время нормальной эксплуатации бортовое устройство и EGF используют протокол, описанный на Рисунок 11, для проверки временной действительности хранящихся сертификатов EGF_MA и VU_MA и определения открытого ключа VU_MA для последующей аутентификации БУ. Во время нормальной эксплуатации никакой дальнейшей взаимной проверки цепочек сертификатов не проводится.

Следует отметить, что Рисунок 11 в целом состоит из первых этапов, отражённых на Рисунок 4 и Рисунок 5. Опять-таки следует иметь в виду, что EGF не является «умной» карточкой, и потому БУ,

скорее всего, не передаст команду Reset для запуска связи и не получит ATR. В любом случае это не входит в область применения настоящего приложения.

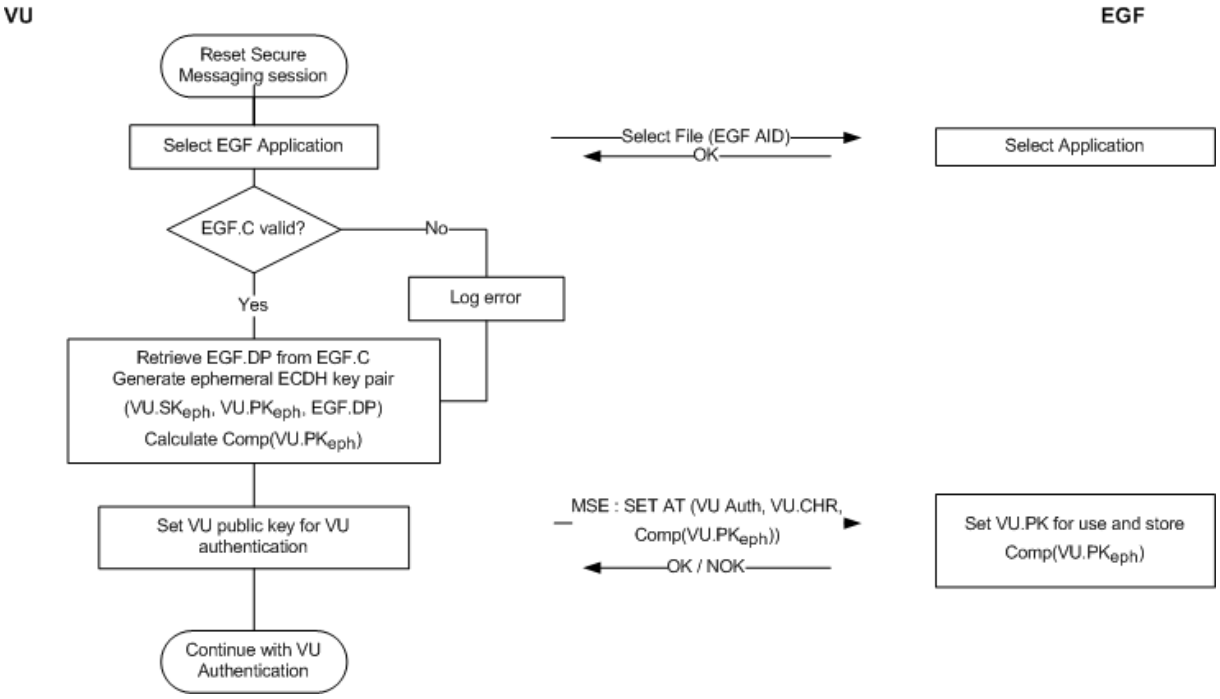


Рисунок 11 Взаимная проверка временной действительности сертификата во время нормальной эксплуатации БУ и EGF

CSM_212 Как показано на Рисунок 11, бортовое устройство регистрирует ошибку, если сертификат EGF_MA более недействителен. Однако взаимная аутентификация, согласование ключей и дальнейшая связь через механизм защищённого обмена сообщениями должны происходить, как обычно.

11.4. Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей

CSM_213 Аутентификация БУ, аутентификация микросхемы и согласование сеансовых ключей между БУ и EGF происходят во время соединения и во всех случаях, когда в условиях нормальной эксплуатации восстанавливается сеанс защищённого обмена сообщениями. БУ и EGF выполняют процессы, описанные в разделах 10.3 и 10.4. Выполняются все требования указанных разделов.

11.5. Защищённый обмен сообщениями

CSM_214 Все команды и ответы, которыми обмениваются бортовое устройство и внешнее устройство ГНСС после успешной аутентификации микросхемы и до конца сеанса, защищены механизмом защищённого обмена сообщениями в режиме только аутентификации. Выполняются все требования раздела 10.5.

CSM_215 Если сеанс защищённого обмена сообщениями между БУ и EGF прерван, БУ немедленно запускает новый сеанс защищённого обмена сообщениями, как описано в разделах 11.3.3 и 11.4.

12. Соединение и связь между БУ и датчиком движения

12.1. Общие положения

CSM_216 Бортовое устройство и датчик движения устанавливают связь при помощи протокола интерфейса, указанного в [ISO 16844-3], в рамках процесса соединения и в условиях нормальной эксплуатации, с учётом изменений, предусмотренных в настоящей главе и в разделе 9.2.1.

Примечание: предполагается, что читатели данной главы знакомы с содержанием [ISO 16844-3].

12.2. Соединение БУ и датчика движения с использованием различных поколений ключей

Как поясняется в разделе 9.2.1, ключ старшего порядка датчика движения и все связанные с ним ключи регулярно заменяются. Это приводит к присутствию на карточках мастерской до трёх ключей AES $K_{M\text{-}WC}$ (последовательных поколений ключей), связанных с датчиком движения. Также и в датчиках движения может быть до трёх различных вариантов зашифрованных данных на базе AES (последовательных поколений ключа старшего порядка датчика движения K_M). В бортовом устройстве есть только один ключ, связанный с датчиком движения, $K_{M\text{-}VU.}$

CSM_217 БУ второго поколения и датчик движения второго поколения соединяются следующим образом (ср. таблицу 6 в [ISO 16844-3]):

1. Карточка мастерской второго поколения вводится в БУ, и БУ подсоединяется к датчику движения.
2. БУ считывает все имеющиеся ключи $K_{M\text{-}WC}$ с карточки мастерской, проверяет номера их версий и выбирает один, соответствующий номеру версии ключа $K_{M\text{-}VU}$ БУ. Если соответствующего ключа $K_{M\text{-}WC}$ на карточке мастерской нет, БУ прерывает процесс соединения и показывает владельцу карточки мастерской соответствующее сообщение об ошибке.
3. БУ вычисляет ключ старшего порядка датчика движения K_M по $K_{M\text{-}VU}$ и $K_{M\text{-}WC,}$ а идентификационный ключ K_{ID} по K_M, как указано в разделе 9.2.1.
4. БУ передаёт указание начать процесс соединения на датчик движения, как описано в [ISO 16844-3], и шифрует серийный номер, который он получил от датчика движения, при помощи идентификационного ключа $K_{ID.}$ БУ передаёт зашифрованный серийный номер обратно в датчик движения.
5. Датчик движения совмещает зашифрованный серийный номер последовательно с каждым зашифрованным серийным номером, который в нём хранится. Если соответствие найдено, происходит аутентификация БУ. Датчик движения отмечает поколение K_{ID}, используемого БУ, и возвращает соответствующую зашифрованную версию своего ключа соединения, т.е. Шифр, созданный при помощи того же поколения K_M.
6. БУ расшифровывает ключ соединения при помощи K_M, генерирует сеансовый ключ $K_{S,}$ шифрует его при помощи ключа соединения и передаёт результат в датчик движения. Датчик движения расшифровывает K_S.
7. БУ собирает информацию о соединении, как указано в [ISO 16844-3], шифрует эту информацию с помощью ключа соединения и передаёт результат в датчик движения. Датчик движения расшифровывает информацию о соединении.
8. Датчик движения шифрует полученную информацию о соединении при помощи полученного K_S и возвращает её БУ. БУ проверяет, является ли информация о соединении той же информацией, которую БУ направил датчику движения на предыдущем этапе. Если да, это доказывает, что датчик движения использовал тот же K_S, что и БУ, и, соответственно, на этапе 5 передал свой ключ соединения, зашифрованный при помощи правильного поколения K_M. Так происходит аутентификация датчика движения.

Следует отметить, что этапы 2 и 5 отличаются от стандартного процесса в [ISO 16844-3]; остальные этапы стандартные.

Пример: Предположим, что соединение происходит в первый год действия сертификата ERCA (3); см. Рисунок 2 в разделе 9.2.1.2. Более того,

- Предположим, что датчик движения был выпущен в последний год срока действия сертификата ERCA (1). Таким образом, он будет содержать следующие ключи и данные:
    - N_s[1]: свой серийный номер, зашифрованный при помощи первого поколения K_{ID},

    - N_s[2]: свой серийный номер, зашифрованный при помощи второго поколения K_{ID},
    - N_s[3]: свой серийный номер, зашифрованный при помощи третьего поколения K_{ID},
    - K_P[1]: свой ключ соединения первого поколения[1], зашифрованный при помощи первого поколения K_M,
    - K_P[2]: свой ключ соединения второго поколения, зашифрованный при помощи второго поколения K_M,
    - K_P[3]: свой ключ соединения третьего поколения, зашифрованный при помощи третьего поколения K_M,
- Предположим, что карточка мастерской был выпущена в первый год срока действия сертификата ERCA (3). Таким образом, на ней будет содержаться второе и третье поколения ключа K_{M-WC}.
- Предположим, что БУ – это БУ второго поколения, в котором содержится второе поколение K_{M-VU}.

В этом случае на этапах 2-5 произойдёт следующее:

- Этап 2: БУ считывает второе и третье поколения K_{M-WC} с карточки мастерской и проверяет номера их версий.
- Этап 3: БУ комбинирует K_{M-WC} второго поколения со своим K_{M-VU}, чтобы вычислить K_M и K_{ID}.
- Этап 4: БУ шифрует серийный номер, который оно получило из датчика движения, при помощи K_{ID}.
- Этап 5: Датчик движения сравнивает полученные данные с N_s[1] и не находит соответствия. Затем он сравнивает данные с N_s[2] и находит соответствие. Он делает вывод, что БУ представляет собой БУ второго поколения и передаёт обратно K_P[2].

[1] Следует отметить, что ключи соединения первого, второго и третьего поколений фактически могут быть одним и тем же ключом, или это могут быть три разных ключа различной длины, как поясняется в CSM_117.

12.3. Соединение и связь между БУ и датчиком движения с использованием AES

CSM_218 Как указано в Таблица 3 в разделе 9.2.1, все ключи, участвующие в соединении бортового устройства (второго поколения) и датчика движения и в их последующей связи, представляют собой ключи AES, а не ключи TDES двойной длины, как указано в [ISO 16844-3]. Длина этих ключей AES может быть 128, 192 или 256 бит. Поскольку размер блока AES составляет 16 байтов, длина зашифрованного сообщения должна быть кратной 16 байтам, по сравнению с 8 байтами TDES. Кроме того, некоторые из этих сообщений будут использоваться для передачи ключей AES, длина которых может быть 128, 192 или 256 бит. Таким образом, число байтов данных в одной инструкции в таблице 5 [ISO 16844-3] меняется, как показано в Таблица 6:

Инструкция	**Запрос/ответ**	**Описание данных**	**Число байтов простого текста в соответствии с [ISO 16844-3]**	**Число байтов простого текста с использованием ключей AES**	**Число байтов зашифрованных данных с использованием ключей AES длиной в битах**		
					128	**192**	**256**
10	запрос	Данные аутентификации + номер файла	8	8	16	16	16
11	ответ	Данные аутентификации + содержание файла	16 или 32, в зависимости от файла	16 или 32, в зависимости от файла	16 / 32	16 / 32	16 / 32
41	запрос	Серийный номер MoS	8	8	16	16	16
41	ответ	Ключ соединения	16	16 / 24 / 32	16	32	32
42	запрос	Сеансовый ключ	16	16 / 24 / 32	16	32	32
43	запрос	Информация о соединении	24	24	32	32	32
50	ответ	Информация о соединении	24	24	32	32	32
70	запрос	Данные аутентификации	8	8	16	16	16
80	ответ	Значение счётчика MoS + данные аут.	8	8	16	16	16

Таблица 6 Число байтов простого текста и зашифрованных данных в одной инструкции в соответствии с [ISO 16844-3]

CSM_219 Информация о соединении, передаваемая в инструкциях 43 (запрос БУ) и 50 (ответ MoS), собирается, как указано в разделе 7.6.10 [ISO 16844-3], за исключением того, что алгоритм AES используется вместо алгоритма TDES в схеме шифрования данных соединения, приводя таким образом к двум шифрованным вариантам AES и заполнению, отмеченному в CSM_220, соответствующему размеру блока AES. Ключ K'_P, используемый для такого шифрования, генерируется следующим образом:

- Если длина ключа соединения K_P составляет 16 байтов: $K'_P = K_P \text{ XOR } (N_s||N_s)$
- Если длина ключа соединения K_P составляет 24 байта: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s)$
- Если длина ключа соединения K_P составляет 32 байта: $K'_P = K_P \text{ XOR } (N_s||N_s||N_s||N_s)$

где N_s – 8-байтовый серийный номер датчика движения.

CSM_220 Если длина простого текста (с использованием ключей AES) не кратна 16 байтам, применяется метод заполнения, представленный в [ISO 9797-1].

Примечание: в [ISO 16844-3] число байтов текстовых данных всегда кратно 8, так что при использовании TDES заполнение не является необходимым. Определение данных и сообщений в [ISO 16844-3] в данной части настоящего приложения не изменяется, что обусловливает необходимость применения заполнения.

CSM_221 В инструкции 11 и в случае, когда необходимо зашифровать более одного блока данных, применяется режим сцепления криптоблоков, представленный в [ISO 10116], с параметром чередования $m = 1$. Используется IV

- Относительно инструкции 11: 8-байтовый блок аутентификации, указанный в разделе 7.6.3.3 [ISO 16844-3], заполненный при помощи метода заполнения 2, описанного в [ISO 9797-1]; также см. разделы 7.6.5 и 7.6.6 [ISO 16844-3].
- В случае всех других инструкций, в которых передаётся больше 16 байтов данных, как указано в Таблица 6: ‘00’ {16}, т.е. шестнадцать байтов с двоичным значением, равным 0.

Примечание: Как показано в разделах 7.6.5 и 7.6.6 [ISO 16844-3], когда MoS шифрует файлы данных для их включения в инструкцию 11, блок аутентификации

- Используется как вектор инициализации для шифрования файлов данных в режиме CBC
- И зашифровывается и включается как первый блок в данные, передаваемые в БУ

12.4. Соединение БУ и датчика движения с использованием аппаратуры разных поколений

CSM_222 Как поясняется в разделе 9.2.1, в датчике движения второго поколения может содержаться шифрование данных соединения на базе TDES (в соответствии с частью A настоящего приложения), что позволяет датчику движения соединяться с БУ первого поколения. В таком случае БУ первого поколения и датчик движения второго поколения соединяются, как описано в части A настоящего приложения и в [ISO 16844-3]. В процессе соединения может использоваться карточка мастерской первого или второго поколения.

Примечания:

- БУ второго поколения невозможно соединить с датчиком движения первого поколения.
- Карточку мастерской первого поколения невозможно использовать для соединения БУ второго поколения с датчиком движения.

13. Защита удалённой связи через DSRC

13.1. Общие положения

Как указано в приложении 14, БУ регулярно генерирует данные удалённого контроля тахографа (RTM) и передаёт их в (внутреннее или внешнее) устройство удалённой связи (RCF). Устройство удалённой связи отвечает за передачу таких данных через интерфейс DSRC, описанный в приложении 14, средству удалённого контроля. В приложении 1 указано, что данные RTM представляют собой конкатенацию:

- **Зашифрованных данных тахографа**зашифрованных текстовых данных тахографа
- **Данных безопасности DSRC** описано ниже

Текстовый формат данных тахографа представлен в приложении 1 и более подробно описан в приложении 14. В разделе описана структура данных безопасности DSRC; официальная спецификация содержится в приложении 1.

CSM_223 Текстовые данные `tachographPayload`, передаваемые БУ на средство удалённой связи (если RCF является внешним по отношению БУ) или из БУ на средство удалённого контроля через интерфейс DSRC (если RCF является внешним по отношению к БУ), защищаются в режиме шифрования с последующей аутентификацией, т.е. данные тахографа сначала шифруются, чтобы обеспечить конфиденциальность сообщения, а затем для обеспечения подлинности и целостности данных вычисляется MAC.

CSM_224 Данные безопасности DSRC состоят из конкатенации следующих элементов данных в следующем порядке; см. также Рисунок 12:

- **Текущие дата и время** текущие дата и время БУ (тип данных `TimeReal`)
- **Счётчик** 3-байтовый счётчик, см. CSM_225
- **Серийный номер БУ** серийный номер БУ (тип данных `VuSerialNumber`)
- **Номер версии ключа старшего порядка DSRC** 1-байтовый номер версии ключа старшего порядка DSRC, на основе которого составляются ключи DSRC, связанные с БУ, см. раздел 9.2.2.
- **MAC** значение MAC, вычисляемое по всем прежним байтам в данных RTM.

CSM_225 3-байтовый счётчик в данных безопасности DSRC представлен в формате изначальных MSB. В первый раз когда БУ вычисляет набор данных RTM после начала их производства, значение счётчика устанавливается на 0. Каждый раз перед вычислением следующего набора данных RTM БУ увеличивает значение данных счётчика на 1.

13.2. Шифрование данных тахографа и генерирование MAC

CSM_226 С учётом элемента текстовых данных с типом данных `TachographPayload`, как описано в приложении 14, БУ шифрует эти данные, как показано на Рисунок 12: ключ DSRC БУ для шифрования $K\_VU_{DSRC}\_ENC$ (см. раздел 9.2.2) используется с AES в режиме сцепления криптоблоков (CBC), как описано в [ISO 10116], с параметром чередования $m = 1$. Вектор инициализации равен *IV = текущие дата и время* || *'00 00 00 00 00 00 00 00'* || *счётчик*, где *текущие дата и время* и *счётчик* описаны в CSM_224. Данные, подлежащие шифрованию, заполняются по методу 2, представленному в [ISO 9797-1].

CSM_227 БУ вычисляет MAC в данных безопасности DSRC, как показано на Рисунок 12: MAC вычисляется по всем прежним байтам в данных RTM, до номера версии ключа старшего порядка DSRC включительно, включая также метки и длины объектов данных. БУ использует свой ключ DSRC для аутентификации $K\_VU_{DSRC}\_MAC$ (см. раздел 9.2.2) при помощи алгоритма AES в режиме CMAC, как указано в [SP 800-38B]. Длина MAC связана с длиной ключей DSRC, связанных с БУ, как описано в CSM_50.

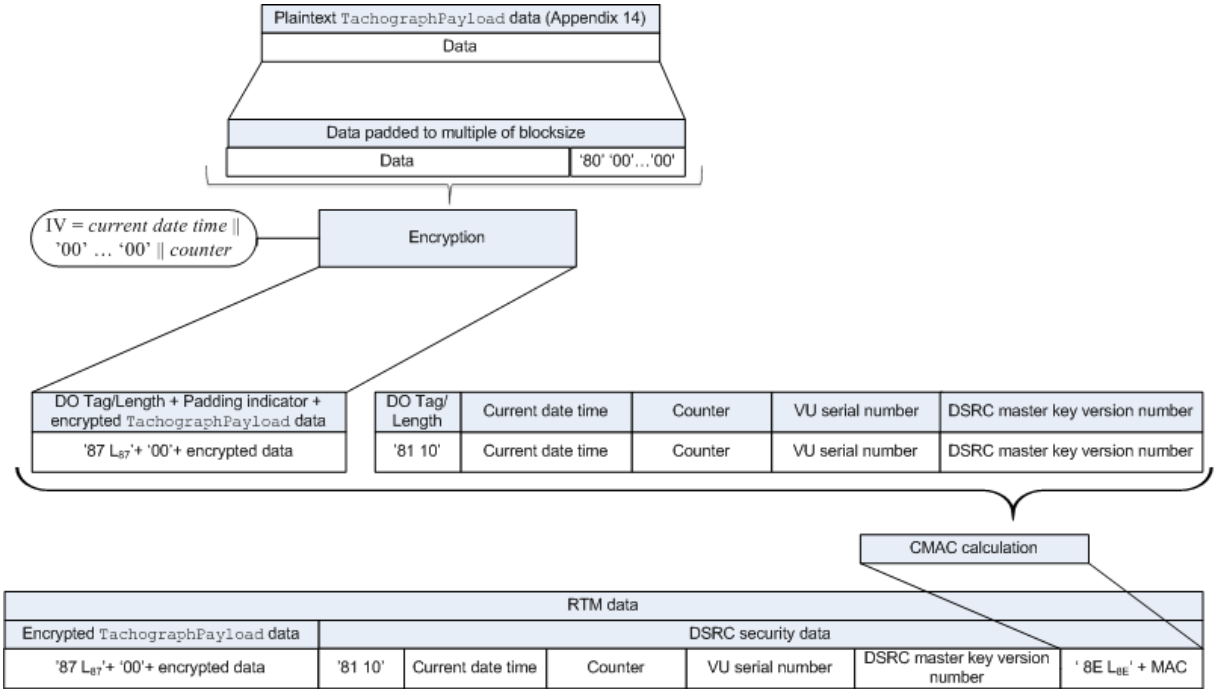


Рисунок 12 Шифрование данных тахографа и генерирование MAC

13.3. Проверка и расшифровка данных тахографа

CSM_228 Когда средство удалённого контроля получает из БУ данные RTM, оно передаёт все данные RTM на контрольную карточку в поле данных команды PROCESS DSRC MESSAGE, как описано в приложении 2. Затем:

1. Контрольная карточка проверяет номер версии ключа старшего порядка DSRC в данных безопасности DSRC. Если контрольной карточке указанный ключ старшего порядка DSRC неизвестен, она возвращает ошибку, указанную в приложении 2, и прекращает процесс.
2. Контрольная карточка использует указанный ключ старшего порядка DSRC в сочетании с серийным номером БУ в данных безопасности DSRC, чтобы получить ключи DSRC, связанные с БУ, K_VU_{DSRC}_ENC и K_VU_{DSRC}_MAC, как указано в CSM_124.
3. Контрольная карточка использует K_VU_{DSRC}_MAC для проверки MAC в данных безопасности DSRC, как указано в CSM_227. Если значение MAC неверно, контрольная карточка возвращает ошибку, указанную в приложении 2, и прекращает процесс.
4. Контрольная карточка использует K_VU_{DSRC}_ENC для расшифровки зашифрованных данных тахографа, как указано в CSM_226. Контрольная карточка убирает заполнение и возвращает расшифрованные данные тахографа средству удалённого контроля.

CSM_229 Для предотвращения повторных атак средство удалённого контроля проверяет свежесть данных RTM, проверяя, чтобы *текущие дата и время* в данных безопасности DSRC слишком существенно не отклонялись от текущего времени средства удалённого контроля.

Примечания:

- Для этого средству удалённого контроля нужен точный и надёжный источник времени.
- Поскольку согласно приложению 14 БУ должно вычислять новый набор данных RTM каждые 60 секунд и часы БУ могут отклоняться от реального времени на 1 минуту, нижний предел свежести данных RTM составляет 2 минуты. Фактическая требуемая свежесть также зависит от точности часов средства удалённого контроля.

CSM_230 Когда мастерская проверяет правильное функционирование DSRC БУ, она передаёт все данные RTM, полученные из БУ, на карточку мастерской в поле данных команды PROCESS DSRC MESSAGE, как описано в приложении 2. Карточка мастерской выполняет все проверки и действия, указанные в CSM_228.

14. Подписание загружаемых данных и проверка подписей

14.1. Общие положения

CSM_231 Данные, полученные из БУ или с карточки за один сеанс загрузки, сохраняются специализированной программируемой аппаратурой (СПА) в виде одного физического файла данных. Данные могут храниться на внешнем носителе. Файл содержит цифровые подписи блоков данных в соответствии с указанными в приложении 7. Файл также содержит следующие сертификаты (см. раздел 9.1):

- При загрузке из БУ:
  - VU_Sign certificate
  - Сертификат MSCA_VU-EGF, содержащий открытый ключ для проверки сертификата VU_Sign
- При загрузке с карточки:
  - Сертификат Card_Sign
  - Сертификат MSCA_Card, содержащий открытый ключ для проверки сертификата Card_Sign

CSM_232 СПА также располагает следующими средствами.

- Если для проверки подписи используется контрольная карточка, как описано на Рисунок 13: Связующий сертификат, объединяющий последний сертификат EUR с сертификатом EUR, период действительности которого непосредственно ему предшествует, если таковые существуют.
- Если проверяется сама подпись: все действительные европейские корневые сертификаты.

Примечание: метод, используемый СПА для извлечения этих сертификатов, в настоящем приложении не указывается.

14.2. Генерирование подписей

CSM_233 Алгоритм подписания для создания цифровых подписей загружаемых данных – ECDSA, как указано в [DSS], с использованием алгоритма хеширования, связанного с размером ключа БУ или карточки, как указано в CSM_50. Формат подписи простой, как указано в [TR-03111].

14.3. Проверка подписей

CSM_234 СПА может проверять подпись загружаемых данных самостоятельно или использовать для этого контрольную карточку. Если используется контрольная карточка, проверка подписи происходит так, как описано на Рисунок 13. Если СПА проводит проверку подписи самостоятельно, проверяются подлинность и действительность всех сертификатов в цепочке сертификатов в файле данных, а также подпись данных по схеме подписи, представленной в [DSS].

Примечания к Рисунок 13:

- Аппаратура, с помощью которой были подписаны подлежащие анализу данные, обозначена буквами EQT.
- Сертификаты EQT и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов VU_Sign или Card_Sign.
- Сертификаты EQT.CA и открытые ключи, указанные на рисунке, предназначены для подписания сертификатов БУ или карточек соответственно.
- Сертификат EQT.CA.EUR, указанный на рисунке – это европейский корневой сертификат, отмеченный в CAR сертификата EQT.CA.
- Сертификат EQT.Link, указанный на рисунке, – это связующий сертификат EQT, если он имеется. Как указано в разделе 9.1.2, это связующий сертификат для новой пары европейских корневых ключей, созданной ERCA и подписанной прежним европейским закрытым ключом.
- Сертификат EQT.Link.EUR – это европейский корневой сертификат, отмеченный в CAR сертификата EQT.Link.

CSM_235 Для вычисления хеша M, передаваемого контрольной карточке в команде PSO:Hash, СПА использует алгоритм хеширования, связанного с размером ключа БУ или карточки, с которых загружаются данные, как указано в CSM_50.

CSM_236 Для проверки подписи EQT контрольная карточка применяет схему подписи, представленную в [DSS].

Примечание: В настоящем документе не указываются конкретные действия, которые следует предпринимать, если подпись файла загружаемых данных невозможно проверить или если проверка была неудачной.

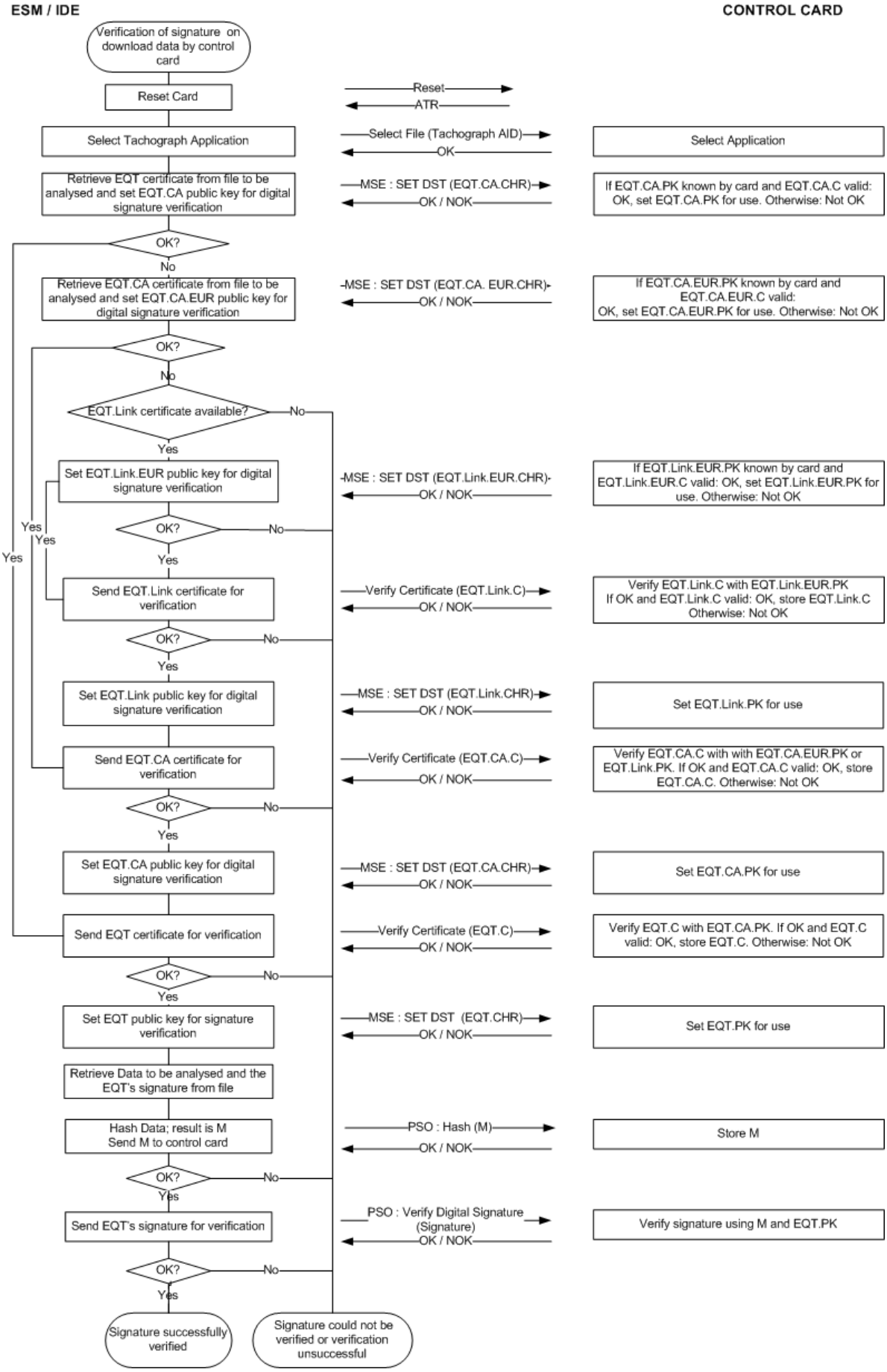


Рисунок 13 Протокол проверки подписи файла загружаемых данных