ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.018— 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Акционерным обществом «РАМЭК-ВС» (АО «РАМЭК-ВС»)

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 026 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 апреля 2018 г. № 207-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Условные обозначения 2
5 Эллиптические кривые 3
6 Вспомогательные функции 4
6.1 Функция вычисления производного ключа 4
6.2 Функция $\pi(Q)$ 4
7 Ключевая система и общие параметры 4
8 Протокол взаимной аутентификации и выработки общего ключа 4
8.1 Механизм взаимной аутентификации 4
8.2 Шаг 1: действия бортового устройства 5
8.3 Шаг 2: действия карты тахографа 5
8.4 Шаг 3: действия бортового устройства 5
8.5 Шаг 4: действия карты тахографа 6
8.6 Шаг 5: действия бортового устройства 7
Приложение А (справочное) Контрольные примеры выполнения протокола выработки общего ключа и выполнения взаимной аутентификации 8
Библиография 16

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические механизмы аутентификации в контрольных устройствах для автотранспорта

Information technology. Cryptographic data security. Cryptographic authentication mechanisms in control devices for motor transports

Дата введения — 2018—09—01

1 Область применения

В настоящих рекомендациях приведено описание криптографического протокола аутентификации и выработки общего ключа, основанного на применении отечественных криптографических преобразований. Предлагаемое решение направлено на обеспечение целостности и аутентичности данных, передаваемых по каналу связи между бортовым устройством и картами тахографа, входящими в состав тахографа, устанавливаемого на транспортные средства.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие документы:

ГОСТ Р 34.10—2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.12—2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13—2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

ГОСТ Р ИСО/МЭК 7816-4—2013 Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена

Р 50.1.113—2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Р 50.1.114—2016 Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на ко-

Издание официальное

торый дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

3.1

бортовое устройство; VU: Контрольное устройство, за исключением датчика движения и электропроводки для подсоединения датчика движения. Бортовое устройство может представлять собой либо единое устройство, либо несколько устройств, установленных в различных местах транспортного средства.

[1, раздел I, пункт oo)]

Примечание — Согласно [2], бортовое устройство содержит в себе программно-аппаратное шифровальное (криптографическое) средство, т. е. средство криптографической защиты информации (блок СКЗИ), реализующее алгоритмы криптографического преобразования информации.

3.2 **карта тахографа;** TC: Карта со встроенной микросхемой, предназначенной для использования в контрольных устройствах (3.3). Карта тахографа позволяет бортовому устройству проверить идентификационные данные держателя карты (или идентификационные данные соответствующей группы) и передавать и хранить данные.

Примечание — Адаптировано из [2], приложение 1, пункт 3.

3.3

контрольное устройство: Комплект оборудования, предназначенный для установки на автотранспортных средствах в целях просмотра, регистрации и хранения в автоматическом и полуавтоматическом режимах данных о движении таких транспортных средств и некоторых периодах работы их водителей.

[1, раздел I, пункт ee)]

Примечания

1 Для целей настоящих рекомендаций термины «контрольное устройство» и «тахограф» являются терминами-синонимами.

2 В состав контрольного устройства входят бортовое устройство (3.1) и следующие внешние компоненты (см. [2]):

- карты тахографа;
- датчик движения;
- антенна для приема сигналов глобальных навигационных спутниковых систем ГЛОНАСС и GPS;
- антенна для приема и передачи сигналов GSM/GPRS (в случае включения в состав бортового устройства модуля связи);
- комплект монтажных частей для соединения компонентов тахографа и их установки на транспортном средстве.

4 Условные обозначения

В настоящих рекомендациях применены следующие обозначения:

V^n — множество всех двоичных строк размерности n, где n — целое неотрицательное число. Нумерация подстрок и компонент строки осуществляется слева направо, начиная с нуля;

V^* — множество всех двоичных строк конечной размерности, включая пустую строку, т. е. для любого $n \geq 0$ выполнено условие $V^n \subset V^*$;

$[Z]_{i,\ldots,j}$ — для битовой строки $Z = (z_0, \ldots, z_{n-1})$, $Z \in V^n$, подстрока $Z' = (z_i, \ldots, z_j)$, $0 \le i \le j \le n-1$;

$A||B$ — конкатенация строк $A \in V^{n_1}$, $B \in V^{n_2}$, т. е. строка, для которой выполнены равенства $A = [A||B]_{0,\ldots,n_1-1}$ и $B = [A||B]_{n_1,\ldots,n_1+n_2-1}$;

$GF(p)$ — для простого числа p — конечное простое поле из p элементов $\{0, 1, \ldots, p-1\}$;

SGN(SK, T) — электронная подпись, выработанная согласно ГОСТ Р 34.10 для сообщения T с использованием ключа электронной подписи SK;

VERIFY(PK, T, S) — результат проверки электронной подписи S согласно ГОСТ Р 34.10 для сообщения T с использованием ключа проверки подписи PK;

ENC(K, I, T) — результат зашифрования сообщения T на ключе K с синхропосылкой I с помощью алгоритма «Магма» ГОСТ Р 34.12 в режиме гаммирования (см. ГОСТ Р 34.13);

DEC(K, I, C) — результат расшифрования шифртекста C на ключе K с синхропосылкой I с помощью алгоритма «Магма» ГОСТ Р 34.12 в режиме гаммирования (см. ГОСТ Р 34.13);

KDF(K, S) — значение функции вычисления производного ключа KDF: $V^{256} \times V^* \to V^{512}$ на основе секретного ключа K и двоичной строки S; способ вычисления этой функции описан в разделе 6;

$HMAC_{512}(K, S)$ — значение функции выработки имитовставки двоичной строки S на секретном ключе K; способ вычисления этой функции описан в Р 50.1.113—2016, пункт 4.1.2;

$\pi(Q)$ — функция, отображающая точку на эллиптической кривой в битовую строку, способ вычисления этой функции описан в разделе 6.

5 Эллиптические кривые

В настоящих рекомендациях использованы вычисления в группе точек эллиптической кривой, определенной над конечным простым полем $GF(p)$. Параметрами эллиптической кривой являются:

$p > 3$ — простое число, определяющее конечное простое поле $GF(p)$;

a, b — коэффициенты эллиптической кривой.

Эллиптическая кривая $E_{a,b}$ задается в короткой форме Вейерштрасса следующим сравнением

$$E_{a,b}(GF(p)) = \{(x, y) : y^2 \equiv x^3 + ax + b \pmod p\} \cup O, \quad (1)$$

где O — бесконечно удаленная точка.

На эллиптической кривой $E_{a,b}$ задается точка P, определяемая:

- своими координатами $P = (x_P, y_P)$, удовлетворяющими сравнению

$$y^2_P \equiv x^3_P + ax_P + b \pmod p; \quad (2)$$

- своим порядком — простым числом q, для которого выполнено условие

$$[q]P = \underbrace{P + \ldots + P}_{q \text{ раз}} = 0. \quad (3)$$

Параметры эллиптической кривой $E_{a,b}$, а также точка P и ее порядок q должны удовлетворять требованиям, накладываемым ГОСТ Р 34.10 на параметры эллиптических кривых при $2^{254} < q < 2^{256}$.

6 Вспомогательные функции

6.1 Функция вычисления производного ключа

В качестве функции вычисления производного ключа

$$KDF: V^{256} \times V^* \rightarrow V^{512} \quad (4)$$

следует использовать псевдослучайную функцию с длиной выхода 512 бит, определенную в Р 50.1.113—2016, подпункт 4.2.1.2.

Отображение KDF определяется равенством

$$KDF(K, S) = HMAC_{512}(K, HMAC_{512}(K, S)||S),$$

где $HMAC_{512}$ — функция вычисления имитовставки, определенная в Р 50.1.113—2016, пункт 4.1.2;

$K \in V^{256}$ — общий ключ, на котором вычисляется имитовставка;

$S \in V^*$ — произвольное сообщение, для которого вычисляется имитовставка.

6.2 Функция $\pi(Q)$

Функция $\pi(Q)$ вычисляется следующим образом: если $Q = (x_Q, y_Q)$ — точка эллиптической кривой, то $\pi(Q) = x_Q$.

7 Ключевая система и общие параметры

Бортовое устройство (*VU*) и карта тахографа (*TC*) обладают:

- идентификаторами участников протокола $VU.CHR \in V^{128}$ и $TC.CHR \in V^{128}$;
- согласованными заранее параметрами *a, b, p* эллиптической кривой $E_{a, b}$, а также точкой $P \in E_{a, b}$, порождающей подгруппу простого порядка *q* (см. раздел 5);
- ключами электронной подписи $VU.SK \in V^{256}$ и $TC.SK \in V^{256}$ соответственно;
- ключами проверки электронной подписи $VU.PK \in V^{512}$ и $TC.PK \in V^{512}$ соответственно;
- сертификатами ключей проверки электронной подписи, подписанными электронной подписью удостоверяющего центра и содержащими в себе как значения ключей проверки электронной подписи (*VU.PK* и *TC.PK* соответственно), так и значения идентификаторов (*VU.CHR* и *TC.CHR* соответственно).

В ходе выполнения протокола взаимной аутентификации вырабатывается общий ключ $K \in V^{256}$, предназначенный для обеспечения конфиденциальности передаваемой информации.

8 Протокол взаимной аутентификации и выработки общего ключа

8.1 Механизм взаимной аутентификации

В основу механизма взаимной аутентификации карты тахографа и бортового устройства положен следующий принцип: каждая сторона должна доказать другой наличие у нее действительной пары ключей, открытый ключ которой сертифицирован общим для участников протокола удостоверяющим центром [1].

Данный механизм запускается со стороны бортового устройства при вводе карты тахографа в считывающее устройство. Процесс начинается с обмена сертификатами и извлечения открытых ключей и завершается созданием общего ключа, используемого для обеспечения конфиденциальности информации, обмениваемой между картой и бортовым устройством. Процесс обмена информацией, а также проверки сертификатов полностью совпадает с регламентируемой [1] последовательностью шагов.

Протокол взаимной аутентификации и выработки общего ключа инициируется бортовым устройством. Протокол представляет собой последовательное выполнение двух команд, направляемых бортовым устройством в карту тахографа, и двух ответов, направляемых картой тахографа в бортовое устройство. Протокол описывается схемой, приведенной на рисунке 1.

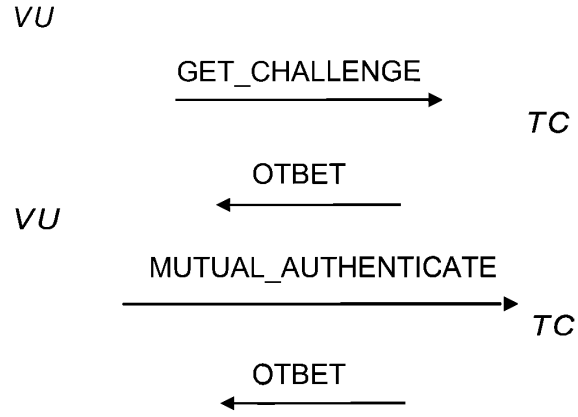

Рисунок 1 — Протокол взаимной аутентификации и выработки общего ключа

На данной схеме использованы пары «команда–ответ» GET_CHALLENGE и MUTUAL_ AUTHENTICATE, форматы и содержание которых устанавливаются в соответствии с ГОСТ Р ИСО/МЭК 7816-4.

8.2 Шаг 1: действия бортового устройства

Бортовое устройство формирует и направляет в карту тахографа команду GET_CHALLENGE.

8.3 Шаг 2: действия карты тахографа

8.3.1 Карта тахографа вырабатывает случайное целое число k_t (последовательность случайных символов, которая может быть интерпретирована как целое число), удовлетворяющее неравенству

$$1 \le k_t \le q - 1, \tag{5}$$

где q — простое число, являющееся порядком подгруппы группы точек эллиптической кривой $E_{a, b}$, порожденной точкой P.

8.3.2 Карта тахографа вырабатывает точку $TC.P$ эллиптической кривой $E_{a, b}$, удовлетворяющую равенству

$$TC.P = [k_t]P. \tag{6}$$

8.3.3 Карта тахографа вычисляет случайную последовательность символов $Nonce_1$ длиной 64 бита (8 байт).

8.3.4 Карта тахографа формирует и направляет в бортовое устройство сообщение M_1, определяемое равенством

$$M_1 = TC.CHR||TC.P\ ||\ Nonce_1. \tag{7}$$

Сообщение M_1 является ответом карты тахографа на команду GET_CHALLENGE.

Примечание — Длина передаваемого сообщения M_1 составляет N + 72 байта, где N — длина идентификатора карты тахографа в байтах.

8.4 Шаг 3: действия бортового устройства

8.4.1 Бортовое устройство проверяет полученное от карты тахографа сообщение M_1. Для этого выполняется последовательность действий по 8.4.1.1 и 8.4.1.2.

8.4.1.1 Проверяется, что содержащееся в сообщении M_1 значение *TC.CHR* совпадает со значением, содержащимся в сертификате открытого ключа карты тахографа.

8.4.1.2. Проверяется[1)], что точка *TC.P* принадлежит эллиптической кривой $E_{a,\,b}$.

8.4.2 Если хотя бы одна из проверок по 8.4.1.1 и 8.4.1.2 не выполнена, то бортовое устройство завершает выполнение протокола, решение об аутентификации карты тахографа не принимается.

8.4.3 Бортовое устройство вырабатывает случайное целое число k_b (последовательность случайных символов, которая может быть интерпретирована как целое число), удовлетворяющее неравенству

$$1 \le k_b \le q - 1, \tag{8}$$

где q — простое число, являющееся порядком подгруппы группы точек эллиптической кривой $E_{a,\,b}$, порожденной точкой P.

8.4.4 Бортовое устройство вырабатывает точку *VU.P* эллиптической кривой $E_{a,\,b}$, удовлетворяющую равенству

$$VU.P = [k_b]P. \tag{9}$$

8.4.5 Бортовое устройство вычисляет точку *VU.Q* на эллиптической кривой $E_{a,\,b}$, удовлетворяющую равенству

$$VU.Q = [k_b]TC.P. \tag{10}$$

8.4.6 Бортовое устройство вычисляет строку

$$VU.T = KDF(\pi(VU.Q), VU.CHR||TC.CHR) \tag{11}$$

и определяет общий ключ K и синхропосылку I равенствами

$$K = [VU.T]_{0,\ldots,255},\ I = [VU.T]_{256,\ldots,287}. \tag{12}$$

8.4.7 Бортовое устройство вычисляет случайную последовательность символов $Nonce_2$ длиной 64 бита (8 байт).

8.4.8 Бортовое устройство формирует строку

$$T_1 = TC.CHR||Nonce_1||Nonce_2||\pi(VU.P)||\pi(TC.P) \tag{13}$$

и вычисляет для нее электронную подпись $S_1 = \mathrm{SGN}(VU.SK, T_1)$.

8.4.9 Бортовое устройство вычисляет значение шифртекста

$$E_1 = ENC(K, I, Nonce_2). \tag{14}$$

8.4.10 Бортовое устройство формирует и направляет карте тахографа сообщение M_2, определяемое равенством

$$M_2 = VU.P||S_1||E_1. \tag{15}$$

Примечание — Сообщение M_2 представляет собой данные, передаваемые карте тахографа в составе команды MUTUAL_AUTHENTICATE. Длина сообщения M_2 составляет 136 байт.

8.5 Шаг 4: действия карты тахографа

8.5.1 Карта тахографа проверяет полученное от бортового устройства сообщение M_2. Для этого выполняется последовательность действий по 8.5.1.1— 8.5.1.5.

[1)] Точка *TC.P* может быть представлена в виде пары своих координат $(x_{TC.P}, y_{TC.P})$. Тогда проверка принадлежности точки кривой состоит в проверке выполнимости сравнения $y^2_{TC.P} \equiv y^3_{TC.P} + ax_{TC.P} + b \pmod p$.

8.5.1.1 Карта тахографа проверяет принадлежность точки $VU.P$ эллиптической кривой $E_{a,\,b}$. Если данное условие не выполняется, решение об аутентификации бортового устройства не принимается, и протокол завершает свою работу.

8.5.1.2 Карта тахографа вычисляет точку $TC.Q$ на эллиптической кривой $E_{a,\,b}$, удовлетворяющую равенству

$$TC.Q = [k_t]VU.P. \tag{16}$$

8.5.1.3 Карта тахографа вычисляет строку

$$TC.T = \mathrm{KDF}(\pi(TC.Q),\ VU.CHR||TC.CHR) \tag{17}$$

и определяет общий ключ K и синхропосылку I равенствами

$$K = [TC.T]_{0,\ldots,255},\ I = [TC.T]_{256,\ldots,287}. \tag{18}$$

8.5.1.4 Карта тахографа расшифровывает значение E_1, вычисляя

$$Nonce'_2 = \mathrm{DEC}(K,\ I,\ E_1). \tag{19}$$

8.5.1.5 Карта тахографа формирует строку

$$T_2 = TC.CHR||Nonce_1||Nonce'_2||\pi(VU.P)||\pi(TC.P) \tag{20}$$

и проверяет электронную подпись под данной строкой, вычисляя значение $\mathrm{VERIFY}(VU.PK,\ T_2,\ S_1)$.

8.5.2 Если подпись верна, то карта тахографа принимает решение об аутентификации бортового устройства. В противном случае решение об аутентификации бортового устройства не принимается, и протокол завершает свою работу.

8.5.3 Карта тахографа вычисляет значение шифртекста

$$E_2 = \mathrm{ENC}(K,\ I,\ Nonce_1). \tag{21}$$

8.5.4 Карта тахографа формирует строку

$$T_3 = VU.CHR||Nonce'_2||E_2||\pi(VU.P)||\pi(TC.P) \tag{22}$$

и вычисляет для нее электронную подпись $S_2 = \mathrm{SGN}(TC.SK,\ T_3)$.

8.5.5 Карта тахографа направляет бортовому устройству значение электронной подписи S_2. Электронная подпись S_2 является ответом карты тахографа на команду MUTUAL_AUTHENTICATE.

Примечание — Длина передаваемого сообщения S_2 составляет 64 байта.

8.6 Шаг 5: действия бортового устройства

8.6.1 Бортовое устройство проверяет полученную от карты тахографа электронную подпись S_2. Для этого выполняются следующие действия.

8.6.1.1 Бортовое устройство вычисляет шифртекст

$$E'_2 = \mathrm{ENC}(K,\ I,\ Nonce_1). \tag{23}$$

8.6.1.2 Бортовое устройство формирует строку

$$T_4 = VU.CHR||Nonce_2||\ E^{t'}\ ||\pi(VU.P)||\pi(TC.P) \tag{24}$$

и проверяет электронную подпись под данной строкой, вычисляя значение $\mathrm{VERIFY}(TC.PK,\ T_4,\ S_2)$.

8.6.2 Если подпись верна, то бортовое устройство принимает решение об аутентификации карты тахографа. В противном случае решение об аутентификации не принимается.

Приложение А
(справочное)

Контрольные примеры выполнения протокола выработки общего ключа и выполнения взаимной аутентификации

А.1 В настоящем приложении приведены три контрольных примера выполнения протокола выработки общего ключа и выполнения взаимной аутентификации (А.3—А.5). Все выводимые далее значения приведены в виде массивов байт, записанных в шестнадцатеричной системе счисления. Слева выведены младшие байты, справа — старшие байты; например, целое число 2^{16} будет записано в следующем виде:

00 00 01

При выводе контрольных значений использованы обозначения, указанные в разделе 4 настоящих рекомендаций.

А.2 Фиксированные параметры

А.2.1 Идентификатор карты тахографа *TC.CHR*:

41 6C 65 78 00 00 00 00 00 00 00 00 00 00 00 00

А.2.2 Идентификатор бортового устройства *VU.CHR*:

45 75 73 74 61 63 65 00 00 00 00 00 00 00 00 00

А.2.3 Параметры эллиптической кривой, используемой для выработки и проверки электронной подписи (значения параметров взяты из тестового примера для ГОСТ Р 34.10—2012, приложение А)

А.2.3.1 Коэффициент *A*:

07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

А.2.3.2 Коэффициент *B*:

7E 3B E2 DA E9 0C 4C 51 2A FC 72 34 6A 6E 3F 56

40 EF AF FB 22 E0 B8 39 E7 8C 93 AA 98 F4 BF 5F

А.2.3.3 Модуль эллиптической кривой *p*:

31 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80

А.2.3.4 Образующая точка *P*:
- координата *x*:

02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- координата *y*:

C8 8F 7E EA BC AB 96 2B 12 67 A2 9C 0A 7F C9 85

9C D1 16 0E 03 16 63 BD D4 47 51 E6 A0 A8 E2 08

А.2.3.5 Порядок образующей точки *q*:

B3 F5 CC 3A 19 FC 9C C5 54 61 97 92 18 8A FE 50

01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80

А.2.4 Эллиптическая кривая для вычисления общего ключа *K* (идентификатор кривой id-tc26-gost-3410-2012-256-paramSetA, значения параметров приняты по Р 50.1.114)

А.2.4.1 Коэффициент *A*:

35 73 7E 27 6F 65 2C B2 33 AA 95 BF 13 20 5E E2

7C A2 35 30 C2 92 48 AF 73 16 98 13 15 3F 17 C2

А.2.4.2 Коэффициент *B*:

13 95 AE F8 A6 37 93 BA F7 7B E1 08 91 CD FC 22

1A D4 A9 59 C3 E7 20 CC 9C ED 28 74 AE 9B 5F 29

А.2.4.3 Модуль эллиптической кривой *p*:

97 FD FF FF FF FF FF FF FF FF FF FF FF FF FF FF

FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

А.2.4.4 Образующая точка *P*:

- координата *x*:

28 AA 2D 74 FE 82 25 8B C7 02 2E 93 96 91 8B 65

BB B2 12 57 42 23 09 88 0D 2C E8 A5 43 84 E3 91

- координата *y*:

5C 2E 32 32 DB 8A 26 AF 40 67 76 44 53 0B DE 5F

56 E9 46 BB C4 86 57 89 75 03 1A AB 23 94 87 32

А.2.4.5 Порядок образующей точки *q*:

67 0C 36 6C 55 AF 15 C1 35 66 7B C8 DF CD D8 0F

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40

А.3 Пример № 1

А.3.1 Ниже указаны ключи подписи и ключи проверки подписи бортового устройства и карты тахографа. Здесь и далее ключами проверки подписи являются точки эллиптической кривой, используемой для выработки и проверки электронной подписи (ГОСТ Р 34.10—2012, приложение А).

А.3.1.1 Ключ подписи *VU.SK* бортового устройства:

70 00 A3 72 DD D2 D4 F7 A3 DC AC 5C D9 7D DA 11

C4 10 EB 1E B8 5F C0 EF 5D B1 C5 BB EF 89 F4 41

А.3.1.2 Ключ проверки подписи *VU.PK* бортового устройства:

- координата *x*:

E6 69 08 D3 00 B0 AD E8 95 B0 56 16 56 0F B2 70

3C 51 F3 07 C4 B8 0A 7D 05 04 93 18 DA D6 2B 3C

- координата *y*:

47 1E 66 DC 13 A3 D5 B6 68 73 77 5D 8A 4D AE 83

79 09 B2 DD 9B 68 FD 6D A0 8A 22 8A 85 79 E4 5E

А.3.1.3 Ключ подписи *TC.SK* карты тахографа:

47 1E 66 DC 13 A3 D5 B6 68 73 77 5D 8A 4D AE 83

79 09 B2 DD 9B 68 FD 6D A0 8A 22 8A 85 79 E4 5E

А.3.1.4 Ключ проверки *TS.PK* подписи карты тахографа:
- координата *x*:

36 0D E7 EC EA BC A2 C9 1A CC BE 49 F4 46 48 AE

5E 34 E6 FB 2F B2 ED 52 D3 23 01 8D C5 2A DD 54

- координата *y*:

EA A7 06 4F D4 D0 AE D0 FD C3 BB 70 21 0D 23 D5

89 14 AD 09 3A 00 6B 7A BD 64 41 D4 2E 45 7C 5F

А.3.2 Поскольку на первом шаге протокола бортовое устройство отсылает не содержащую данных команду GET_CHALLENGE, далее приведены контрольные значения начиная со второго шага протокола.

А.3.3 Шаг 2

А.3.3.1 Случайное значение K_t:

82 BC 52 22 12 F1 48 A3 6C 60 8E 76 C4 CE 6F 07

87 14 7E 32 30 AA BD 7A 66 46 55 3D 0D C3 F9 39

А.3.3.2 Случайная последовательность символов $Nonce_1$:

E3 91 2A C3 AF 19 2B CC

А.3.3.3 Сформированное картой тахографа сообщение M_1:

41	6C	65	78	00	00	00	00	00	00	00	00	00	00	00	00
CD	D5	4E	D5	B3	B8	43	4F	3F	5B	03	9E	58	FE	43	0D
AA	F3	35	C4	67	CF	6B	1A	75	99	51	55	45	EF	4E	3C
BD	44	64	70	34	35	0E	92	FB	AE	12	00	FD	D9	84	6B
7F	81	42	5A	8C	6E	CF	55	BC	A6	94	88	CB	60	68	FF
E3	91	2A	C3	AF	19	2B	CC								

А.3.4 Шаг 3

А.3.4.1 Случайное значение K_b:

9F 3E 3E 71 CB B2 C8 4E 25 9E 8B 38 0D E5 0F BB

06 60 C8 03 52 54 1D B5 B9 D7 34 8E 91 8E 74 42

А.3.4.2 Значение выработанного общего ключа *K*:

1A C3 2E 22 D8 F8 93 75 75 3D A1 0C 86 B3 20 4A

9E 15 12 7E C8 7F 28 AE CD 40 6C 19 8F 39 78 41

А.3.4.3 Значение выработанной синхропосылки *I*:

F7 7F E1 9B

А.3.4.4 Случайная последовательность символов $Nonce_2$:

41 82 DD B5 9B 2C F5 52

А.3.4.5 Случайное значение *k*, используемое при выработке электронной подписи:

5B DA 64 C3 26 76 85 43 26 1D 86 F4 BB C1 23 C0

1C 47 38 6E 5E 5C 90 98 F8 52 72 B9 BA CC 96 18

А.3.4.6 Сформированное бортовым устройством сообщение M_2:

A0	68	49	9E	33	2F	6C	8B	FD	22	CB	3A	5D	6D	5E	9E
38	95	56	7C	5C	54	33	DC	34	F8	3A	09	3B	72	3D	F8
62	7B	EF	0F	97	71	8F	08	4F	22	EA	D0	4B	AD	60	3A
56	68	7B	4C	11	64	BE	FE	2E	B9	09	92	29	11	20	BA
75	A7	39	DA	E0	C9	70	0A	B0	6E	A2	2E	54	55	B9	BA
F0	0E	E6	CA	1E	A4	74	81	0A	39	B4	FC	9B	0C	9D	6E
8B	DD	35	98	DE	00	28	A7	AA	B4	20	01	0C	42	AB	C3
C0	4D	28	5A	DF	4B	09	7A	CD	76	87	5D	C1	F8	96	73
CC	E4	78	BE	B3	9B	8C	8E								

А.3.5 Шаг 4

А.3.5.1 Значение выработанного общего ключа *K*:

1A C3 2E 22 D8 F8 93 75 75 3D A1 0C 86 B3 20 4A

9E 15 12 7E C8 7F 28 AE CD 40 6C 19 8F 39 78 41

А.3.5.2 Значение синхропосылки *I*:

F7 7F E1 9B

А.3.5.3 Случайное значение *k*, используемое при выработке электронной подписи картой тахографа:

DC 58 E5 99 D5 D9 5E 2C AA 27 DE 62 F7 11 56 59

54 D0 C8 BC 28 4A D7 E8 40 D4 01 D9 B0 8C 3A 1D

А.3.5.4 Значение электронной подписи S_2, вычисленное картой тахографа:

CC	96	97	0F	2F	10	68	EB	B0	77	7A	4C	A3	01	DE	A3
45	6B	03	8C	B5	63	D3	AA	AD	19	97	9E	46	5A	D4	48
B9	7B	46	72	E4	F7	17	E0	2D	F9	C0	77	83	0C	1D	05
9A	2F	19	D3	A0	0A	8F	C7	25	3B	D3	84	41	B4	18	3F

А.3.6 Шаг 5

Здесь и далее данный шаг не рассматривается, поскольку заключается в выполнении операций по проверке электронной подписи S_2, выработанной картой тахографа, бортовым устройством.

А.4 Пример № 2

А.4.1 Ниже указаны ключи подписи и ключи проверки подписи бортового устройства и карты тахографа.

А.4.1.1 Ключ подписи *VU.SK* бортового устройства:

77 2B 82 C1 53 24 51 BE 9C 5D A8 BD 43 38 C4 0D

94 24 A4 8F 17 0E C5 5D D3 96 68 9A 36 61 C3 42

А.4.1.2 Ключ проверки подписи *VU.PK* бортового устройства:

- координата *x*:

34 3B 28 9B 71 5E 08 DD 8D 59 56 44 01 D2 1E B6

27 B5 F1 0D 3D 06 B9 86 74 86 92 8A 61 68 21 2B

- координата *y*:

93 B4 4D 1F 4E 52 63 87 C2 94 80 6D 40 27 F8 0D

8C 22 C0 16 58 3B C2 86 A2 36 F8 E4 2F 3B B7 13

А.4.1.3 Ключ подписи *TC.SK* карты тахографа:

49 9A 81 C3 E8 03 12 F5 82 4F DD AE 09 A0 48 03

33 BF 58 7D C1 DA 07 27 E0 B3 32 FA 08 73 2D 03

А.4.1.4 Ключ проверки *TS.PK* подписи карты тахографа:
- координата *x*:

9A 7B 4A CF 70 F3 8D 77 5D A7 2F FB 77 90 37 5B

E5 30 DC 6E 50 B5 21 7D 71 56 B4 E1 74 5C 16 6D

- координата *y*:

B7 DE 06 C0 86 3D 30 C1 A0 EE B7 E9 84 29 84 97

1D 58 19 8C C4 26 57 7D 7B 28 31 96 8A 63 F7 20

А.4.2 Шаг 2

А.4.2.1 Случайное значение K_t:

BA 35 C7 48 D8 F0 A3 32 72 84 8F 94 28 49 38 E7

62 EC 41 9D D5 C3 D6 7C F1 16 67 65 32 D1 60 0C

А.4.2.2 Случайная последовательность символов $Nonce_1$:

1C A1 65 C5 AE 47 7E 0F

А.4.2.3 Сформированное картой тахографа сообщение M_1:

41 6C 65 78 00 00 00 00 00 00 00 00 00 00 00 00
16 D4 0E CC 72 B8 C0 DE 6B B0 A3 2B 12 AC 17 C9
8F B8 33 15 0C 34 3E 45 E5 BA C5 2F EC 3C AC C8
28 AB E2 D5 1F B6 B7 FF EF 0C DE 47 8D 6E 57 54
0D 84 D5 A2 89 C4 55 BA 09 47 F3 2E 4B 58 99 65
1C A1 65 C5 AE 47 7E 0F

А.4.3 Шаг 3

А.4.3.1 Случайное значение K_b:

54 4E 8E DE D0 64 69 94 58 26 73 1E C9 82 7E 1C

6F 5C 44 DB B3 A7 47 C2 2B 54 DF 4C 77 0C 8E 7F

А.4.3.2 Значение выработанного общего ключа *K*:

B6 4E 5A F2 FF A7 CC CD 20 B1 AF F7 39 8E EC A4

BE 7D 38 88 A8 7C EF A7 AB 49 A4 E7 E2 67 7D 44

А.4.3.3 Значение выработанной синхропосылки *I*:

4C AE 1D 70

А.4.3.4 Случайная последовательность символов $Nonce_2$:

46 CA 9F 55 F2 9F 57 4C

А.4.3.5 Случайное значение *k*, используемое при выработке электронной подписи:

DC 12 05 6E 2E 4C E3 F5 FA 0A F9 84 ED A6 63 1C

E4 C5 80 BC 53 74 44 C5 EF D8 96 43 3A 26 5A 28

А.4.3.6 Сформированное бортовым устройством сообщение M_2:

7C 17 94 07 69 39 69 ED 3B BF EB 49 16 A9 D6 23
9F 2B 7F 7B BF 53 7F A9 8E A6 77 BD 9E 8B 4C 91
0A 8F 18 94 33 16 35 03 E2 04 AA A8 7E D7 F0 9B
39 A1 6D 3E BC 64 23 D4 C2 6E F2 9A 7E 43 AD 01
14 E6 12 74 A1 55 92 87 D3 8B A6 1B 50 C0 48 2F
AA 3E 92 39 EC 0E B0 56 81 3B E6 65 0E 1D 9B 2B
CC 38 FE 22 95 B0 42 FF 6C 2F 93 FF 53 1F BA 16
99 C9 D8 67 14 9F 21 B4 66 3F E6 68 68 2E EE 04
9C 74 1F CA FE B2 46 84

А.4.4 Шаг 4

А.4.4.1 Значение выработанного общего ключа *K*:

B6 4E 5A F2 FF A7 CC CD 20 B1 AF F7 39 8E EC A4

BE 7D 38 88 A8 7C EF A7 AB 49 A4 E7 E2 67 7D 44

А.4.4.2 Значение синхропосылки *I*:

4C AE 1D 70

А.4.4.3 Случайное значение *k*, используемое при выработке электронной подписи картой тахографа:

51 0A 01 5F 57 17 22 9C 39 5E 1D 59 0F 97 1C E8

FE A2 9E 88 85 92 81 B4 CA E1 7D 01 86 EC 69 E7

А.4.4.4 Значение электронной подписи S_2, вычисленное картой тахографа:

E3 E1 5B 40 17 1B BA 0F 1F 8D 2D B8 95 D9 7C 65
C8 D7 0D 29 0E D9 E8 2E CA 8B 10 DF 42 A7 43 6E
6C 28 CB 46 E2 42 CA 66 B5 DF EF 2A D7 E9 5A 9B
FE 91 CF 14 37 C5 07 1C 19 C9 EC ED 1B E1 DA 50

А.5 Пример № 3

А.5.1 Ниже указаны ключи подписи и ключи проверки подписи бортового устройства и карты тахографа.

А.5.1.1 Ключ подписи *VU.SK* бортового устройства:

DA 20 AA 7D 0C 06 A9 CB 7E A9 61 96 70 5B 4C E4

75 52 58 5B 0D B1 C0 64 1E D1 2D 9A EB 78 77 5B

А.5.1.2 Ключ проверки подписи *VU.PK* бортового устройства:

- координата *x*:

32 15 0F D3 74 35 31 3C 82 41 E8 05 D3 AD DE D8

A9 94 80 99 89 BE 4F AF 3B 94 35 9E 24 AA 04 0E

- координата *y*:

95 B3 B9 9F F1 8D A6 C1 5D C2 B9 85 08 05 87 DE

AC 38 74 55 DD 60 B3 27 02 BF C8 17 89 21 08 6C

А.5.1.3 Ключ подписи *TC.SK* карты тахографа:

F7 41 CC 90 9D 63 0C AB 60 E7 D8 72 6E 8A 2E 81

16 D1 A8 2C C2 35 C6 A6 5A 13 29 72 EF 36 0F 6F

А.5.1.4 Ключ проверки *TS.PK* подписи карты тахографа:
- координата *x*:

2E 5F A8 E0 E9 AE FB D5 5C 8B EB D8 84 AD E4 7B

A3 DF 1F DB B9 43 F3 AC 50 57 5C 3A 84 7B A0 58

- координата *y*:

B4 09 16 A8 F0 DA 38 2D 90 E6 D8 5F E1 58 36 34

64 27 52 7E F5 59 41 31 1C 0F 24 54 73 D8 D4 44

А.5.2 Шаг 2

А.5.2.1 Случайное значение K_t:

EB 58 97 C6 56 4B CE 01 39 73 1C A8 72 F5 79 DC

5E 15 E8 30 14 97 19 34 31 93 FF 1D 49 B0 E5 6B

А.5.2.2 Случайная последовательность символов $Nonce_1$:

4B 3F 58 EB 0D B5 AF 1F

А.5.2.3 Сформированное картой тахографа сообщение M_1:

41	6C	65	78	00	00	00	00	00	00	00	00	00	00	00	00
FA	61	B0	22	99	0D	AA	05	13	4C	9E	82	0D	18	C7	41
47	45	1E	03	C1	1B	FF	EC	FA	16	BF	9B	D1	32	36	EC
B0	B9	09	94	7B	BF	10	B2	CE	51	E5	47	64	B7	71	88
3E	EA	44	A2	72	FF	AD	73	3C	9B	57	71	CD	10	B1	3E
4B	3F	58	EB	0D	B5	AF	1F								

А.5.3 Шаг 3

А.5.3.1 Случайное значение K_b:

34 2F 1B 9C DE 00 76 FC E7 10 0A DE 97 B1 99 D0

94 12 86 DA 3C 07 BC 69 7A 50 8A 4C 5D EE 4C 4D

А.5.3.2 Значение выработанного общего ключа *K*:

92 CD 6B A5 D1 05 00 04 3C 5C 57 15 10 2C 56 6A

60 80 3B A0 DC 0D 7A 55 28 15 9B E8 AB A9 15 46

А.5.3.3 Значение выработанной синхропосылки *I*:

34 88 D5 94

А.5.3.4 Случайная последовательность символов $Nonce_2$:

92 ED 44 3A B1 4A 09 11

А.5.3.5 Случайное значение k, используемое при выработке электронной подписи:

36 15 97 79 20 A8 1A 0E 78 26 EB 9C 38 EB FA FD

7B B4 89 CB AE 70 AC AC F9 C5 21 05 BB C4 C4 55

А.5.3.6 Сформированное бортовым устройством сообщение M_2:

37	8A	53	2C	1D	10	54	5B	D9	B1	AE	65	FC	84	7E	30
C3	DA	CA	C3	DE	56	6B	ED	8D	56	C4	70	BA	BE	49	F4
FA	D5	2F	51	0D	74	78	52	FB	45	B0	21	04	43	58	3A
EA	C2	D3	87	FF	F6	54	E0	24	1E	65	2D	60	2C	5F	5A
D8	AC	13	2B	55	42	83	51	49	5F	83	B6	F5	9F	A9	9C
6E	5A	F3	6D	61	FF	98	BD	AD	9A	6C	10	D0	26	20	42
DD	7C	0C	E4	8F	65	2B	60	B9	79	9E	E5	66	A3	9D	E1
7D	19	F0	35	80	7E	44	C9	0F	61	6C	4F	33	25	1A	3E
BD	94	03	85	A1	47	02	2F								

А.5.4 Шаг 4

А.5.4.1 Значение выработанного общего ключа K:

92 CD 6B A5 D1 05 00 04 3C 5C 57 15 10 2C 56 6A

60 80 3B A0 DC 0D 7A 55 28 15 9B E8 AB A9 15 46

А.5.4.2 Значение синхропосылки I:

34 88 D5 94

А.5.4.3 Случайное значение k, используемое при выработке электронной подписи картой тахографа:

C1 DB E8 1A 6F D3 3F 5C 06 EA 72 D6 A3 8C 9A 67

C5 DB 41 C4 BE 6F 44 C2 3E B9 5E D8 73 C5 ED 59

А.5.4.4 Значение электронной подписи S_2, вычисленное картой тахографа:

D1	73	5E	14	66	60	66	57	94	89	73	00	7B	D3	FF	DE
93	AD	EF	62	9B	0D	39	A4	05	39	1D	50	BB	69	20	4D
01	38	F9	34	23	E3	E0	97	22	7B	50	BD	28	A1	C0	4E
E5	5C	8A	04	64	4E	6F	53	E6	46	F0	C8	F4	9D	E8	79

Библиография

[1] Добавление 1В к приложению ЕСТР, содержащее требования к конструкции, испытаниям, установке и инспекции цифрового контрольного устройства, используемого на автомобильном транспорте // Европейское соглашение, касающееся работы экипажей транспортных средств, производящих международные автомобильные перевозки (Европейская экономическая комиссия. Комитет по внутреннему транспорту) (ЕСТР/AETR). — ECE/TRANS/SC.1/2006/2/Add.1. — 2008

[2] Приказ Министерства транспорта Российской Федерации от 13 февраля 2013 г. № 36 «Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства»

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: криптографическая защита информации, криптографическая аутентификация, тахограф, бортовое устройство, контрольное устройство, общий ключ, протокол

БЗ 4–2018/25

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.04.2018. Подписано в печать 08.05.2018. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
123001 Москва, Гранатный пер., 4. gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru