Виктор С. Горбатов¹, Игорь Ю. Жуков², Олег Н. Мурашов²
¹*Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, ORCID 0000-0001-9998-9733*
²*ООО «Национальный мобильный портал»,
Волгоградский пр., 2, офис 36, Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, ORCID 0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, ORCID 0000-0002-4467-2170*

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ И ВЫРАБОТКИ ОБЩЕГО
КЛЮЧА КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА
DOI: <http://dx.doi.org/10.26583/bit.2017.4.03>

Аннотация. В работе описывается протокол выработки общего ключа с аутентификацией абонентов, предназначенного для использования в бортовых устройствах (тахографах), которые устанавливаются на транспортные средства с целью обеспечения транспортной безопасности дорожного движения. Данный протокол основан на применении известных отечественных криптографических преобразований и направлен на обеспечение целостности и аутентичности данных, передаваемых по каналу связи между бортовым устройством и картами тахографа, входящими в состав контрольных устройств автотранспортных средств. Протокол разработан в соответствии с рекомендациями Росстандарта по принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, оформлен в виде проекта национального стандарта, предлагаемого для общественного обсуждения и утверждения в установленном порядке. Основным результатом данного исследования является формулирование определенных свойств безопасности, идентичных тем задачам, которые ставит перед собой нарушитель с целью его компрометации. Учет методов компрометации позволяет уже на этапе создания протокола заложить в него структурные особенности, обеспечивающие выполнение заданных свойств безопасности и последующее обоснование их достаточности.

Ключевые слова: безопасность транспорта, бортовое устройство, криптографический протокол, механизмы аутентификации, свойства безопасности

Для цитирования. ГОРБАТОВ, Виктор С; ЖУКОВ, Игорь Ю; МУРАШОВ, Олег Н. КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ АУТЕНТИФИКАЦИИ И ВЫРАБОТКИ ОБЩЕГО КЛЮЧА КОНТРОЛЬНЫХ УСТРОЙСТВ АВТОТРАНСПОРТА. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 27-34, nov. 2017. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/274>>. Дата доступа: 28 nov. 2017. doi:<http://dx.doi.org/10.26583/bit.2017.4.03>.

Victor S. Gorbatov¹, Igor Y. Zhukov², Oleg N. Murashov²
¹*National Research Nuclear University MEPHI
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, ORCID 0000-0001-9998-9733*
²*Ltd «The National Mobile Portal», Volgogradskiy pr., 2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, ORCID 0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, ORCID 0000-0002-4467-2170*

**Authentication and common key generation cryptographic protocol for vehicle
tachographs**

DOI: <http://dx.doi.org/10.26583/bit.2017.4.03>

Abstract. We present a public key generation protocol. The key is used for subscriber authentication in tachographs installed on vehicles in order to provide traffic safety. The protocol is based on the well-known Russian cryptographic algorithms. It ensures integrity and authenticity of data transmitted through communication channel between the on-board devices

and vehicle tachograph cards. The protocol was developed in accordance with the Rosstandart recommendations and complies with the development and modernization principles for data protection encryption (cryptographic) means. The protocol was suggested as a national standard draft and is open for public discussion in accordance with the established procedure.

The main results of our study is the formulation of certain security tasks identical to those used by potential infringers to compromise the protocol. This allows one to account for structural features that will ensure further protocol compliance to the target security characteristics, as well as to guarantee subsequent justification of feature set sufficiency.

Keywords: Smart Building, Management Systems, Internet of Things (IoT)

For citation. GORBATOV, Victor S.; ZHUKOV, Igor Y.; MURASHOV, Oleg N.. Authentication and common key generation cryptographic protocol for vehicle tachographs. IT Security, [S.l.], v. 24, n. 4, p. 27-34, nov. 2017. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/274>>. Date accessed: 28 nov. 2017. doi:<http://dx.doi.org/10.26583/bit.2017.4.03>.

1 Взаимная аутентификация

Контрольное устройство автотранспорта – комплект оборудования, предназначенный для обеспечения транспортной безопасности дорожного движения путем перманентной регистрации его основных параметров [1], в частности данных о движении транспортных средств и некоторых периодах работы их водителей. Обычно под контрольным устройством понимается тахограф, как некое бортовое устройство и внешние компоненты [2]: карта тахографа с встроенной микросхемой, предназначенной для проверки идентификационных данных держателя карты (или идентификационные данные соответствующей группы), передачи и хранения данных [1, 2], датчик движения, антенна для приема сигналов глобальных навигационных спутниковых систем и прочее.

Согласно нормативному документу отечественного государственного регулятора в области транспортной безопасности [2] бортовое устройство должно содержать в себе программно-аппаратное шифровальное (криптографическое) средство (блок СКЗИ), реализующее алгоритмы криптографического преобразования информации [2] и обеспечивающее следующие функции: аутентификацию; регистрацию информации в некорректируемом виде в защищенной памяти (защищенный архив блока СКЗИ); хранение конфиденциальной информации, используемой для создания электронной подписи и ее проверки (далее - ключевой информации), а также аутентифицирующей информации.

В основу механизма взаимной аутентификации карты тахографа и бортового устройства положен следующий принцип [1]: каждая сторона должна доказать другой наличие у нее действительной пары ключей, открытый ключ которой сертифицирован общим для участников протокола Удостоверяющим центром. 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 сеансового ключа, используемого для обеспечения конфиденциальности передачи информации 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 и представляет собой последовательное выполнение двух команд, направляемых бортовым устройством в карту тахографа, и двух ответов от тахографа в бортовое устройство. Карта тахографа проверяет полученное от бортового устройства сообщение и, 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. Бортовое устройство также проверяет полученную от карты тахографа электронную подпись. Если подпись верна, то бортовое устройство принимает решение об аутентификации карты тахографа. В противном случае решение об аутентификации не принимается.

Протокол разработан в соответствии с рекомендациями [3], оформлен в виде проекта национального стандарта [4] и предлагается для общественного обсуждения и дальнейшего утверждения в установленном порядке.

2 Модель нарушителя

С целью обоснования достаточности общепринятых мер криптографической защиты, рекомендуемых для выполнения протокола взаимной аутентификации [3,4] необходимо уточнить модель нарушителя, то есть определить какими возможностями обладает нарушитель и какие задачи ставит перед собой нарушитель, для того чтобы скомпрометировать анализируемый протокол. Традиционно, при анализе криптографических протоколов исследуются возможности нарушителя с использованием модели Долева-Яо [5]. В ней нарушитель может перехватывать все сообщения, передаваемые в ходе протокола, а также производить накопление переданной информации, которая может быть использована для его компрометации. Как известно такой метод компрометации протокола принято называть «пассивным».

Учитывая, что бортовое устройство при общении с картой тахографа использует, как правило, контактный чип, можно допустить, что нарушитель перехватывает всю передаваемую информацию, используя для этого сигналы электромагнитного излучения или специальные технические средства перехвата обмена информацией между участниками протокола. Вопросы противодействия установке на бортовые устройства технических средств перехвата передаваемой информации выходят за рамки настоящего исследования и будут рассмотрены отдельно.

Кроме пассивного перехвата, традиционно, в модели Долева-Яо нарушитель обладает определенными возможностями по модификации, навязыванию, подмене передаваемых сообщений, используя для этого либо накопленную ранее информацию, либо производя вычисления в процессе выполнения протокола. Кроме того, нарушитель может организовывать одновременное выполнение некоторого числа сессий выполняемого протокола. Сессии могут выполняться одновременно как для инициатора протокола (в нашем случае, это бортовое устройство), так и для отвечающей стороны (это карта тахографа). При этом нарушитель может использовать информацию, передаваемую в ходе всех выполняемых сессий протокола. Такой метод компрометации протокола принято называть «активным».

Рассматривая данную модель применительно к исследуемому протоколу, необходимо заметить, что в силу технических особенностей реализации, в каждый период времени бортовое устройство и/или карта тахографа могут находиться в состоянии выполнения только одной сессии протокола. С другой стороны, мы можем считать, что нарушитель может использовать специальное техническое устройство, которое может служить каналом передачи и обработки информации, эмулирующим работу одной карты для нескольких легитимных бортовых устройств, и одновременно, работу бортового устройства для нескольких легитимных карт тахографа. В остальном, мы будем считать, что все возможности модели Долева-Яо для нарушителя доступны.

3 Свойства безопасности протокола

Будем называть задачи, которые ставит перед собой нарушитель, свойствами безопасности, и будем считать, что нарушение этих свойств и приводит к компрометации протокола. Поскольку в настоящее время нет единой общепринятой системы классификации свойств безопасности, далее будем придерживаться классификации, изложенной в книгах [5-7]. В соответствии с ней отобраны следующие свойства безопасности:

1. Сложность компрометации ключевой системы (keysecurity)

Трудоемкость определения общего сеансового ключа К, вырабатываемого в ходе выполнения протокола, должна быть достаточно высокой, сравнимой с трудоемкостью компрометации алгоритма шифрования, для которого вырабатывается ключ. В работе [2] было высказано замечание, что указанным свойствам должен удовлетворять произвольный протокол выработки общего ключа в предположении, что для взаимной аутентификации абонентов используются долговременные ключи. В нашем случае в качестве долговременных ключей выступают ключи электронной подписи, обозначаемые в тексте рекомендаций по стандартизации [3] соответственно ТС.К и VU.К.

2. Сложность определения долговременных ключей (longtermkeyssecurity)

Трудоемкость определения долговременных ключей электронной подписи ТС.SK, VU.SK должна быть настолько высокой, чтобы обеспечивать функционирование тахографа, использующего протокол, в течение достаточно большого интервала времени.

3. Защита от чтения вперед/назад (knownkeysecurity)

Каждая сессия выполнения протокола должна вырабатывать уникальный общий сеансовый ключ К. Ситуация, при которой один или несколько общих ключей, выработанных в разных сеансах выполнения протокола, станут известны нарушителю, не должна приводить к компрометации общих ключей, вырабатываемых в других сеансах.

4. Защита при компрометации долговременных ключей (forwardsecrecy)

Компрометация долговременных ключей – ключей электронной подписи ТС.SK, VU.SK не должна приводить к компрометации общих ключей, выработанных ранее.

5. Подтверждение ключа (keyconfirmation)

После выработки общего сеансового ключа К каждый из абонентов – бортовое устройство и карта тахографа должны обладать уверенностью в том, что другой абонент обладает тем же общим сеансовым ключом К.

6. Взаимная аутентификация участников протокола (mutualauthenticate)

Каждая сторона должна доказать другой стороне наличие у нее действительного секретного ключа, однозначно связанного с доверенным открытым ключом.

7. Защита от подмены владельца ключа (KCI, keycompromiseimpersonation)

Допустим, что долговременный ключ карты тахографа ТС.SK скомпрометирован и известен нарушителю, а сертификат соответствующего открытого ключа ТС.РК еще не помещен в список отозванных сертификатов, доступных бортовому устройству. В этом случае нарушитель, очевидно, может выдавать себя за владельца скомпрометированной карты перед бортовым устройством. Вместе с тем, подобная ситуация не должна приводить к тому, чтобы нарушитель мог выдавать себя за бортовое устройство перед законным владельцем скомпрометированной карты. Аналогичное свойство должно выполняться в случае, если нарушителю удастся компрометировать долговременный ключ VU.SK бортового устройства.

8. Защита от выработки ключа с третьим участником протокола (unknownkeyshare)

В случае выполнения данного свойства безопасности не должна возникать ситуация при которой бортовое устройство (карта тахографа) считает, что вырабатывает общий секретный ключ с легитимной картой тахографа (бортовым устройством) А, а на самом деле вырабатывает общий секретный ключ с некоторой другой, то же легитимной, картой (бортовым устройством) В.

9. Защита от навязывания ключевых значений (nokeycontrol)

Ни один из участников протокола не может навязать значение общего секретного ключа по своему выбору другому участнику протокола.

Перечисленные свойства безопасности можно условно разделить на две группы: первая накладывает требования к стойкости протокола и невозможности компрометации нарушителем ключевой системы. Вторая группа носит функциональный характер и накладывает требования к аутентификации участников протокола, корректности и качеству выработанного ключа. Таким образом атаки, с помощью которых нарушитель может попытаться нарушить свойства безопасности, можно разделить на два больших класса:

- 1) пассивные атаки;
- 2) активные атаки, включая временные атаки, основанные на изучении накопленной информации.

Такое представление помогает в исследовании достаточности мер защиты протокола от компрометации, что и будет использовано в дальнейшем исследовании.

4 О выполнении свойств безопасности

Одним из подходов к анализу протоколов является систематическое исследование практических приемов компрометации и разработка определенного перечня принципов и положений, позволяющих предотвратить известные атаки. Их классификации и методы компрометации протоколов могут быть найдены в различных источниках, например, в работах [5-7]. Учет методов компрометации протоколов позволяет уже на этапе создания протокола заложить в него структурные особенности, обеспечивающие защиту и выполнение изложенных ранее свойств безопасности. Рассмотрим эту возможность для ряда указанных выше свойств безопасности применительно к исследуемому протоколу.

4.1 Защита от чтения вперед/назад

Данное свойство безопасности предъявляется к протоколам для того, чтобы в случае компрометации общего секретного ключа, выработанного в одном из сеансов протокола, обеспечить секретность передаваемой в других сеансах протокола информации. Единственное, что может связывать в исследуемом протоколе общие сеансовые ключи, выработанные в различных сеансах — датчик случайных чисел. Если предположить, что используемый в программно-аппаратной реализации протокола датчик случайных чисел вырабатывает псевдослучайные последовательности, статистически неотличимые от равновероятных, то можно утверждать, что вырабатываемые абонентами точки ТС.Р и VU.Р также равновероятны. В этом случае общие ключи, вырабатываемые в различных сеансах протокола, также могут рассматриваться как независимые случайные величины, равномерно распределенные в V256. Поэтому невозможно построить методы определения общих секретных ключей, отличные от случайного угадывания и можно считать, что для исследуемого протокола выполняется третье свойство безопасности.

4.2 Независимость общего ключа от долговременных ключей абонентов

Долговременными ключами протокола являются ключи электронной подписи абонентов. Поскольку информация об этих ключах никак не используется при генерации общего секретного ключа, можно считать, что для исследуемого протокола выполнено четвертое свойство безопасности.

4.3 Подтверждение ключа

Предложенный протокол обеспечивает явное подтверждение ключа, так как после его завершения каждая из сторон VU и ТС удостоверяется в том, что другая сторона

успешно выработала общий ключ. Вероятность ложного подтверждения ключа не превосходит вероятности подбора верного шифртекста для заданного открытого текста при неизвестном ключе и синхропосылке, то есть не превосходит 2-64. Следовательно, можно считать, что для исследуемого протокола выполнено и пятое свойство безопасности.

4.4 Противодействие KCI-атаке

Под KCI-атакой (имперсонификация при компрометации долговременного секретного ключа) понимается [7] атака, при выполнении которой противник, получивший доступ к долговременному секретному ключу абонента А, может выдать себя перед А за любого другого абонента. Если протокол противостоит KCI-атаке, то для него выполнено седьмое свойство безопасности из перечисленного выше перечня свойств. В исследуемом протоколе, при условии стойкости схемы электронной подписи ГОСТ Р 34.10-2012 доступ противника к долговременному секретному ключу TC.SK не даст ему возможности подделать цифровую подпись S1 на шаге 3 протокола, поскольку та зависит от секретного ключа VU.SK. Одновременно, доступ к долговременному секретному ключу VU.SK не даст ему возможности подделать цифровую подпись S2 на шаге 4 протокола, зависящую от секретного ключа TC.SK. Исключением является случай совпадения двух секретных ключей, $VU.SK = TC.SK$. Если противник пытается выдать себя перед абонентом за него самого (т.е., например, перед VU за VU), то по определению KCI-атаки он имеет доступ к секретному ключу VU.SK и может полностью имитировать его действия, но этот случай является «вырожденным». В противном случае вероятность совпадения двух случайно выбранных секретных ключей можно оценить величиной $1/q$.

4.5 Противодействие UKS-атаке

Под UKS-атакой понимается [8] инцидент, в результате которого абоненты вырабатывают общий ключ, но один из них считает его общим с третьим абонентом. При этом компрометации общего ключа как таковой не происходит, но нарушаются требования, связанные с аутентификацией абонентов. Если протокол противостоит UKS-атаке, то для него выполнено восьмое свойство безопасности. Для противодействия указанному виду инцидентов в протоколе следует использовать функцию выработки производного ключа, зависящего от идентификаторов абонентов. Таким образом, в поток сообщений исследуемого протокола включена функция, связывающая сеанс с идентификаторами конкретных абонентов. Для реализации UKS-атак может быть использовано свойство DSKS – Duplicate Signature Key Selection, которым обладают многие схемы цифровой подписи [9], в том числе и ГОСТ Р 34.10-2012. Указанное свойство состоит в возможности для заданного сообщения M и подписи (r, s) подобрать параметры схемы подписи, в данном случае точку эллиптической кривой P' порядка q, а также секретный ключ SK' такие, что подпись (r, s) будет признана корректной подписью, выработанной при помощи ключа SK', но с отличными параметрами схемы. Для противодействия UKS-атакам, основанным на данном свойстве схемы цифровой подписи ГОСТ Р 34.10-2012, в поток сообщений исследуемого протокола включено вычисление подписей от строк, содержащих в качестве подстроки E1, E2, вычислить которые без знания общего ключа возможно лишь с пренебрежимо малой вероятностью. Таким образом, без знания общего ключа противник не имеет доступа к сообщениям, под которыми ему необходимо подделать подписи для успешной аутентификации. По нашему мнению, для повышения уровня защищенности анализируемого протокола необходимо использовать эллиптические кривые, либо соответствующие рекомендациям по стандартизации Р 50.114-2016, либо получившие положительное заключение государственного регулятора по результатам их криптографических исследований.

4.6 Защита от навязывания

Данное свойство безопасности позволяет каждому из участников протокола быть уверенным в том, что второй участник протокола не навязал ему ключ, выработанный заранее. В генерации общего секретного ключа принимает участие величина $\pi(Q)$, где Q общая для абонентов секретная точка эллиптической кривой. Значения координат этой точки существенным образом зависят от двух случайных значений, вырабатываемых независимо двумя участниками в ходе выполнения протокола. Это не позволяет кому-либо из участников протокола навязать другому значение точки Q , а, следовательно, и общего секретного ключа. Следовательно, мы можем считать, что для исследуемого протокола выполнено девятое свойство безопасности.

Заключение

Таким образом, в исследуемом криптографическом протоколе аутентификации и выработки общего ключа контрольных устройств автотранспорта уже заложены структурные свойства, позволяющие обеспечить выполнение ряда свойств безопасности и предусмотреть методы защиты от большого класса известных атак. Следующим этапом исследования должно стать полное обоснование достаточности мер противодействия известным атакам и методам компрометации исследуемого протокола с целью рекомендации для его практического применения.

СПИСОК ЛИТЕРАТУРЫ:

- 1 Европейское соглашение по работе экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР). Европейская экономическая комиссия. Комитет по внутреннему транспорту. Записка секретариата. Добавление 1В к приложению ЕСТР, содержащее требования к конструкции, испытаниям, установке и инспекции цифрового контрольного устройства, используемого на автомобильном транспорте. – ECE/TRANS/SC.1/2006/2/Add.1. – 2008.
- 2 Приказ Минтранса России от 13 февраля 2013г. №36. Эл. Ресурсы: http://www.mintrans.nso.ru/sites/mintrans.nso.ru/wodby_files/files/wiki/2014/12/prikaz_36_13.pdf. Дата обращения 06.06.2017.
- 3 Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. — 2016. — 36 стр.
- 4 Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Криптографические механизмы аутентификации для применения в контрольных устройствах, обеспечивающих работу автотранспорта (Проект второй редакции). — 2017. — 21 стр.
- 5 Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. — М.:Академия. — 2009. — 272 с.
- 6 Boyd C., Mathuria A. Protocols For Authentication And Key Establishment: Springer. — 2003. — 323 p.
- 7 Нестеренко А.Ю. Новый протокол выработки общего ключа. Системы высокой доступности. — № 2. — 2012. — стр. 81-90.
- 8 Diffie W., van Oorschot P., Wiener M. Authentication And Authenticated Key Exchanges. Designs. — 1992. — 2. — P. 107-125.
- 9 BaekJ., KimK. Remarks. On The Unknown Key-Share Attacks//IEICE Trans. — 2000. — E83-A. — № 12. — P. 99-106.

REFERENCES:

- [1] European agreement on work of crews of vehicles engaged in international road transport (AETR). Economic Commission for Europe. The inland transport Committee. Note by the Secretariat. Appendix 1B to the Annex to the AETR related to requirements for construction, testing, installation, and inspection of the digital control device used in road transport.. – ECE/TRANS/SC.1/2006/2/Add.1. – 2008.
- [2] Prikaz Mintransa Rossii ot 13 fevralya 2013 g. № 36. EHL. resurs http://www.mintrans.nso.ru/sites/mintrans.nso.ru/wodby_files/files/wiki/2014/12/prikaz_36_13.pdf. Data obrashcheniya 06.06.2017. (In Russian).
- [3] Rosstandart. Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Rekomendacii po standartizacii. Principy razrabotki i modernizacii shifroval'nyh (kriptograficheskikh) sredstv zashchity informacii. — 2016. — 36 p. (In Russian).

- [4] Rosstandart. Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Rekomendacii po standartizacii. Kriptograficheskie mekhanizmy autentifikacii dlya primeneniya v kontrol'nyh ustroystvah, obespechivayushchih rabotu avtotransporta (Proekt vtoroj redakcii). — 2017. — 21 p. (In Russian).
- [5] SHERemushkin A.V. Cryptographic protocols. The main characteristics and vulnerabilities.. — М.:Akademiya. — 2009. — 272 p. (In Russian).
- [6] Boyd C., Mathuria A. Protocols For Authentication And Key Establishment: Springer. — 2003. — 323 p.
- [7] Nesterenko A.YU. The new Protocol develop common key. Sistemy vysokoj dostupnosti. — № 2. — 2012. — P. 81-90. (In Russian).
- [8] Diffie W., van Oorschot P., Wiener M. Authentication And Authenticated Key Exchanges. Designs. — 1992. — 2. — P. 107–125.
- [9] BaekJ., KimK. Remarks. On The Unknown Key-Share Attacks. IEICE Trans. — 2000. — E83-A. — № 12. — P. 99-106.

*Поступила в редакцию - 22 июня 2017 г. Окончательный вариант – 04 ноября 2017 г.
Received – June 22, 2017. The final version – November 04, 2017.*