ЕСТР. Основные положения по управлению ключами, сертификатами и оборудованием при внедрении системы цифровых тахографов на территории Российской Федерации.

ВЕРСИЯ 2.2

МОСКВА 2014

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Версия	Дата представления	Внесенные изменения	Кем предложены изменения
1.0(1)	февраль 2010	Первоначальный вариант	Первоначальный вариант - разработан ОАО «НИИАТ» совместно с ОАО «РусТАХОНЕТ»
1.0(2)	февраль 2010	Первоначальный вариант с правками	ОАО «НИИАТ»
1.0(3)	март 2010	Первоначальный вариант с правками	ОАО «РусТАХОНЕТ» в процессе согласования с ЕРСА
1.0	апрель 2010	Подготовка окончательной версии	ОАО «РусТАХОНЕТ»
1.0	апрель 2010	Согласовано	Министерство транспорта Российской Федерации
1.0	апрель 2010	Одобрено	Европейская комиссия, Объединенный исследовательский центр
2.0	март 2012	Текст с изменениями	Министерство транспорта Российской Федерации, ФБУ «Росавтотранс», ОАО «НИИАТ»
2.0	март 2012	Согласовано	Министерство транспорта Российской Федерации
2.0	апрель 2012	Одобрено	Европейская комиссия, Объединенный исследовательский центр
2.1	ноябрь 2012	Согласовано	Министерство транспорта Российской Федерации
2.1	декабрь 2012	Одобрено	Европейская комиссия, Объединенный исследовательский центр
2.2	март 2014	Согласовано	Министерство транспорта Российской Федерации
2.2	апрель 2014	Одобрено	Европейская комиссия, Объединенный исследовательский центр

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Содержание

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

1. Введение

Данный документ определеят основные положения, касающиеся мероприятий по управлению ключами, сертификатами и оборудованием при внедрении системы цифровых тахографов на территории Российской Федерации.

Данный документ разработан с учетом положений следующих документов:

- Европейское соглашение, касающееся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР) подписанное 01 июля 1970 г.;
- Меморандум о взаимопонимании между службами Европеской комиссии и Европейской экономической комиссии ООН, январь 2009 г.;
- Правила Комиссии № 1360/2002 от 13 июня 2002 года и № 432/2004 от 5 марта 2004 года адаптирующие в седьмой раз в целях технического прогресса Правила Совета (ЕЭС) № 3821/85 о записывающем устройства, используемом на автомобильном транспорте
- Система цифровых тахографов. Основная политика Европейского союза. Версия 2.1. Публикация 53429 объединенного исследовательского центра Европейской комссии, 28 июля 2009 г., http://dtc.jrc.ec.europa.eu;
- Рекомендации и модель политики. Управление ключами, сертификатами и оборудованием (Регистрация, генерация ключей, выдача сертификатов, персонализация, распределение, использование и окончание срока действия) для системы Тахограф;
- «Общее руководство по безопасности», версия 2.0;
- Распоряжение Правительства РФ от 23 января 2008 г. № 46-р об определении Компетентного органа по выполнению обязательств, связанных с участием Российской Федерации в Европейском соглашении, касающемся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР);
- Постановление Правительства Российской Федерации от 12 сентября 2011г. № 769 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам транспорта»;
- Приказ Минтранса России от 02 июля 2009 г. № 106 «О реализации Европейского соглашения, касающегося работы экипажей транспортных средств, производящих международные автомобильные перевозки»;
- Приказ Минтранса России от 20 октября 2009 г. № 180, зарег. Минюстом России 02 февраля 2010 года , рег. № 16210 «О картах, используемых в цифровых контрольных устройствах контроля за режимами труда и отдыха водителей в соответствии с требованиями Европейского соглашения, касающегося работы экипажей транспортных средств, производящих международные автомобильные перевозки»;
- Распоряжение Министра транспорта Российской Федерации от 07 октября 2011 года № ИЛ-113-р.

Обозначания и сокращения, использованные в настоящем документе приведены в Разделе 15.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

1.1. Ответственные организации

Ответственными за оранизацию и проведение мероприятий по управлению ключами, сертификатами и оборудованием при внедрении системы цифровых тахографов на территории Российской Федерации являются:

● **NA** - Компетентный орган по выполнению обязательств, связанных с участием Российской Федерации в Европейском соглашении, касающемся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР) - Министерство транспорта Российской Федерации.

Адрес: Российская Федерация, 109012, Москва, ул. Рождественка, д. 1, стр. 1;
Тел./факс + 7 (495) 626-10-88;

● Орган по сертификации ключей **(CA)**

Перечень организаций расположен по адресу:
http://rosavtotransport.ru/ru/aetr/ca/;

● Органы по выдаче карт **(CIA)**:

Перечень организаций расположен по адресу:
http://rosavtotransport.ru/ru/aetr/cia/;

● Органы по персонализации **(CP)**:

Перечень организаций расположен по адресу:
http://rosavtotransport.ru/ru/aetr/cp/.

Для выполнения отдельных видов работ по выпуску карт, по сертификации ключей, по персонализации карт ФБУ «Росавтотранс» привлекает субподрядные организации в порядке, предусмотренном законодательством Российской Федерации.

● ERCA - главный сертификационный центр Евросоюза.

Субъекты, на которые распространяются требования настоящего документа выделены желтым цветом.

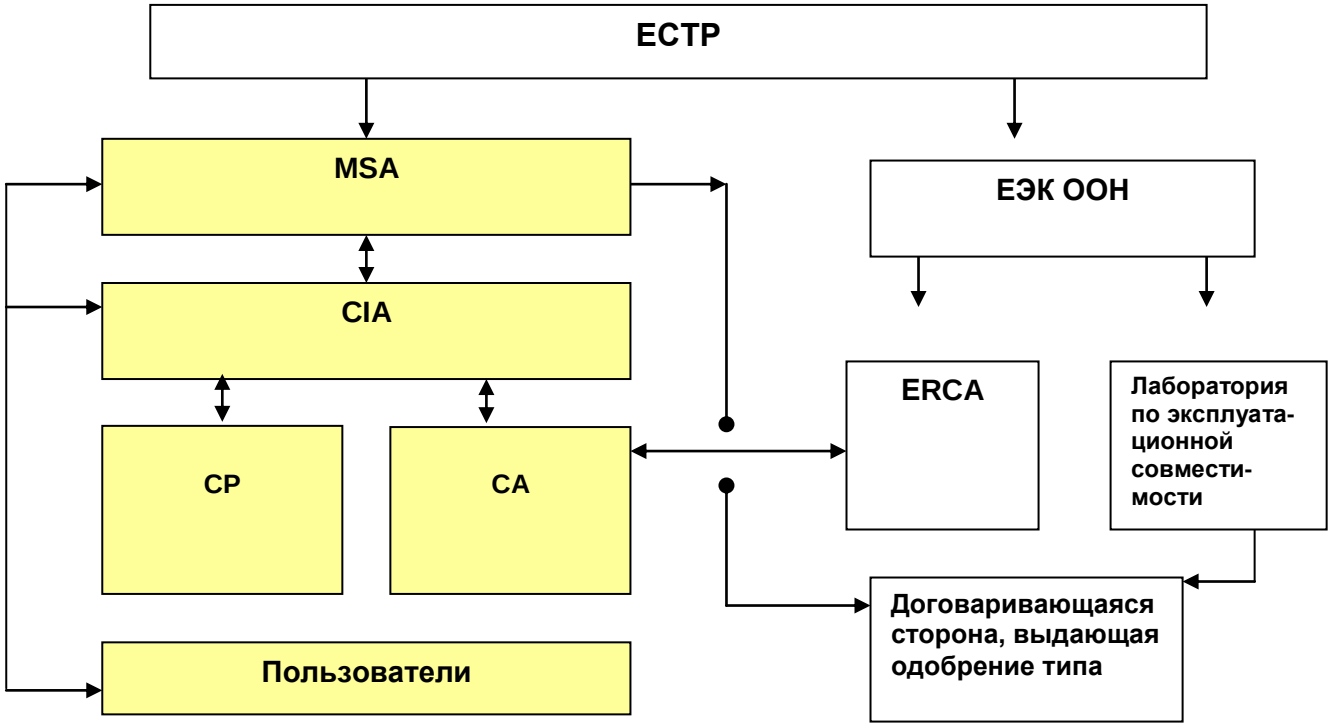

Рис. 1. Организационная структура системы цифровых тахографов

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

1.2. Одобрение

Настоящий документ одобрен главным сертифицирующим органом по цифровым тахографам Европейской комиссии май 2012.

Главный сертифицирующий орган по цифровым тахографам
Институт по защите и безопасности граждан
Европейская комиссия
Объединенный исследовательский центр, Испра (TP.360)
Виа Е. Ферми, 2749
I-21027 Испра (BA)

1.3. Доступность и контакты

Настоящий документ доступен на сайте: www.rosavtotransport.ru

Запросы, связанные с применением настоящего документа могут быть направлены в ФБУ «Росавтотранс» Минтранса России:

Контактное лицо: Сухарев Сергей Александрович
Адрес: Российская Федерация, 125480, Москва, Героев Панфиловцев, 24,
Тел.: +7(495) 496-85-92
E – mail: info@rosavtotransport.ru

Вопросы, связанные техническим аспектами настоящего документа должны быть направлены в ФБУ «Росавтотранс».

Контактное лицо: Краковский Максим Игоревич
Адрес: Российская Федерация, 125480, Москва, ул. Героев Панфиловцев, 24,
Тел.: +7 (495) 496-91-98,
E – mail: aetr@rosavtotransport.ru

2. Область применения

[r1] Данный документ действует только в части системы цифровых тахографов.

[r2] Ключи и сертификаты, выданные органом по сертификации ключей (MSCA) могут быть использованы только внутри системы цифровых тахографов.

[r3] Карты, выданные органом по выпуску карт (CIA) могут быть использованы только внутри системы цифровых тахографов.

Область применения настоящего документа отражена рис. 2.

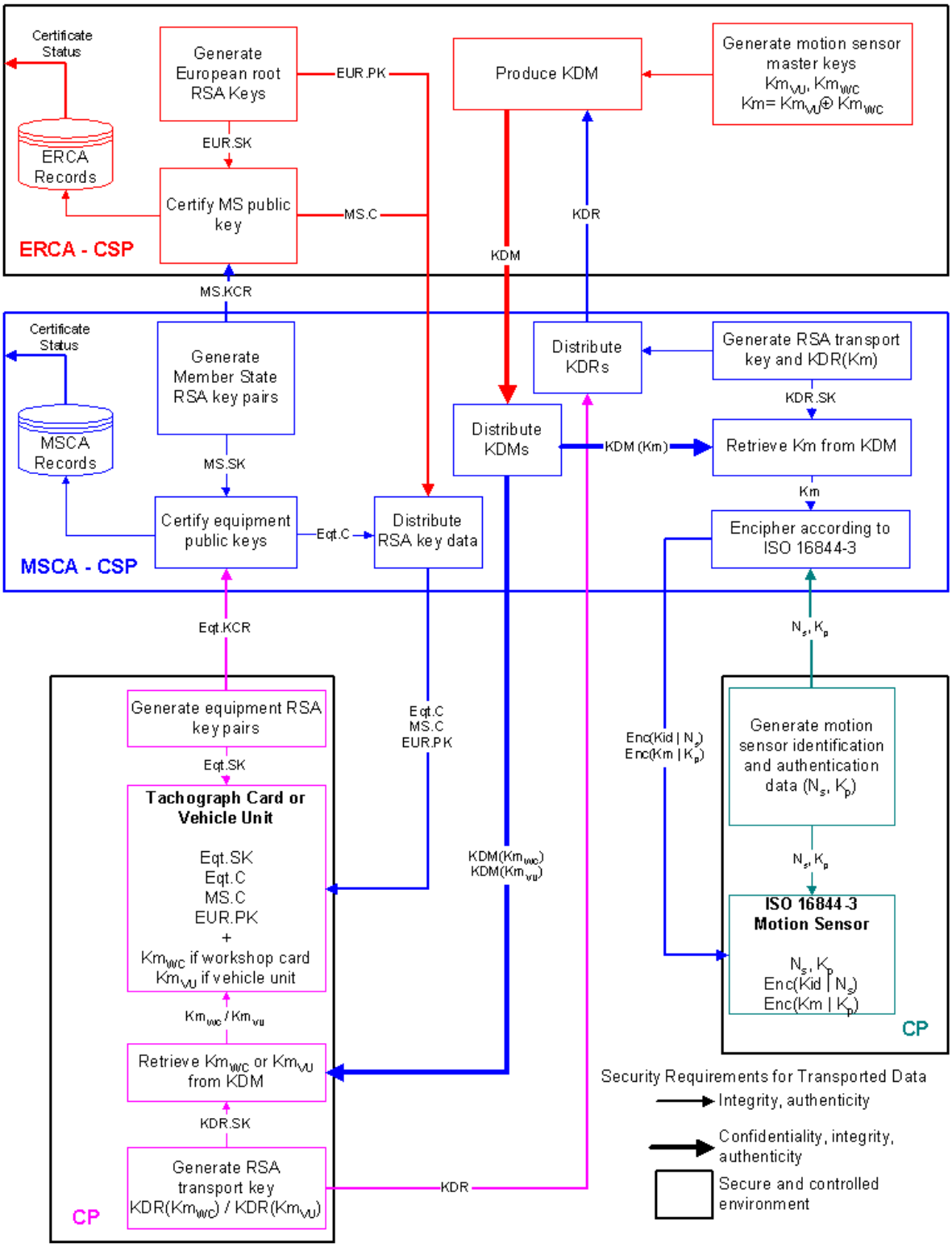

Рис. 2

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

3. Общие положения

Настоящий раздел содержит положения, касающиеся обязательств участников системы цифровых тахографов, указанных в разделе 2.

3.1.Обязательства

Этот раздел содержит обязательства:

- Компетентного органа по ЕСТР Российской Федерации – Министерства транспорта Российской Федерации (MSA);
- ФБУ «Росавтотранс»: органа по выпуску карт (CIA); органа по сертификации ключей (CA); органа по персонализации (CP);
- субподрядчиков;
- пользователей (держателей карт).

3.1.1. Обязательства Компетентного органа по ЕСТР Российской Федерации (NA) и органа по выпуску карт (CIA)

В соответствии с настоящим документом, на Компетентный орган по ЕСТР Российской Федерации и орган по выпуску карт возложены следующие обязательства:

[r4] Компетентный орган по ЕСТР Российской Федерации (NA):

а) обеспечивает реализацию положений настоящего документа путем нормативно-правового регулирования и контроля за деятельностью CIA, CA, CP;

б) уполномачивает в соответствии с законодательством РФ CIA, CA, CP;

в) проводит проверки деятельности CIA, CA, CP;

г) рассматривает и согласовывает документы о практике реализации CIA, CA, CP;

д) информирует заинтересованных лиц о положениях настоящего документа;

е) информирует пользователей и производителей карт о требованиях настоящего документа;

ж) направляет настоящий документ в EPCA на согласование при его принятии и в дальнейшем при внесении в него изменений.

[r5] Орган по выпуску карт (CIA) должен:

а) соблюдать требования настоящего документа;

б) издавать документы CIA о практической реализации своих функций, которые разработаны в соответствии с требованиями ЕСТР и настоящего документа, иными, приятыми в установленном порядке документами;

в) обеспечивать эффективное управление финансовыми и организационными ресурсами с целью осуществления своих функций в соответствии с требованиями ЕСТР и настоящего документа, включая вопросы менеджмента финансовых рисков;

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

г) обеспечивать передачу CA и CP полной и достоверной информации, необходимой для выпуска карт в соответствии с предоставленными заявлениями для дальнейшего занесения на поверхность и в память карт;

в) информировать заинтересованных лиц о положениях настоящего документа, в т.ч. пользователей и производителей карт.

3.1.2.Обязательства органа по сертификации ключей (CA)

[r6] Орган по сертификации CA должен:

а) соблюдать требования настоящего документа;

б) издавать документы о практической реализации своих функций, которые разработаны в соответствии с требованиями ЕСТР и настоящего документа, иными, приятыми в установленном порядке документами и одобренными NA;

в) обеспечивать эффективное управление финансовыми и организационными ресурсами с целью осуществления своих функций в соответствии с требованиями ЕСТР и настоящего документа, включая вопросы менеджмента финансовых рисков.

[r7] Орган по сертификации должен принимать все необходимые меры для обеспечения уверенности в том, что требования, изложенные в настоящем документе соблюдаются.

[r8] Орган по сертификации несет ответственность за соответствие реализуемых им процедур требованиям настоящего документе даже в случае если некоторые из своих полномочий он передает другим организациям. Орган по сертификации ответственен за обеспечение того, чтобы организации, которым он передал определенные полномочия осуществляли свою деятельность в соответствии с требованиями ЕСТР, настоящего документа, иными, приятыми в установленном порядке документами.

3.1.3.Обязательства органа по персонализации карт (CP)

[r9] Орган по персонализации карт должен:

а) соблюдать требования настоящего документа;

б) издавать документы о практической реализации своих функций, которые разработаны в соответствии с требованиями ЕСТР и настоящего документа, иными, приятыми в установленном порядке документами и одобренными NA.

в) обеспечивать эффективное управление финансовыми и организационными ресурсами с целью осуществления своих функций в соответствии с требованиями ЕСТР и настоящего документа, включая вопросы менеджмента финансовых рисков.

[r10] Орган по персонализации должен принимать все необходимые меры для обеспечения уверенности в том, что требования, изложенные в настоящем документе соблюдаются.

[r11] Орган по персонализации несет ответственность за соответствие реализуемых им процедур, требованиям настоящего документе, даже в случае если некоторые из своих полномочий он передает другим организациям.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

3.1.4.Обязательства субподрядных организаций

[r12] Субподрядные организации, которым орган по сертификации и орган по персонализации карт передают выполнение каких-либо возложенных на них Компетентным органом по ЕСТР Российской Федерации функций несут ответственность в соответствии с принятыми на себя договорными обязательствами.

3.1.5.Обязательства держателей карт

[r13] Орган по выпуску карт должен обеспечить посредством заключения соответствующих соглашений выполнение держателями карт следующих обязательств:

а) пользователь должен предоставлять органу по выпуску карт точную и полную информацию, необходимую для выпуска соответствующих карт;

б) пользователь должен использовать полученные ключи и сертификаты только в системе цифровых тахографов;

в) пользователь должен использовать карты только в системе цифровых тахографов;

г) пользователь должен предпринимать меры для предотвращения несанкционированного использования карт и закрытой части ключей оборудования;

д) пользователь должен использовать только собственные карты, ключи и сертификаты, переданные органом по выпуску карт (ЕСТР, Приложение, статья 11.4.a);

е) пользователь должен владеть только одной действующей картой водителя (ЕСТР, Приложение, статья 11.4.a);

ж) пользователь может одновременно: иметь карту мастерской и карту предприятия (ЕСТР, Приложение Добавление 1B, VI:1); иметь несколько карт мастерской;

з) пользователь не должен использовать поврежденную карту или карту с истекшим сроком действия;

и) пользователь должен до завершения срока действия карты или ключей, указанного в свидетельстве (сертификате), незамедлительно поставить в известность орган по выпуску карт в следующих случаях:

- когда карта была украдена, потеряна или существует потенциальная угроза для дальнейшего использования карты (ЕСТР, Приложение, статья 12.1);
- когда содержание сертификата (свидетельства) является неточным (ошибочным).

3.1.6. Обязательства производителей тахографов

В настоящее время в Российской Федерации не применяется.

3.1.7.Обязательства производителей датчиков движения

В настоящее время в Российской Федерации не применяется.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

3.2.Ответственность

Примечание: в настоящем документе не определяется форма и размер ответственности, являющиеся предметом регулирования соответствующих нормативных правовых актов РФ.

Орган по сертификации ключей (CA) и орган по персонализации карт (CP) не несут ответственности по отношению к конечным пользователям, а несут ответственность только по отношению к Компетному органу РФ по ЕСТР (NA) и органу по выпуску карт (CIA).

Любые вопросы, связанные с ответственностью перед конечным пользователем, находятся в сфере компетенции Компетного органа РФ по ЕСТР (NA) и органа по выпуску карт (CIA).

[r16] Карты, ключи и сертификаты предназначены только для использования внутри системы цифровых тахографов. Использование других сертификатов на картах в системе цифровых тахографов не допускается. В этой связи ни одна из организаций (Компетный орган РФ по ЕСТР, орган по выпуску карт, орган по сертификации ключей, орган по персонализации) не несут ответственности за подобные сертификаты.

3.2.1.Ответственность Компетентного органа РФ по ЕСТР и органа по выпуску карт перед пользователями и иными, связанными с ними сторонами

[r17] Компетентный орган РФ по ЕСТР и орган по выпуску карт несут ответственность только за те действия, которые были совершены с нарушением положений настоящего документа. В случае если Компетентный орган РФ по ЕСТР и орган по выпуску карт действовали в соответствии с настоящим документом или иными документами, утвержденными в установленном порядке, эти действия не могут быть квалифицированы как незаконные.

3.2.2.Ответственность органа по сертификации ключей и органа по персонализации карт перед Компетентным органом РФ по ЕСТР

[r18] Орган по сертификации ключей и орган по персонализации несут ответственность только за те действия, которые были совершены с нарушением или в разрез с положениями настоящего документа. В случае если вышеуказанные органы действовали в соответствии с положениями настоящего документа или иными документами, принятыми в установленном порядке, регламентирующими практические процедуры сертификации ключей и персонализации карт, эти действия не могут быть квалифицированы как незаконные.

3.3.Трактования и реализация

3.3.1. Регулирующее законодательство («верховенство закона», «основной закон»)

Практические процедуры сертификации ключей и выпуска карт должны отвечать требованиям ЕСТР и соответствующего законодательства Российской

Федерации. Если ЕСТР установлены требования отличающиеся от требований законодательства РФ, то применяются требования ЕСТР (п. 4 ст. 15 Конституции РФ).

3.4.Конфиденциальность

Конфиденциальность в части защиты персональных данных при использовании и обработке таких данных должна отвечать требованиям директивы Совета Европарламента N 95/46/ЕС от 24 октября 1995 года "О защите граждан в связи с обработкой персональных данных и о свободном передвижении таких данных" ("Директива о приватности") и Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» в части, не противоречащей директиве N 95/46/ЕС с учетом положений пункта 4 статьи 4 данного закона и пункта 4 статьи 15 Конституции Российской Федерации.

3.4.1. Виды информации, для которых должна соблюдаться конфиденциальность

[r19] Любые персональные данные или любая другая информации такого рода, в т.ч. информация о предприятии, используемая органом по сертификации ключей, органом по персонализации, а так же субподрядными организациями, и не используемая для нанесения на карту при ее выпуске в обращения является конфиденциальной и не может быть передана для открытого распространения без соответствующего разрешения субъекта персональных данных или его представителя, если иное не предусмотрено ЕСТР и законодательством Российской Федерации (см. 3.4.).

[r20] Вся персональная информация и закрытые части ключей используемые органом по сертификации и органом по персонализации должны быть строго конфиденциальны.

[r22] Информация и данные, используемые при реализации системы цифровых тахографов не должны быть доступны для всеобщего использования за исключением случаев установленных законодательством.

[r23] Информация и данные, используемые при реализации системы цифровых тахографов не должны быть доступны для всеобщего использования за исключением случаев установленных законодательством.

3.4.2.Информация, которая не рассматривается в качестве конфиденциальной

[r24] Сертификаты не считаются конфиденциальной информацией.

[r25] Идентификационные данные, а так же персональная информация и информация об организации, наносимая на карту, а также в сертификаты не являются конфиденциальными, если иное не предусмотрено ЕСТР, законодательством РФ (см. 3.4.), специальными соглашениями или статусом пользователя.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

4.Требование к документированию процедур, реализуемых органом по выпуску карт, сертификации ключей и органом по персонализации карт

[r26] Орган по выпуску карт, сертификации ключей и орган по персонализации должны иметь документы, отражающие изложение практических методов и процедур осуществления своей деятельности в соответствии с требованиями ЕСТР и настоящего документа. Данные документы («Руководства по практике») должны быть утверждены соответствующими органами и согласованы с Компетентным органом по ЕСТР.

В частности:

а) «Руководства по практике» должны определять обязательства всех внешних организаций, связанные с реализацией функций органа по сертификации ключей и органа по персонализации, включая примерные процедуры и методы контроля.

б) «Руководства по практике» должны быть доступными для Компетентного органа по ЕСТР РФ, а также для пользователей системы цифрового тахографа, иных заинтересованных сторон (например, для контролирующих органов).

При этом орган по сертификации ключей и орган по персонализации не обязаны разглашать пользователям всех деталей практической реализации своих обязательств.

в) «Руководства по практике» должны обеспечить выполнение возложенных на соответствующие органы обязательств и предусматривать ответственность за их несоблюдение.

г) Органы по выпуску, сертификации и по персонализации карт должны определить порядок пересмотра «Руководств по практике».

д) Органы по выпуску, сертификации и по персонализации карт должны уведомлять Компетентный орган РФ по ЕСТР обо всех изменениях, которые они планируют внести в «Руководства по практике», и после одобрения измененного документа сделать его доступным. Незначительные изменения в «Руководстве по практике» могут быть внесены в текст документа без одобрения Компетентный органа РФ по ЕСТР.

5. Управление оборудованием

Состав оборудования, используемого при внедрении системы цифровых тахографов включает в себя:

- карты контрольных устройств (тахографов);
- контрольные устройства (бортовые устройства – модули транспортных средств);
- датчики движения.

Оборудование управляется следующими пользователями:

- органом по выпуску карт (регистрация заявлений на выдачу, замену, обновление карт, распределение карт, регистрация заявлений на выдачу сертификатов ключей оборудования и т.д.);

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

- органом по сертификации (выпуск ключей и сертификатов);
- органом по персонализации (графическая и электронная персонализация, аннулирование (уничтожение) карт).

Компетентный орган РФ по ЕСТР выполняют следующую роль в управлении оборудованием:

- осуществляют официальное утверждение типа оборудования.

Орган по выпуску карт выполняет следующую роль:

- прием заявлений на выдачу (продление срока, замену и т.п.) карт, заявлений на выдачу сертификатов ключей оборудования;
- проведение процедуры регистрации заявлений;
- распределение карт;
- регистрация карт и хранение данных.

Орган по сертификации и орган по персонализации выполняют следующую роль:

- контроль качества (тестовые испытания);
- контроль за ключами;
- персонализация карт;
- распределение ключей и сертификатов.

5.1. Карты тахографов

5.1.1. Контроль качества – функции органа по сертификации и органа по персонализации карт

[r27] Орган по сертификации и орган по персонализации карт должны гарантировать персонализацию только тех видов карт, которые предусмотрены ЕСТР (см. 5.1.7.5).

5.1.2. Заявление на выдачу карты

[r28] Орган по выпуску карт должен сообщать пользователям информацию о сроках и условиях использования карт. Информация должна быть изложена в форме доступной для понимания.

[r29] Пользователь обязан, подавая заявление на получение карты и получая ее в последствие, принять установленные сроки и условия ее использования.

5.1.2.1.Заявление пользователя

Заявление на получение карты для тахографа должно быть подано в форме, утвержденной органом по выпуску карт и согласованной с Компетентным органом РФ по ЕСТР.

Эта форма должна содержать данные, которые позволяют правильно идентифицировать пользователя.

Далее приводится информация необходимая для выдачи карт водителя, мастерской, контролера, предприятия.

[r30] *Для карты водителя:*

- Ф.И.О.;

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

- дата рождения;
- фотография;
- место обычного проживания;
- почтовый адрес (если он отличается от места обычного проживания);
- номер паспорта, кем и когда выдан (для иностранных граждан – данные о заграничном паспорте, ином идентификационном документе);
- наименование страны, выдавшей водительское удостоверение;
- номер национального водительского удостоверения (на дату выдачи карты);
- предпочитаемый язык общения.

Примечание: Карта водителя может быть выдана заявителю, имеющему постоянное место жительство в стране, где он подает заявление на получение карты.

Под постоянным местом жительства понимается проживание водителя на территории государства в течение не менее 185 дней каждого календарного года в силу его личных или профессиональных обязательств, либо ввиду личных обстоятельств.

В случае смены водительского удостоверения в течение срока действия карты замена карты не производится.

[r31] *Для карты мастерской:*

- полное и сокращенное наименование юридического лица (индивидуального предпринимателя);
- адрес места расположения исполнительного органа (юридический адрес);
- почтовый адрес юридического лица (индивидуального предпринимателя);
- должность, Ф.И.О. руководителя юридического лица (индивидуального предпринимателя) или лица (лиц), назначенного(ных) приказом по предприятию ответственным(и) за получение, хранение и использование карт, их паспортные данные (номер, кем и когда выдан); дата рождения; номер и дата приказа о назначении ответственным за получение, хранение и использование карты.

Информация о ранее выданных картах:

- номер;
- срок действия.

Примечание: Карты мастерской выдаются юридическим лицам или индивидуальным предпринимателям, зарегистрированным на территории Российской Федерации и допущенным в установленном порядке к выполнению работ по установке, проверке, техническому обслуживанию и ремонту контрольных устройств.

[r32] *Для карты контролера:*

- наименование контрольного (надзорного) органа, его территориального управления;
- адрес месторасположения территориального управления;
- по каждому лицу, получающему карты: должность, Ф.И.О.; дата рождения; фотография; паспортные данные, в соответствии с национальным документом, идентифицирующем личность (номер, кем и когда выдан).

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Карты контролера выдаются по представлению соответствующего надзорного органа лицам:

- являющимся сотрудниками контрольных (надзорных) органов Российской Федерации, уполномоченных законодательством Российской Федерации для осуществления контроля за режимами труда и отдыха водителей при осуществлении международных автомобильных перевозок;

- не имеющим на момент подачи заявления в случае первичной выдачи карты иной действующей карты (независимо от ее типа), выданной Компетентным органом по ЕСТР Российской Федерации, иной договаривающейся стороны ЕСТР.

[r33] *Для карты предприятия:*

- полное и сокращенное наименование юридического лица (индивидуального предпринимателя);
- адрес места расположения исполнительного органа (юридический адрес);
- почтовый адрес предприятия;
- должность, Ф.И.О. руководителя предприятия или лица (лиц), назначенного(ных) приказом по предприятию ответственным(и) за получение, хранение и использование карт, их паспортные данные (номер, кем и когда выдан); номер и дата приказа о назначении ответственным за получение, хранение и использование карты.

Информация о ранее выданных картах:

- номер;
- срок действия.

Карты предприятия выдаются юридическим лицам и индивидуальным предпринимателям, зарегистрированным на территории Российской Федерации, осуществляющим (планирующим осуществлять) международные перевозки грузов и пассажиров автомобильным транспортом, попадающие в сферу действия ЕСТР.

5.1.2.2.Соглашение

[r34] Заявитель, подавая заявление на получение карты и получая карту тем самым подтверждает свое согласие с условиями Компетентного орган по ЕСТР РФ в следующем:

- соглашается со всеми сроками и условиями в части использования карт тахогафа, включая согласие на использование своих персональных данных в целях осуществления контроля за режимами труда и отдыха водителей;
- соглашается и подтверждает, что за все время использования карты (в процессе эксплуатации) начиная с момента ее получения, до тех пор пока действие карты не будет приостановлено в установленном порядке:

карта не будет передана третьему лицу, не уполномоченному в ее использовании с целью ее применения в системе;

вся информация, предоставленная органу по выпуску карт является достоверной и соответствует той информации, которая занесена на карту;

карта будет использована только с учетом имеющихся «физических» ограничений.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

5.1.2.3.Условия принятия органом по выпуску карт решения о возможности выдачи карты – для карты водителя.

[r35] Карта водителя может быть выдана заявителю, имеющему обычное место проживания (не менее 185 дней) в стране, где он подает заявление на получение карты.

[r36] Орган по выпуску карт должен быть уверен, что заявитель не является пользователем карты, выданной в другой стране.

[r37] Орган по выпуску карт должен быть уверен, что заявитель имеет водительские права соответствующей категории.

5.1.3. Возобновление (продление) срока действия) карты – осуществляется органом по выпуску карт

[r38] Карта сервисного центра (мастерской) выдается на срок не более одного года с даты выдачи карты.

[r39] Карта водителя выдается на срок не более трех лет с даты выдачи карты.

[r40] Карта предприятия выдается на срок не более пяти лет с даты выдачи карты.

[r41] Карта контролера выдается на срок не более двух лет с даты выдачи карты.

*Примечание: приведенные в **[r38], [r39], [r40], [r41]** сроки действия карт соответствует установленным Приказом Минтранса России от 20 октября 2009 № 180, зарег. Минюстом России 02 февраля 2010 г., рег. № 16210.*

[r42] Порядок напоминания пользователям о сроке окончания действия карточки определен орган по выдаче карт в руководстве по практике «ЕСТР. Руководство по выдаче, замене, приостановлению и аннулированию действия карт, используемых в устройствах контроля режимов труда и отдыха водителей при реализации требований Европейского соглашения, касающегося работы экипажей транспортных средств, производящих международные автомобильные перевозки».

[r43] Заявление на продление срока действия карты определено в руководства по практике «ЕСТР. Руководство по выдаче, замене, приостановлению и аннулированию действия карт, используемых в устройствах контроля режимов труда и отдыха водителей при реализации требований Европейского соглашения, касающегося работы экипажей транспортных средств, производящих международные автомобильные перевозки».

5.1.3.1.Карта водителя

[r44] При необходимости обновления карты в связи с окончанием срока ее действия, держатель карты должен направить заявление о выдаче карты на новый срок не позднее чем за 15 (пятнадцать) дней до даты истечения срока действия карты.

Порядок обновления карты соответствует порядку выдачи.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

[r45] Если пользователь действует в соответствии с установленными требованиями, орган по выпуску карт должен выдать новую карту до окончания срока действия текущей карты.

5.1.3.2.Карта мастерской

[r46] Пользователь должен подать заявление о продление карты как минимум за 15 дней до окончания срок действия карты.

[r47] Орган по выпуску карт должен продлить срок действия карты мастерской в течение 5 рабочих дней с даты регистрации заявления, оформленного в установленном порядке с предоставлением всех необходимых документов и данных.

5.1.3.3.Карта предприятия

[r48] Пользователь должен подать заявление о продление карты как минимум за 15 дней до окончания действия карты.

[r49] Если пользователь действует в соответствии с вышеуказанными требованиями, орган по выпуску карт должен выдать новую карту предприятию до окончания срока действия текущей карты.

5.1.3.4.Карта контролера

[r50] Пользователь должен подать заявление о продление карты как минимум за 15 дней до окончания срока ее действия.

[r51] Орган по выпуску карт должен продлить срок действия карты контролера в течении 5 рабочих дней с даты регистрации заявления, оформленного в установленном порядке с предоставлением всех необходимых документов и данных.

5.1.4. Выдача карт на новый срок (обновление) или обмен карт – осуществляется органом по выпуску карт

[r52] Пользователь, меняющий страну постоянного места жительства, может обратиться в орган по выпуску карт с заявлением об обмене карты водителя. В том случае если на момент подачи заявления об обмене, текущая карта является действительной (срок действия карты не истек), заявитель в качестве подтверждения предъявляет только адрес нового места жительства.

[r53] Орган по выпуску карт взамен старой карты выдает новую, а изъятую карту отправляет в соответствующий компетентный орган договаривающейся стороны ЕСТР.

[r54] Обмен карты в следствие изменения места жительства (страны проживания) производиться в соответствии с процедурой выдачи новой карты.

5.1.5. Замена утерянных, украденных, поврежденных карт и карт, работающих со сбоями – осуществляется органом по выпуску карт

[r55] В случае если карта потеряна или украдена, пользователь должен незамедлительно сообщить о данном факте в орган по выпуску карт любым

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

доступным способом (телефон, электронная почта и т.п.) и указать при этом свои паспортные данные.

[r56] Информация об украденных или потерянных картах должна быть размещена в «черном списке» и быть доступной для всех стран – договаривающихся сторон ЕСТР.

[r57] Поврежденная и неисправная карта должна быть направлена в орган по выпуску карт для уничтожения и занесения в «черный список».

[r58] Если карта утеряна, украдена, повреждена или неисправна, пользователь должен подать заявление о замене карты в течении 7 (семи) календарных дней с момента наступления причин замены.

[r59] Если пользователь придерживается вышеупомянутого требования, орган по выпуску карт должен выдать новую карту с ключами и сертификатами взамен старой в течение 5 рабочих дней с момента подачи пользователем заявления оформленного в установленном порядке с предоставлением всех необходимых документов и данных.

[r60] Срок действия карты, выдаваемой взамен старой исчисляется с момента выдачи старой карты. Если до истечения срока действия выдаваемой взамен старой карты осталось меньше 6 месяцев, орган по выпуску карт может выдать новую карту.

5.1.6.Регистрация заявления о выдаче карты - осуществляется органом по выпуску карт

[r61] Орган по выпуску карт должен регистрировать все представленные на выдачу карт заявления. Эти данные должны быть доступны для органа по сертификации и органа по персонализации с целью дальнейшего использования этой информации для генерации сертификатов и персонализации карт.

5.1.7. Персонализация карт – осуществляется органом по персонализации карт

Персонализация карт осуществляется графическим и электронным способом. Данный процесс осуществляется с привлечением субподрядной организации, указанной в п.1.1. настоящего документа, что не уменьшает ответственности NA.

5.1.7.1.Графическая персонализация

[r62] Карты подвергаются графической персонализации в соответствии с Приложением - Добавление 1B к ЕСТР, раздел IV и Приказом Минтранса России от 20 октября 2009 г. № 180, зарег. Минюстом России 02 февраля 2010 года , рег. № 16210.

5.1.7.2.Ввод данных пользователя

[r63] Данные заносятся на карту в соответствии с требованиями Приложения - Добавление 1B к ЕСТР: подраздел 2, правила: TCS_403, TCS_408, TCS_413 и TCS_418, в зависимости от типа карты.

5.1.7.3.Ввод ключа

[r64] Закрытая часть ключей должна вводиться в карту таким образом,

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

чтобы не возникла возможность изменения ключей внутри карты. Целесообразно осуществлять данный процесс таким образом, чтобы ключ не покидал среду его генерации. Содержание карты должно гарантировать, что не один человек ни при каких обстоятельствах не сможет получить контроль над закрытой частью ключа без прохождения процедуры идентификации, раздел 7.2.Ключи оборудования.

5.1.7.4. Ввод сертификата

[r65] Сертификат пользователя должен быть введен в карту до момента ее передачи пользователю.

5.1.7.5.Контроль качества

[r66] Орган по персонализации должен располагать документированными процедурами, обеспечивающими контроль заносимой на карту графической и электронной информации с целью проверки их соответствия фактическим данным пользователя.

5.1.7.6.Аннулирование (уничтожение) не выданных карт

[r67] Все поврежденные карты (или карты по каким – либо причинам не выданные конечному пользователю) должны быть физически и электронно уничтожены (утилизированы) в течение не более 3-х дней с момента наступления соответствующего события.

[r68] Все поврежденные карты должны быть зарегестрированны в базе данных для аннулированных карт.

5.1.8. Регистрация карт и хранение информации (баз данных) – осуществляется органом по выпуску карт

[r69] Орган по выпуску карт отслеживает каждую карту и номер каждой карты, выданные пользователям и заносит их в соответствующий реестр.

Орган по выпуску карт хранит перечень изготовленных карт - серийные номера, сертификаты.

5.1.9. Персонализация и выдача карт пользователю.

Примечание:

Выдача карт пользователю – осуществляется органом по выпуску карт. Персонализация – осуществляется органом по персонализации.

[r70]

- Утвержденные процедуры по персонализации должны быть документально прописаны с целью:

обеспечения минимизации времени на хранение персонализированных карт;

предотвращения возможных повреждений, потерь и ошибок;

безопасного хранения до передачи пользователю, включая хранение в нерабочее (ночное) время.

- Персонализированная карта должна быть немедленно направлена туда, где она будет передана или выдана пользователю.

- Персонализированные карты должны всегда храниться отдельно от не персонифицированных карт.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

- Карты для тахографов должны распространяться таким образом, чтобы минимизировать риск пропажи или утраты карт.
- При выдаче карт конечному пользователю необходимо установить его личность в соответствие с идентификационными документами.
- Пользователь (получатель) должен предоставить действующий документ, удостоверяющий его личность.
- Момент передачи карты должен быть удостоверен подписью пользователя (получателя).

5.1.10.Аутентификация кодов (PIN) – осуществляется органом по персонализации карт

Положения настоящего пункта распространяются только на карты сервисных центров (мастерских).

[r71] Карты мастерских должны иметь PIN–код, используемый для аутентификации карты и технического оборудования (Приложение – добавление 1В к ЕСТР, подраздел 10: карты тахографа: 4.2.2).

[r72] PIN –код должен содержать как минимум 4 цифры (Приложение – добавление 1В к ЕСТР, подраздел 10: контрольное устройство: 4.1.2).

5.1.10.1.Генерация PIN содов

[r73] PIN – код должен генерироваться в защищенной среде, вводиться в карту мастерской при соблюдениии установленных требований безопасности. Напечатанный на бумажном носителе PIN – код должен быть помещен в конверт. PIN – код может храниться в компьютере при условии соблюдения необходимых мер по предотвращению возможного управления данным PIN–кодом несанкционированного пользователя. Система генерации PIN–кодов должна отвечать требованиям ITSEC (Information Technology Security Evaluation Criteria – критерии информационной технологической безопасности) уровень E3, CC EAL4 (общие критерии безопасности уровень 4) или аналогичным критериям безопасности (Приложение – добавление 1В к ЕСТР, подразделы 10, 11).

5.1.10.2.Распределеение PIN - кодов

[r74] PIN –код может передаваться по обычной почте.

[r75] PIN – код не должны распространяться совместно с соответствующими картами.

5.1.11. Деактивация и уничтожение карт – осуществляется органом по выпуску карт и органом по персонализации карт

[r76] Необходимо обеспечить возможность деактивации и карт и ключей, распространяемых к ней. Решение о деактивации и уничтожении карт должно приниматься органом по выпуску карт, процедура деактивации должна проводиться органом по персонализации.

[r77] Деактивация карт должна проводиться с использованием соответствующего оборудования. После этого необходимо убедиться, что ключи и карта

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

функционально деактивированы. Кроме того, карта должна быть уничтожена физически.

Карты уничтожаются в шредере, сертифицированном для уничтожения банковских и идентификационных карт.

[r78] Деактивированные карты должны быть зарегистрированы в базе данных и их номера занесены в «черный список».

5.2. Контрольное устройство (тахограф) и датчик движения

В настоящее время в Российской Федерации не применяется.

6. Управление общими (корневыми) и транспортными ключами: общеевропейские ключи, ключи договаривающихся сторон (национальные ключи), ключи датчиков движения, транспортные ключи (ключи для переноса).

Этот раздел описывает процедуры управления:

- общеевропейскими ключами – открытая часть ключа Главного Европейского сертификационного центра (ERCA);
- национальными ключами Российской Федерации, а именно подписанной пары ключей Российской Федерации;
- ключами датчиков движения;
- транспортными ключами (ключами для переноса).

Открытая часть ключей ERCA (открытый (публичный) ключ) используется для подписания (подтверждения, сертификации) национальных ключей договаривающихся сторон ЕСТР, в т. ч. Российской Федерации. Закрытая часть ключей никогда не покидает ERCA.

Национальные ключи Российской Федерации – это подписанные ключи Российской Федерации, которые могут быть названы корневыми ключами.

Ключи датчиков движения – это симметричные ключи, помещаемые (вводимые) в карты мастерских, техническое оборудование и датчики движения для взаимного распознования. Сертификационный орган Российской Федерации получает ключи датчиков движения от Европейского сертификационного органа, хранит и распространяет их среди производителей.

Транспортные ключи (ключи для переноса) – это симметричные ключи, используемые для надежной передачи ключей даьчиокв движения между Европейским сертификационным центром (ERCA) и СА.

В случае если сертификационный орган РФ нуждается в других ключах, а не в тех которые перечислены выше, это не может быть рассмотрено как часть системы тахографов и не имеет ничего общего с настоящим документом.

Орган по сертификации ключей должен гарантировать конфиденциальность и целостность открытой и закрытой части всех ключей сгенерированных, используемых и хранимых в своей системе, а так же исключить случаи

незаконного использования этих ключей.

6.1.Открытые (публичные) ключи ERCA

[r98] Орган по сертификации ключей должен хранить открытую часть ключей ERCA (EUR.PK) таким образом, чтобы обеспечить их целостность и доступность в любой момент времени.

[r99] Орган по персонализации должен гарантировать, что открытая (публичная) часть ключа ERCA (EUR.PK) вводиться во все карты.

6.2.Ключи договаривающихся сторон

Ключи РФ – это подписанная пара ключей, сгенерированных органом по сертификации РФ, используемая для сертификации ключей оборудования.

Набор (пара) ключей состоит из открытой части (MS.PK) и закрытой (MS.SK) части ключей.

Открытая часть ключей сертифицируется ERCA, но всегда генерируется органом по сертификации самостоятельно.

[r100] Закрытая часть ключей Российской Федерации может быть использована только для подписания сертификатов карт тахографа и для формирования запроса в ERCA на подписание сертификатом ключа (KCR).

6.2.1. Генерация национальных ключей РФ

[r101] Генерация набора ключей РФ в соответствии с требованиями ЕСТР должна быть осуществлена с использованием оборудования, которое представляет собой надежную систему, соответствующую требованиям безопасности установленным в FIPS 140-2 уровень 3 или выше.

[r102] Устройство для генерации ключей должно быть автономным.

[r103] Фактически используемое устройство и требования, которым отвечает это устройство прописаны в руководстве по практике органа по сертификации.

[r104] Генерация набора ключей органом по сертификации ключей РФ требует наличия как минимум трех разных представителей. Как минимум один из них выполняет роль администратора органа по сертификации или администратора органам по персонализации), другие представители выполняют роль доверенных лиц (см. раздел 9.3 настоящего документа).

[r105] Генерация ключей должна осуществляться с использованием алгоритма RSA с длиной модуля ключа n=1024 бит (Приложение – Добавление 1В к ЕСТР, подраздел 11, подпункты 2.1, 3.2).

[r106] Орган по сертификации ключей должен владеть как минимум двумя (2) парами ключей с действующими совместно подписанными сертификатами с целью гарантии непрерывности процесса и как максимум пятью (5) парами ключей РФ с действующими совместно подписанными сертификатами с целью гаран-

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

тии непрерывности процесса, поскольку Европейский сертификационный центр не может обеспечить быструю замену сертификатов.

6.2.2. Срок действия ключей договаривающихся сторон

[r107] Срок действия закрытой части пары ключей РФ составляет не более 2 лет с момента сертификации соответствующей открытой части ключей. Ключи не могут быть использован после окончания срока их действия ни по какой причине.

[r108] Открытая часть ключей не имеет срока действия.

6.2.3. Хранение ключей договаривающейся стороной

[r109] Закрытая часть ключей должна содержаться и управляться специальным устройством, в работу которого не может быть осуществлено ни какого вмешательства, отвечающим требованиям безопасности установленным в FIPS 140-2 уровень 3.

[r110] Для доступа к ключам органа по сертификации ключей, требуется двойной контроль. Это означает, что никто в одиночку не может использовать средства (методы, механизмы), необходимые для получения доступа к оболочке (месту, файлу и т.д.) где храниться закрытая часть ключей. Однако, это не означает, что сертификаты ключей оборудование должны выдаваться с использованием принципов двойного контроля.

6.2.4. Дубликат закрытой части ключей РФ

[r111] Подписанная часть закрытых ключей РФ может быть продублирована процедурой восстановления ключей, требующей по крайней мере двойного контроля. Используемая процедура должна быть прописана в руководстве по практике. Однако, если набор ключей используется в соответствии с **[r106]**, необходимость изготовления дубликата отсутствует.

6.2.5. «Условное депонирование» закрытой части ключей РФ

[r112] Закрытая часть подписанных ключей РФ не может быть депонирована – передана на хранение третьему лицу.

6.2.6. Угроза (опасность) для закрытой части ключей

[r113] Во избежание возможности получения огласки закрытой части ключей, а так же во избежание возможной угрозы, необходимо разработать подробную инструкцию, прописанную в руководстве по практике органа по сертификации ключей. В этом документе необходимо разработать меры, которые необходимо предпринять пользователю или персоналу, ответственному за безопасность в случае возникновения возможных угроз.

[r114] В случае угрозы (опасности) для закрытой части ключей, орган по сертификации ключей как минимум должен проинформировать Компетный орган РФ по ЕСТР, Европейский сертификационный орган и национальные органы по сертификации ключей других договаривающихся сторон ЕСТР.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

6.2.7. Окончание срока действия ключей договаривающейся стороны

[r115] Орган по сертификации ключей должен разработать специальный порядок, обеспечивающий наличие действующих, сертифицированных подписанных пар ключей.

[r116] После того, как срок действия подписанных национальных ключей РФ закончился, открытая часть ключей должна быть архивирована, а закрытая часть ключей должна быть:

- уничтожена таким образом, чтобы она не могла быть восстановлена; или
- сохранена таким образом, чтобы она была надежно защищена от возможности дальнейшего использования.

6.3. Ключи датчиков движения

[r117] Орган по сертификации ключей должен сделать запрос в Европейский сертификационный центр на получение ключей датчиков движения Km_{wc} (Приложение Добавление 1B, подраздел 11:3.1.3). Орган по сертификации ключей не обращается за получением основного (главного) ключа датчика движения Km или ключа датчика движения для оборудования KmVU.

[r120] Орган по сертификации должен направить ключ мастерской Km_{WC} в орган по персонализации для введение в карты мастерской.

[r121] Орган по персонализации должен взять на себя функцию по обеспечению того, чтобы ключи датчиков движения для мастерских Km_{WC} были введены во все карты мастерских (Приложение Добавление 1B, подраздел 11:3.1.3).

[r122] **О**рган по сертификации и орган по персонализации должны, в процессе хранения, использования и распределения, обеспечить защиту ключей датчиков движения для мастерской Km_{wc} с высокой гарантией физической и логической безопасности. Km_{wc} должен содержаться и управляться специальным устройством, в работу которого не может быть осуществлено ни какого вмешательства, отвечающего требованиям FIPS 140-2 уровень 3 или выше.

6.4. Транспортные ключи (ключи для переноса)

[r123] Для безопасной передачи $Km_{wc,}$ орган по сертификации ключей РФ и/или орган по персонализации должен сгенерировать ассиметрическую (RSA) пару ключей. Орган по сертификации ключей РФ или орган по персонализации должен в процессе хранения, использования и распределения обеспечить защиту ключей с высокой гарантией физической и логической безопасности. Ключи должны содержаться и управляться в надежной системе, соответствующей требованиям установленным в FIPS 140-2 уровень 3 или выше.

6.5. Запрос на сертификацию ключа и запрос на получение ключа датчика движения

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

Все транспортные ключи применяемые органом по сертификации отвечают треблования в части технических средств, среды и протоколов, установленных политикой ERCA. Компетентный орган должен назначить ответственное лицо с целью обеспечения функционирования среды (механизмов), при помощи которой происходит общение органа по сертификации CA и ERCA.

[r123.1] Орган по сертификации ключей РФ предоставляет открытую часть ключей (CA.PK) на сертификацию в ERCA, используя протокол запроса на сертификацию ключа (KCR) описанный в Приложении A «Система цифровых тахографов. Основная политика Европейского союза.»

[r123.2] CA должен признать открытый ключ (EUR.PK) в формате распределения, описанном в Приложение B к документу «Система цифровых тахографов. Основная политика Европейского союза».

[r123.3] CA делает запрос на KmWC в ERCA, используя протокол запроса ключа (KDR), описанный в Приложении D к документу «Система цифровых тахографов. Основная политика Европейского союза».

[r123.4] CA использует физическую среду для переноса ключа и сертификата, описанные в Приложении C к документу «Система цифровых тахографов. Основная политика Европейского союза».

[r123.5] CA должен гарантировать, что идентификатор ключа и модели ключей, передаваемые в ERCA на сертификацию и получение ключа датчика движения являются уникальными внутри системы.

7. Ключи оборудования (ассиметричные)

Ключи оборудования – это ассиметричные ключи, генерированные в процессе выпуска/производства оборудования (карты; цировые контрольные устройства) и сертифицированные органом по сертификации ключей договаривающейся стороны в системе цировых тахографов.

Управление ключами датчиков движения приводится в разделе 6.3.

7.1.Основные аспекты деятельности органа по персонализации и органа по сертификации ключей договаривающейся стороны, включая производителей оборудования

[r124] Инициализация оборудования (карты и техническое оборудование), загрузка ключей и персонализация должны осуществляться в управляемой и безопасной зоне. Доступ в данную зону должен быть строго ограничен, управление безопасностью зоны должно осуществляться за ее пределами, доступ в зону требует как минимум 2 лица с целью обеспечения безопасности. В процессе регистрации должна быть сохранена возможность доступа в зону и управления безопасностью в системе.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

[r125] Информация в системе, связанная с генерацией ключей не может быть оставлена в ней в том виде, в котором эта информация может нанести вред реализации положений настоящего документа.

[r126] Применительно к картам тахографа: информация в системе, связанная с персонализацией карт, не может быть оставлена в ней в том виде, в котором эта информация может нанести вред реализации положений настоящего документа.

[r127] В настоящее время не используется в Российской Федерации.

[r128] Организации (исполнители по субконтрактам), осуществляющие генерацию ключей и персонализацию карт от лица более чем одного государства – участника ЕСТР должны реализовывать свои полномочия отдельно друг от друга. При этом, должна вестись регистрация каждого отдельного процесса и соответствующий орган должен иметь доступ к данным процессам при необходимости.

[r129] В настоящее время не используется в Российской Федерации.

[r130] Орган по сертификации ключей и орган по персонализации должны обеспечить ведение регистрации процессов персонализации карт и сертификации ключей, таким образом, что бы был обеспечен единый взаимоувязанный учет заказов, списка соответствующих номеров оборудования и сертификатов. Компетентный орган РФ по ЕСТР должен иметь доступ к этим процессам при необходимости.

7.2.Ключи оборудования

7.2.1. Генерация ключей оборудования

[r131] Ключи могут быть генерированы либо органом по персонализации, либо органом по сертификации ключей. (Приложение – Добавление 1В к ЕСТР, Раздел 11: 3.1.1).

[r132] Организация, выполняющая генерацию ключей должна быть уверена, что ключи к оборудованию генерированы надлежащим способом и что закрытая часть ключей к оборудованию надежно защищена (храниться в надежном месте).

[r133] Генерация ключей должна осуществляться при помощи оборудования, которое отвечает требованиям, безопасности установленным в FIPS 140-2 уровень 3: генерацию ключей осуществляет HSM ProtectServer Gold, имеющий сертификаты FIPS 140-2 уровень 3.

[r134] Ключи должны быть генерированы с использованием алгоритма RSA с длиной модуля ключа n=1024 биты (Приложение – Добавление 1В к ЕСТР, Раздел 11: 2.1,3.2).

[r135] Процедуры генерации и хранения закрытой части ключей не должны допускать того, чтобы эти процедуры выходили за пределы системы, создавшей их. Более того, вся информация должна быть удалена из системы немедленно после введения ключей в устройство.

[r136] Ответственностью организации по генерации ключей является реализация соответствующих мероприятий, направленных на создание

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

уникальной части открытых ключей до того момента пока не будет выдано сертификата. (По своей природе система генерации ключей является случайной, и поэтому вероятность генерации не уникальных ключей незначительна).

7.2.1.1.Генерация пакетных ключей

[r137] Генерация ключей может быть осуществлена «пакетным способом» заранее, до момента подачи запроса на получение сертификата, или непосредственно при подача запроса на выдачу ключей.

[r138] Пакетная обработка данных должна быть выполнена с использованием автономного оборудования, отвечающего вышеизложенным требованиям безопасности. Целостность ключей должна быть защищена до тех пор, пока действует сертификат.

7.2.2.Легитимность ключей оборудования

7.2.2.1.Ключи на картах

[r139] Срок использования закрытой части ключей карт совместно с сертификатами, выданными в соответствии с настоящим документом не должен превышать срока действия сертификатов.

7.2.3. Регистрационное оборудование (тахографы)

[r140] В настоящее время не используется в Российской Федерации.

7.2.4.Хранение и защита закрытой части ключей оборудования - карты

[r141] Орган по персонализации должен гарантировать, что закрытая часть ключей карты, выданной пользователю защищена в соответствии с процедурами, указанными в настоящем документе.

[r142] Дубликаты (копии) закрытой части ключей не могут храниться нигде кроме карты тахографа, до тех пор, пока не потребуется проведения генерации ключей и персонализации устройства.

[r143] Ни при каких обстоятельствах закрытая часть ключей карты не может быть выведена из карты или храниться вне ее.

7.2.5. Хранение и защита закрытой части ключей оборудования – регистрирующее оборудование

В настоящее время не используется в Российской Федерации.

7.2.6.Условное депонирование и архивация закрытой части ключей оборудования

[r147] Закрытая часть ключей оборудования не может быть ни «условно депонирована», ни архивирована.

7.2.7.Архивация закрытой части ключей оборудования

[r148] Все сертификаты открытой части ключей должны быть архивированы органом по сертификации ключей.

7.2.8.Окончание срок действия ключей оборудования

[r149] По окончании срока действия карт, открытая часть ключей должна быть заархивирована, а закрытая часть ключей должна быть:

- уничтожена таким образом, чтобы закрытая часть ключей не могла быть восстановлена.

8.Управление сертификатами ключей оборудования

Этот раздел затрагивает вопросы жизненного цикла процедуры сертификации ключей, состоящей из регистрационных действий, выдачи сертификата, распределения, использования, восстановления, продления срока действия и окончания срока действия ключей.

8.1.Ввод данных

8.1.1.Карты тахографов

Держатели карт не подают заявление на получение сертификатов ключей, эти сертификаты выдаются на основании информации указанной в заявление на получение карты тахографа (см. пункт 5.1.2.), а так же информации о заявители, хранящейся в базе данных органа по выпуску карт.

[r151] Орган по сертификации ключей подтверждает уникальность идентификатора ключа KID и модулей ключей карт внутри своего домена.

8.1.2. Регистрирующее оборудование

В настоящее время не используется в Российской Федерации.

8.2.Сертификаты для карт

8.2.1.Сертификаты для карт водителей

[r154] Сертификаты для карт водителей выдаются только заявителям, прошедшим одобрение на получение карты водителя.

8.2.2.Сертификаты для карт мастерских

[r155] Сертификаты для карт мастерских выдаются только заявителям, прошедшим одобрение на получение карты мастерской.

8.2.3.Сертификаты для карт контролеров

[r156] Сертификаты для карт контролеров выдаются только заявителям, прошедшим одобрение на получение карты контролера.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

8.2.4.Сертификаты для карт предприятий

[r157] Сертификаты для карт предприятий выдаются только предпритяим, успешно прошедшим одобрение на получение карты предприятия.

8.3.Сертификаты для регистрирующего оборудования (модулей транспортных средств)

В настоящее время не используется в Российской Федерации.

8.4.Срок действия сертификатов ключей карт

[r160] Срок действия сертификатов ключей карт не может превышать срока действия карт (см. раздел. 5):

- срок действия сертификатов ключей карт водителей не может быть больше 3 лет;
- срок действия сертификатов ключей карт мастерских не может быть больше 1 года;
- срок действия сертификатов ключей карт контролирующего органа не может быть больше 2 лет.
- срок действия карт сертификата ключей предприятия– перевозчика не может быть больше 5 лет.

8.5.Выдача сертификатов ключей на карты

[r161] Орган по сертификации ключей должен гарантировать, что выдаваемые им сертификаты ключей целостны и подлинны. Содержание сертификатов определяется Приложением – Добавлением 1B ECTP, Раздел 11.

[r161.1] В процессе запроса на сертификат СР должен гарантировать, что он владеет как закрытой, так и открытой частями этого ключа. При этом закрытая часть ключа никогда не должна покидать оборудования, где он был сгенерирован.

8.6.Продление и обновление сертификатов ключей на карты

См. управление оборудованием. Поскольку срок действия сертификатов и карт совпадает, они должны работать совместно.

8.7. Распространение информации о сертификатах кючей оборудования

[r162] Орган по сертификации ключей должен передавать данные о сертификатах ключей в реестр органа по выпуску карт для обеспечения согласованности между сертификатами ключей, картами и пользователями.

[r163] Орган по выпуску карт должен гарантировать доступность сертификатов ключей для пользователей и всех заинтересованных сторон.

[r164] Орган по выпуску карт должен гарантировать, что все сроки и условия, а так же другие требования документа по реализации управленческих дей-

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

ствий органа по сертификации ключей и другая информация должны быть доступны для всех пользователей и заинтересованных сторон.

[r164.4] Орган по выпуску карт должен сделать доступной информацию сообщать о статусе сертификатов.

8.8.Использование сертификатов ключей на карты

[r165] Сертификаты ключей, описанные в настоящем документе используются только в системе цифровых тахографов.

8.9.Аннулирование сертификатов ключей на оборудование

[r166] Сертификаты ключей не могут аннулироваться. В случае аннулирования сертификата, данная информация должна быть доступной.

9.Управление информационной безопасностью в национальном органе по сертификации ключей и органе по персонализации карт

Этот раздел посвящен мерам по обеспечению информационной безопасности, проистекающим из настоящего документа.

9.1. Управление информационной безопасностью в национальном органе по сертификации ключей и органе по персонализации карт

[r167] Орган по сертификации ключей и орган по персонализации гарантируют, что реализуемые административные и управленческие процедуры отвечают требованиям международных и национальных стандартов по безопасности.

[r168] Орган по сертификации ключей и орган по персонализации несут ответственность за реализацию всех аспектов процедур выпуска сертификатов ключей даже в том случае, если некоторые из этих функций переданы третьей стороне. Ответственность третьих сторон должна быть четко установлена органом по сертификации ключей и органом по персонализации и соответствующим образом прописаны с целью обеспечения того, что третья сторона реализует те требования, которые установлены органом по сертификации ключей и органом по персонализации. Орган по сертификации ключей и орган по персонализации несут ответственность за разъяснения соответствующих обязательств третьим лицам.

[r169] Инфраструктура информационной безопасности предполагает постоянное управление безопасностью внутри органа по сертификации ключей и органом по персонализации. Любые изменения, которые могут повлиять на уровень безопасности, должны быть одобрены Компетентным органом.

[r170] Орган по сертификации ключей должен разработать систему управления безопасностью в соответствии с ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Процедуры формальной сертификации деятельности органа по сертификации ключей не проводится.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

9.2.Классификация «активов» и управление в органе по сертификации ключей и органе по персонализации карт

[r171] Орган по сертификации ключей и орган по персонализации должны гарантировать, что для всех используемых ресурсов и информации обеспечивается должный уровень защиты.

В частности:

а) Орган по сертификации ключей и орган по персонализации должны идентифицировать общие риски, чтобы оценить возможные угрозы для бизнеса и определить (установить) необходимые требования безопасности и операционные (эксплуатационные) процедуры.

б) Орган по сертификации ключей и орган по персонализации должны обеспечить внедрение всех информационных ресурсов и должны разработать классификацию в части требований защиты тех ресурсов, которые подвержены рискам.

9.3.Контроль за выполнением персоналом органа по сертификации ключей и органа по персонализации карт требований безопасности

9.3.1.«Доверительные функции»

[r172] Орган по сертификации ключей и орган по персонализации, обеспечивающие реализацию положений настоящего документа, должны определить как минимум 3 (специфические, определенные) функции (роли) для своего персонала, как указано далее. Должны быть также определены различные механизмы (разработаны мероприятия) в части разделения функций (обязанностей, полномочий) на случай инсайдерских атак настолько подробно, насколько это установлено в документе о практической реализации управленческих решений органа по сертификации ключей и органа по персонализации.

[r173] Понимая, что действия одного человека не могут обеспечить полной безопасности, ответственность органа по сертификации ключей и органа по персонализации в рамках всей системы в части обеспечения безопасности заключается в том, что эту задачу должно решать большое количество людей, обладая широким кругом полномочий (или много людей и множество функций). Любое действие, реализованное конкретным человеком (персоналом) должно иметь органиченное влияние на систему, соразмерное с полномочиями (задачами, ролью) этого человека.

[r174] Рекомендованными ролями являются:

а) администратор органа по сертификации ключей/ администратор органа по персонализации (CAA/PA);

б) системный администратор (SA);

в) представитель службы информационной безопасности (ISSO).

[r175] Роли администратора органа по сертификации ключей или администратора органа по персонализации заключаются в следующем:

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

а) генерация ключей;

б) генерация сертификатов (запрос на выдачу сертификата обрабатывается и исполняется оборудованием органа по сертификации в соответствии с установленными правилами);

в) персонализация и безопасное распространение оборудования;

г) административные функции, связанные с управлением баз данных органа по сертификации ключей и органа по персонализации и идентификацией рисков.

[r176] Роль системного администратора, заключается в следующем:

а) разработка первоначальной конфигурации системы, включая безопасный запуск и безопасное отключение системы;

в) первичная обработка (ввод) всех новых пользователей (нового персонала);

г) установка первичной конфигурации сети;

д) создание аварийной системы перезапуска «оболочки» (среды) на случай внезапной потери данных (системы);

е) создание резервных копий системы, обновление программного обеспечения и его восстановление, включая безопасное хранение и распространение резервных копий и их обновление. Резервные копии должны запускаться (использоваться) по крайней мере раз в неделю, и система должна быть включена/выключена, каждый раз после того, как была запущена резервная копия;

ж) изменение имени хоста и/или адреса сети.

[r177] Роль представителя службы информационной безопасности заключается в следующем:

а) уполномочивание в реализации функций по обеспечению безопасности и управление доступом администраторов органа по сертификации ключей или администраторов органа по персонализации;

б) подписание (разработка) кодов для новых пользователей (нового персонала);

в) выполнение архивирования необходимых отчетов системы;

г) обработка результатов деятельности администраторов органа по сертификации ключей или администраторов органа по персонализации в части соответствия требованиям безопасности системы. Обработка результатов должна осуществляться как минимум один раз в неделю;

д) непосредственный обзор и наблюдение за ежегодными результатами отчетов органа по сертификации ключей и органа по персонализации;

е) участие в генерации ключей РФ.

Важно, чтобы представитель службы информационной безопасности, который непосредственно не вовлечен в процесс выдачи сертификатов, исполнял исключительно надзорную (контрольную) роль в части изучения (проверки) отчетов системы или регистрационных действий системы с целью выполнения персоналом только тех функций, которые установлены настоящим документом.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

9.3.2.Разграничение функций

[r178] Для целей органа по сертификации ключей и органа по персонализации, для выполнения каждой из вышеперечисленных функций (ролей) должны быть назначены разные люди (как минимум по одному человеку на задачу).

9.3.3.Идентификационная и аутентификационная роль каждого

[r179] Идентификационная и аутентификационная роль администратора органа по сертификации ключей и администратора органа по персонализации, системного администратора, представителя службы по информационной безопасности должны быть совместимы и соответствовать методами, процедурам и условиям, заявленным в настоящем документе.

9.3.4.Подготовка, квалификация, опыт и разрешительные требования

[r180] Наличие в штате администратора органа по сертификации ключей и администратора органа по персонализации, наделенных полномочиями по созданию и управлению сертификатами ключей и информацией, является обязательным. Человек, наделенный полномочиями администратора органа по сертификации ключей и администратора органа по персонализации должен быть «целостным», проявлять неоспоримую лояльность и заслуживать доверие и должен осознавать необходимость создания безопасности и реализовывать это в своих ежедневных действиях при выполнении своих полномочий.

[r181] Весь персонал органа по сертификации ключей и органа по персонализации, занимающий должности с доступом к конфиденциальной информации, включая администраторов, представителя службы информационной безопасности, должен соответствовать следующим требованиям:

- не исполнять других обязанность, которые могут негативно отразиться на исполнении текущих обязанностей;
- не быть ранее уволенными с работы по причине не исполнения или не надлежащего исполнения своих должностных обязанностей;
- иметь должную квалификацию и специальную подготовку для исполнения своих должностных обязанностей;
- должен отвечать критериям благонадежности.

9.3.5.Требования к подготовке

[r183] Персонал должен быть должным образом обучен и подготовлен для исполнения своих должностных обязанностей.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

9.4.Контроль за системой безопасности органа по сертификации ключей и органа по персонализации

[r184] Орган по сертификации ключей и орган по персонализации должны гарантировать, что система безопасна и работает правильно с минимальным риском сбоев. Система должна отвечать ряду требований, в частности:

а) целостность системы и информация должны быть защищены от вирусов, несанкционированного доступа, а так же от использования нелицензионного оборудования и программного обеспечения;

б) угроза сбоев должна быть минимизирована с помощью процедур «обратной связи» и сообщений об угрозе.

[r185] Орган по сертификации ключей и орган по персонализации должны обеспечить создание эффективной системы контроля за безопасностью с помощью разделения полномочий, установленных настоящим документом, в соответствующих документах более низкого уровня по реализации управленческих решений.

[r186] Контроль за безопасностью должен обеспечить управление доступом и возможность отслеживания угроз (сбоев) по этапам (уровням) «сверху вниз» (с возможностью перехода на самый низкий уровень) используя закрытую часть ключей органа по сертификации.

[r187] Контроль за безопасностью системы, осуществляемый компьютерными системами, которые используются субподрядными организациями зависит от тех обязанностей, которые возложены на данные организации. Субподрядные организации, выполняющие роль администраторов органа по сертификации и администраторов органа по персонализации в части ввода сертификатов в карты или инициализацию таких карт должны отвечать требованиям, установленным к органу по сертификации ключей и органу по персонализации.

9.4.1.Специфические технические требования для компьютерной безопасности

[r188] Инициализация операционной системы закрытой части ключей органа по сертификаци ключей РФ должна осуществляться как минимум при помощи двух лиц, оба из которых аутентифицированы системой.

9.4.2.Ранг (рейтинг) компьютерной безопасности

[r189] Орган по сертификации ключей и орган по персонализации не требуют формальной оценки до тех пор, пока они отвечают всем требованиям, указанным в этом разделе.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

9.4.3.Средства управления развитием системы

[r190] Орган по сертификации ключей и орган по персонализации должны использовать системы, заслуживающие доверия и программные продукты, защищенные от изменения.

[r191] Анализ требований безопасности должен проводиться в соответствии с требованиями технических заданий любого рабочего проекта, реализуемого органом по сертификации ключей и органом по персонализации или от лица этих органов с целью гарантии того, что безопасность встроена в информационную систему.

[r192] Изменение процедур контроля должно быть прописано на этапах разработки (выпуска), модификации и экстренных ситуаций для любой операционной системы.

9.4.4.Административное управление безопасностью

[r193] Роли (функции, задачи) системы (см. раздел 9.3) должны быть внедрены и реализованы.

9.4.5.Средства управления безопасностью сети

[r194] Управление (например, брандмауэры) должно осуществляться с целью защиты домена внутренней сети органа по сертификации ключей и органа по персонализации от доменов внешней сети, а так же от воздействия третьих лиц.

[r195] Важные (конфиденциальные) данные должны быть надежно защищены в процессе их передачи через сети, которые незащищены.

9.5.Процедуры аудита безопасности

Процедуры аудита безопасности в этом разделе распространяются на все компьютеры и компоненты системы, которые имеют отношение к выпуску ключей, сертификатов процесса выпуска оборудования в соответствии с настоящим документом.

9.5.1. Цели проведения аудита

[r196] Аудит безопасности, связанный с компьютером/системой органа по сертификации ключей и органом по персонализации, должен проводиться (осуществляться) в целях контроля:

а) созданных записей (привилегированных или нет);

б) транзакций, требующих совместного использования записей, вида запроса, индикаторов (информационных сообщений) того, что транзакция закончена или нет, и возможной причины того, что сделка не закончена;

в) инсталляции нового программного обеспечения и его обновления;

г) времени, месте и другой дескриптивной информации обо всех операциях;

д) запуске и выключении программы;

е) времени и месте обновления «аппаратного» оборудования;

ж) времени и даты регистрации сбоев;

з) времени и даты архивации операций.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

9.5.2.Частота проведения аудита данных

[r197] Аудит должен производиться регулярно и анализироваться в части возможных незаконных мероприятий. Процедуры аудита должны быть установлены в документе о практической реализации политики органа по сертификации ключей.

9.5.3.Период хранения данных об аудите

[r198] Результаты проверки (аудита) должны храниться как минимум 7 лет.

9.5.4.Защита регистрационных данных

[r199] Для результатов аудита (регистрационных данных) должна быть обеспечена целостная защита. Все данные (результаты) должны быть опечатаны на все время их хранения.

[r200] Результаты аудита (регистрационные данные) должны проверяться и консолидироваться ежемесячно. Как минимум два человека из числа администраторов органа по сертификации ключей и администраторов органа по персонализации должны быть наделены функциями проверки и консолидации.

9.5.5. Дублирование регистрационных данных

[r201] Две копии консолидированных результатов аудита (регистрационных данных) должны храниться друг от друга отдельно с целью обеспечения надежности и сохранности данных.

[r202] Результаты аудита (регистрационные данные) должны храниться таким образом, чтобы обепечить возможность постоянной проверки регистрационных данных в процессе их хранения.

[r203] Результаты аудита (регистрационные данные) должны быть защищены от несанкционированного доступа.

9.5.6.Система сбора данных

[r204] Применительно к конфиденциальным данным может быть применена только процедура внутреннего аудита.

9.6.Архивация данных

9.6.1.Виды информации (данных), собираемые органом по выпуску карт

[r205] Регистрационная информация должна включать все соответствующие данные, которыми обладает орган по выпуску карт, в т.ч.:

- запросы на получение сертификатов и вся официальная переписка органа по сертификации ключей и органа по персонализации, пользователей;
- подписанные зарегистрированные заявления пользователей на получение карт, включая идентификацию личности лица, принимающего заявления;
- подписанный документ о получении карты;
- договорные соглашения в части сертификатов и карт;
- обновление сертификатов и весь документооборот с пользователями;

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

- аннулированные сообщения и все записанные сообщения (документы), которыми обменивались создатель запроса и/или пользователь;
- документы, ранее применяемые и существующие в настоящий момент.

9.6.2. Виды информации (данных), собираемые органом по сертификации ключей и органом по персонализации

[r206] Записи должны включать все соответствующие данные, которыми обладает орган по сертификации ключей и орган по выпуску карт, в т.ч.:

а) содержание выданных сертификатов;

б) регистрационные журналы, включая данные ежегодного аудита органа по сертификации ключей и органа по выпуску карт, согласованные (предусмотренные) в соответствии с документами о практической реализации положения настоящего документа;

в) документы, касающиеся вопросов сертификации ключей ранее применяемые и существующие в настоящий момент и их связь с документами о практической реализации положений настоящего документа.

[r207] Все записи, в части поданных и подписанных электронных запросов органа по сертификации ключей и органа по персонализации или персонала субподрядчиков должны содержать ответственность администраторов для каждого запроса, а так же всю необходимую информацию, которая нужна для того, чтобы избежать отказа при проведении проверки в течении всего срока хранения данных.

9.6.3. Период хранения архива

[r208] Архивы должны храниться и быть надежно защищены от изменения и разрушения в течении всего периода, установленного документом о реализации практических действий.

9.6.4. Процедуры сбора и изменения архивной информации

[r209] Орган по сертификации ключей и орган по персонализации должны действовать в части конфиденциальности в соответствии с требованиями, установленными в разделе 3.4.

[r210] Записи индивидуальных транзакций могут быть обнародованы по запросу организаций, вовлеченных в процедуру осуществления транзакций, или по запросу их законного представителя.

[r211] Орган по сертификации ключей и орган по персонализации должны обеспечить доступ по запросу к процедурной документации, согласованной с применяемым документом о реализации практических (управленческих) действий согласно раздела 11.5.

[r212] Для проведения описанных выше операций может быть установлена плата, покрывающая расходы на «восстановление (возврат)» записей.

[r213] Орган по сертификации ключей и орган по персонализации должны обеспечить доступность архивов, а также обеспечить хранение архивной информации в доступном для понимания формате в течении всего периода

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

хранения данных, даже если деятельность органа по сертификации и органа по персонализации прервана, остановлена или истекли полномочия.

[r214] В случае если деятельность органа по сертификации ключей и органа по персонализации должны быть прерваны, приостановлены или прекращены, орган по сертификации ключей и орган по персонализации должны направить уведомление всем организациям клиентов, подтверждающее возможность продолжения доступа к архиву Все запросы на доступ к архивированной информации должны быть направлены в орган по сертификации ключей и орган по персонализации или организацию, обозначенную как орган по сертификации ключей и орган по персонализации, до прекращения его деятельности.

9.7. Непрерывное планирование деятельности органа по сертификации ключей и органа по выпуску карт

[r215] Орган по сертификации ключей и орган по персонализации должны иметь перспективный план обеспечения безопасности, содержащий следующие положения:

- действия по обеспечению безопасности ключей;
- действия при внезапной потере данных из-за, например, воровства, огня, отказа аппаратных средств или программного обеспечения;
- действия при неправильной работе системы, возникающие по любой причине.

9.7.1.Угроза (опасность) для закрытой части ключей

Угроза (опасность) для закрытой части ключей описана в раздел 6.

9.7.2. Восстановление вследствие иных угроз

[r216] Орган по сертифкации ключей и орган по персонализации и субподрядные организации должны разработать порядок защиты и минимизации влияние разлчиных угроз на безопасность и эффективность системы в целом.

9.8. Физический (инструментальный) контроль за безопасностью органа по сертификации ключей и системы персонализации

[r217] Физические процедуры управления безопасностью должны быть разработаны с целью управления доступом к программному обеспечению и аппаратным средствам органа по сертифкации ключей и органа по персонализации. Это подразумевает разработку автоматизированных рабочих мест сертификационного органа, а так же персонализацию аппаратных средств и других внешних шифровальных модулей для аппаратных средств и карт. Регистрация должна быть реализована для всех физических записей этой области.

[r218] Ключи РФ для подписания сертификатов должны иметь физическую и логическую защиту так как это указано во внутренних документах органа по персонализации.

[r219] Обязанностью органа по сертификации и органа по персонализации является хранение резервной копии и распространения средств таким способом,

чтобы эффективно предотвратить потери, вмешательство, или несанкционированное использование хранимой информации.

Резервные копии должны храниться для целей восстановления данных и для архивации наиболее важной информации. Резервные средства должны храниться отдельно от местоположения системы сертификационного органа/органа по персонализации, чтобы обеспечить восстановление в случае стихийного бедствия первичного варианта.

[r220] Проверка безопасности местоположения (базирования) центрального оборудование органа по сертификации и органа по персонализации должна проводиться как минимум один раз в течении 24 часов. Если это условие выполняется постоянно, тогда может проводиться визуальная проверка раз в «смену» (один раз в течении рабочего дня) с целью того, чтобы гарантировать, что система и ее отдельные компоненты (устройства/карты) надежно защищены, в случае их не использования», чтобы так же гарантировать что физическая безопасность системы (дверные замки и сигнализация) работает должным образом, для того чтобы не было несанкционированного доступа к системе.

9.8.1.Физический доступ

[r221] Доступ к физическому местоположению ключей РФ и компонентам, которые используются совместно с ними требует одновременного присутствия как минимум 2 людей, которые лично уполномочены для доступа.

[r222] Доступ к другим средства (функциям, полномочиям) органа по сертификации ключей и органа по персонализации разрешен только тому персоналу, которые уполномочен осуществлять одну из функций, указанных в разделе 9.3.1. Доступом можно управлять с использованием списка доступа к месторасположению системы. Если в списке доступа нет лица, который должен осуществить доступ к системе, такой человек должен сопровождаться тем, кому разрешен доступ и его имя значится в списке. Если список управления доступом не установлен для соответствующего «подразделения (участка, этапа)», необходимо быть уверенным, что соответствующие документы (данные, информация, материалы) органа по сертификации ключей и органа по персонализации будут надежно сохранены в надежном месте.

10. Срок исполнения обязательств органа по сертификации ключей РФ и органа по персонализации

10.1.Истечение срока полномочий (заключительные положения) – ответственность органа по сертификации ключей РФ и органа по персонализации.

Истечение срока действия полномочий органа по сертификации и органа по персонализации подразумевает либо ситуацию когда договаривающаяся сторона выходит из системы тахографов, либо сама система прекращает свое существование и в этой связи наличие орган по сертификации ключей или другого уполномоченного органа не представляет дальнейшей необходимости.

Истечение срока полномочий органа по сертификации ключей и органа по персонализации происходит в той ситуации, когда все полномочия (функции, оказание услуг) организаций, занимающихся внедрением системы тахографов, прекратили действие. Такой порядок не распространяется на ситуацию когда функции переданы от одной организации другой или когда сертификационный орган получил полномочия по «хранению» новой пары ключей РФ или ключей европейского сертификационного центра.

[r223] Орган по сертификации ключей РФ гарантирует, что задачи указанные ниже должны быть реализованы.

[r224]Перед тем, как орган по сертификации ключей и орган по персонализации прекратят свои полномочия, должны быть реализованы как минимум следующие мероприятия:

а) проинформировать всех пользователей и других заинтересованных лиц, с которыми у органа по сертификации ключей и органа по персонализации есть соглашения или реализована другая форма установленных отношений;

б) опубликовать информацию о завершении полномочий органа минимум за 3 месяца до завершения срока действия;

в) прекратить (завершить) полномочия всех уполномоченных организаций, действующих от лица органа по сертификации ключей и органа по персонализации в части выдачи (выпуска) сертификатов;

г) предпринять необходимые меры, чтобы обеспечить непрерывный доступ к архивным данным в случае если у Европейского сертификационного центра возникнет такая необходимость.

10.2. Передача ответственности органа по сертификации ключей или органа по персонализации

Передача ответственности (функций) органа по сертификации ключей и органа по персонализации осуществляется тогда, когда Компетентный орган РФ по ЕСТР выбрал в качестве органа по сертификации ключей и органа по персонализации другую организацию в соответствии с установленными процедурами.

[r225] Компетентный **о**рган должен гарантировать, что передача необходимых полномочий (ответственности) и активов будет осуществлена должным образом.

[r226] Прежний органа по сертификации ключей и орган по персонализации должны передать все корневые ключи новому органу по сертификации ключей в порядке, установленном Компететным органом РФ по ЕСТР.

[r227] Прежний орган по сертификации ключей и орган по персонализации должны уничтожить все копии ключей, которые не были переданы новому органу.

11. Аудит

[r228] Компететный органом РФ по ЕСТР ответственен за проведение аудита в органе по сертификации ключей и органе по персонализации.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

11.1.Частота проведения проверок (аудита)

[r229] Орган по сертификации ключей и орган по персонализации, функционирующие в соответствии с настоящим документом, должны обеспечить проведение ежегодного аудита у себя на соответствие требованиям настоящего документа. Первый раз в течение первых 12-ти месяцев с начала осуществления деятельности после одобрения настоящего документа. В случае, если при аудите не выявлены несоответствия, следующий аудит может быть проведен в течение следующих 24 месяцев. В случае, если при аудите выявлены несоответствия, то следующий аудит проводится в течение следующих 12 месяцев.

11.2. Область проведения проверок

[r230] Аудит должен затрагивать все сферы деятельности органа по сертификации ключей и органа по персонализации.

[r231] Аудит проводиться в целях выявления соответствия деятельности органа по сертификации ключей и органа по персонализации положениям настоящего документа.

[r232] **А**удит должен проводиться так же в части деятельности субподрядчиков.

11.3. Кто проводит проверки

[r233] Компететный орган РФ по ЕСТР может консультироваться с внешними компетентными сертифицированными или аккредитованными организациями в части одобрения документов о реализации управленческих (практических) действий органа по сертификации ключей и органа по персонализации с целью повысить ответственность заинтересованных сторон. В других случаях, Компететный орган РФ по ЕСТР обеспечивает проведение аудита самостоятельно.

11.4.Действия, предпринятые по результатам проверки

[r234] В случае выявления несоответствия при проведении процедур аудита, Компететный орган РФ по ЕСТР должен предпринять действия, соответствующие содержанию и важности этих несоответствий.

11.5.Сообщение результатов

[r235] Результаты аудита, на уровне, обеспечивающем статус безопасности системы, должны быть доступны по запросу заинтересованных лиц. Первичные отчеты, сформированные по результатам аудита не могут быть доступны, за исключение особой необходимости.

[r235.1] Компетентный орган анализирует результаты аудита в отчете, который должен включать в себя также корректирующие мероприятия, включая график их реализации с целью обеспечения всех обязательств NA. Отчет должен быть направлен в ERCA на английском языке.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

12. Процедура изменения положений настоящего документа

12.1.Положения, которые могут быть изменены без согласования

[r236] Единственными изменениями, которые могут быть сделаны в части дополнения или изменения положений настоящего документа являются изменения следующего характера:

а) редакционные или типографические изменения (исправления);

б) изменения в «контактную информацию».

12.2.Изменения с уведомления

12.2.1. Уведомления

[r237] О любых изменениях положений настоящей политики необходимо уведомить за 90 дней.

[r238] Изменение положений, в части определения ответственности или полномочий ответственных за реализацию настоящего документа организаций, которые существенно не влияют на большую часть пользователей или других заинтересованных сторон, работающих в соответствии с положениями настоящего документа могут быть внесены в его текст с учетом необходимости уведомить соответствующий орган за 30 дней.

12.2.2. Сроки для комментариев (разъяснений)

[r239] Заинтересованные организации в соответствии с регламентом работы могут оставлять свои комментарии в течении 15 дней с момента уведомления.

12.2.3. Кого необходимо проинформировать

[r240] Уведомление о внесении изменений в политику необходимо отправить:

- EPCA;
- органу по выпуску карт;
- органу по сертификации ключей и органу по персонализации, включая субподрядные организации;
- Европейской Комиссии.

12.2.4. Срок заключительного уведомления о внесении изменений

[r241] Если предложенное изменение было скорректировано как следствие замечаний, уведомление о скорректированном предложенном изменении должно быть дано не менее, чем за 30 дней до вступления в силу такого изменения.

12.3. Изменения, требующие одобрения обновленной национальной политики сертификационного органа

[r242] Если изменения, внесенные в настоящий документ оказывают значительное влияние на большое количество пользователей, Компетентный орган РФ по ЕСТР должен представить обновленный вариант документа на одобрение в ЕРСА.

13.Соотношение между Европейской политикой и настоящим документом.

№	Разделы Европейской политики	Разделы документа РФ
1.	§5.3.1	1.1. Ответственные организации
2.	§5.3.2	6.2.1. Генерация национальных ключей РФ [r101], [r102], [r103]
3.	§5.3.3	6.2.1. Генерация национальных ключей РФ [r104]
4.	§5.3.4	6.2.2. Срок действия ключей договаривающихся сторон [r107], [r108]
5.	§5.3.5	6.2.1. Генерация национальных ключей РФ [r106]
6.	§5.3.6	6.2. Ключи договаривающихся сторон
7.	§5.3.7	6.3. Ключи датчиков движения [r117]
8.	§5.3.8	6.2. Ключи договаривающихся сторон
9.	§5.3.9	6.2. Ключи договаривающихся сторон
10.	§5.3.10	6. Управление общими (корневыми) и транспортными ключами: общеевропейские ключи, ключи договаривающихся сторон (национальные ключи), ключи датчиков движения, транспортные ключи (ключи для переноса)
11.	§5.3.11	6.2.7. Окончание срока действия ключей договаривающейся стороны [r115], [r116]
12.	§5.3.12	6.2.1. Генерация национальных ключей РФ 7.2.1. Генерация ключей оборудования
13.	§5.3.13	6.2.3. Хранение ключей договаривающейся стороной [109], [110]

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

№	Разделы Европейской политики	Разделы документа РФ
		7.2.3. Хранение и защита закрытой части ключей оборудования - карты 7.2.4. Хранение и защита закрытой части ключей оборудования – регистрирующее оборудование
14.	§5.3.14	6.2.3. Хранение ключей договаривающейся стороной [110] 7.2.3. Хранение и защита закрытой части ключей оборудования - карты 7.2.4. Хранение и защита закрытой части ключей оборудования – регистрирующее оборудование
15.	§5.3.15	6.2.3. Хранение ключей договаривающейся стороной [110] 6.2.4. Дубликат закрытой части ключей РФ
16.	§5.3.16	8. Управление сертификатами ключей оборудования 8.5. Выдача сертификатов ключей на оборудование
17.	§5.3.17	6.2.5. «Условное депонирование» закрытой части ключей РФ [r112] 7.2.5. Условное депонирование и архивация закрытой части ключей оборудования [r147]
18.	§5.3.18	6.3. Ключи датчиков движения [r122] 8. Управление сертификатами ключей оборудования
19.	§5.3.19	6.3. Ключи датчиков движения [r118]
20.	§5.3.20	6.3. Ключи датчиков движения [r122]
21.	§5.3.21	6.3. Ключи датчиков движения [r121]
22.	§5.3.22	6.3. Ключи датчиков движения [r117]
23.	§5.3.23	6.3. Ключи датчиков движения

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

№	Разделы Европейской политики	Разделы документа РФ
		[r122] 8. Управление сертификатами ключей оборудования
24.	§5.3.24	7.2.1. Генерация ключей оборудования 7.2.4. Хранение и защита закрытой части ключей оборудования – регистрирующее оборудование
25.	§5.3.25	6.2. Ключи договаривающихся сторон 6.2.1. Генерация национальных ключей РФ [r106] 7.2.1. Генерация ключей оборудования
26.	§5.3.26	9.1. Управление информационной безопасностью в национальном органе по сертификации ключей и органе по персонализации карт [r168]
27.	§5.3.27	6.2. Ключи договаривающихся сторон 6.2.1. Генерация национальных ключей РФ [r105] 8.7. Распространение информации о сертификатах кючей оборудования [r164] 8.9. Аннулирование сертификатов ключей на оборудование [r166]
28.	§5.3.28	6.2.1. Генерация национальных ключей РФ [r101], [r102], [r103]
29.	§5.3.29	6. Управление общими (корневыми) и транспортными ключами: общеевропейские ключи, ключи договаривающихся сторон (национальные ключи), ключи датчиков движения, транспортные ключи (ключи для переноса) 7.2.1. Генерация ключей оборудования
30.	§5.3.30	8.1.2. Регистрирующее оборудование [r153]
31.	§5.3.31	8.7. Распространение информации о сертификатах кючей оборудования [r164]
32.	§5.3.32	7.2.2. Легитимность ключей оборудования 7.2.2.1. Ключи на картах [r139]

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

№	Разделы Европейской политики	Разделы документа РФ
33.	§5.3.33	7.2.3. Хранение и защита закрытой части ключей оборудования - карты [r141]
34.	§5.3.34	8.3. Сертификаты для регистрирующего оборудования (модулей транспортных средств) [r158]
35.	§5.3.35	5.1. Карты тахографов 5.1.2. Заявление на выдачу карты
36.	§5.3.36	6.2.6. Угроза (опасность) для закрытой части ключей
37.	§5.3.37	6.2.6. Угроза (опасность) для закрытой части ключей 9.1. Управление информационной безопасностью в национальном органе по сертификации ключей и органе по персонализации карт
38.	§5.3.38	9.2. Классификация «активов» и управление в органе по сертификации ключей и органе по персонализации карт [r171]
39.	§5.3.39	9.3. Контроль за выполнением персоналом органа по сертификации ключей и органа по персонализации карт требований безопасности
40.	§5.3.40	9.5.1. Цели проведения аудита
41.	§5.3.41	10. Срок исполнения обязательств органа по сертификации ключей РФ и органа по персонализации
42.	§5.3.42	12. Процедура изменения положений настоящего документа
43.	§5.3.43	11. Аудит
44.	§5.3.44	11.1. Частота проведения проверок (аудита)
45.	§5.3.45	11.5. .Сообщение результатов

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

№	Разделы Европейской политики	Разделы документа РФ
46.	§5.3.46	11.4. Действия, предпринятые по результатам проверки

14.Ссылки

[BPM] Digital Tachograph Card Issuing Best Practice Manual. Card Issuing Group, 16 November 2001. - owned by the European Commission.

[CC] Common Criteria. ISO/IEC 15408-1:2009 "Information technology - Security techniques - Evaluation criteria for IT security – Part 1: Introduction and general model".

[CC] Common Criteria. ISO/IEC 15408-2:2008 "Information technology - Security techniques - Evaluation criteria for IT security – Part 2: Security functional components".

[CC] Common Criteria. ISO/IEC 15408-3:2008 "Information technology - Security techniques - Evaluation criteria for IT security – Part 3: Security assurance components".

[CEN] CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Policy requirements for certification authorities issuing public key certificates

[FIPS] FIPS PUB 140-2 (May 25, 2001): "Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)

[ISO 17799] BS ISO/IEC 17799: 2005. Information technology -- Code of practice for information security management.

[CSG] Common Security Guideline, Card Issuing Project. – owed by the European Commission

[ERCA] Digital Tachograph System European Root Policy, Version 2.1; European Commission Joint Research Center Publication 53429; 28th July 2009; published at http://dtc.jrc.ec.europa.eu.

[AETR] European Agreement Concerning the Work of Crews of Vehicles Engaged in International Road Transport (AETR) concluded at Geneva on 1 July 1970

[AETR-PP] Implementation of the AETR - Project plan for AETR Contracting Parties (ECE/TRANS/SC.1/2006/9)

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

[AETR-PS] Practice Statement “AETR. Statement of issuing, distribution, renewal and revocation card using in the control devices of work and rest of crew of vehicle engaged in international road transport.”

[RF-MIN TRAN -180] The Order of Ministry of Transport of Russia on October, 20th, 2009 № 180. registered by Ministry of Justice of the Russian Federation on February, 02, 2010, № 16210 “About the cards used in the digital control device for the control of works and rests of drivers of vehicles engaged in international road transport”.

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

15. Использованные обозначения и сокращения

ЕСТР	**AETP**	Европейское соглашение, касающееся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР), подписанное в г. Женеве 01 июля 1970 г.
	CA	Certification Authority – Сертификационный орган
	CB	Control Body – Контролирующий орган
	CBC	Control Body card – карточка контролирующего органа
	CIA	Card Issuing Authorities – Орган по выдаче карточек
	CID	CardHolder Identification Data – Идентификационные данные держателя карточки
	CKG	Card Key Generation – генерация ключей карточки
	CM	Card manufacturers – производители карточек
	CPe	Card Personalisers – карточка персонала
	CP	Card Personalizing service - орган по персонализации карт
	CR ID	Certificate Request identification – идентификационный запрос на получение сертификата
	DC	Divers Card – карточка водителя
	HSM	Генератор случайных чисел
	EQT.C	Equipment Certificate (for card or vehicle unit) – сертификаты оборудования (для карточек и технического оборудования)
	EQT.PK	Equipment Public Key (for card or vehicle unit) – открытая часть ключей для оборудования (для карточек и технического оборудования)
	EQT.SK	Equipment Secret Key (for card or vehicle unit) – закрытая часть ключей для оборудования (для карточек и технического оборудования)
	ERCA	European Root Certification Authority – Европейский Сертификационный центр

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

	EUR.PK		European Public Key – открытая часть общеевропейских ключей
	EUR.SK		European Secret Key - открытая часть общеевропейских ключей
	IDE		Intelligent Dedicated Equipment – интеллектуальное специализированное оборудование
	IT		Information Technology – информационные технологии
	KID		Key Identifier (Идентификатор ключа)
	KPG		Kp Generation (pairing key) – генерация пары (набора) ключей
	MO		MOtion sensor – датчик движения
	MOM		MOtion sensor Manufacturers – производители датчиков движения
ДС	**MS**	Договаривающаяся сторона	Member State
КО	**MSA**	Компетеный орган по ЕСТР	Member State Authority
	NA	Национальный орган по ЕСТР	National Authority
	MS.C		Member State Certificate – сертификаты РФ
	MS.PK		Member State Public Key – открытая часть ключей РФ
	MS.SK		Member State Secret Key – закрытая часть ключей РФ
	MSCA		Member State Certification Authority – сертификационный орган РФ
	PKI		Public Key Infrastructure – инфраструктура открытой части ключей
	RE		Recording Equipment – регистрирующее оборудование
	RHC		Road Haulage Companies – компания перевозчик
	RHCC		Road Haulage Companies Card – карточка компании – перевозчика
	RSA		Rivest, Shamir, Adelmann (asymmetric encryption scheme) - Rivest, Shamir, Adelmann (асимметрические шифровальные схемы)
	TC		Tachograph Card (карточка тахографа)
	TDES		Triple DES (Date Encryption Standard) – стандарт шифрования данных
	TS		Tachograph System – система тахографов

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru

VU	Vehicle Unit – техническое оборудование
VUKG	Vehicle Unit Key Generation – генерация ключей технического оборудования
VUM	Vehicle Unit Manufacturers – производители технического оборудования
W	vehicle manufacturers, fitters or Workshops – производители оборудования, мастерские
WC	Workshops card – карточка мастерской

Минтранс России, +7 (495) 626-10-88
ФБУ «Росавтотранс»,+7 (495) 496-85-83, E-mail: aetr@rosavtotransport.ru