



Экономический и Социальный Совет

Distr.: General
30 July 2021
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по автомобильному транспорту

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

Двадцать седьмая сессия

Женева, 12 октября 2021 года

Пункт 4 предварительной повестки дня

Система «ТАХОнет»

Представлено Португалией

Настоящий документ, представленный Португалией в качестве государства, председательствующего в Европейском союзе, содержит пересмотренный проект текста возможного нового приложения к Соглашению ЕСТР, касающегося системы «ТАХОнет». Настоящий документ воспроизводит неофициальный документ № 3 (июнь 2021 года), в котором пересмотрен документ ECE/TRANS/SC.1/GE.21/2019/1/Rev.2.



Новое добавление к ЕСТР

Добавление 4

«ТАХОнет» Характеристики системы электронного обмена информацией о карточках водителя

1. Область применения и цель

1.1 В настоящем добавлении излагаются положения и условия, касающиеся подключения Договаривающихся сторон ЕСТР к **системе электронного обмена информацией о карточках водителя «ТАХОнет»** через службу «eDelivery».

1.2 Договаривающиеся стороны, которые подключаются к **системе электронного обмена информацией о карточках водителя «ТАХОнет»** через службу «eDelivery», соблюдают положения настоящего добавления.

2. Определения

a) «Договаривающаяся сторона» или «сторона» означает любую Договаривающуюся сторону ЕСТР;

b) «eDelivery» означает разработанную Европейской комиссией службу передачи данных между третьими сторонами с помощью электронных средств, которая позволяет представлять доказательства, имеющие отношение к обработке переданных данных, в том числе свидетельства отправки и получения этих данных и их защиты от любого риска несанкционированного изменения;

~~c) «ТАХОнет» означает систему электронного обмена информацией о карточках водителей между Договаривающимися сторонами, внедренную Европейской комиссией;~~

cd) «центральный концентратор» означает информационную систему, обеспечивающую возможность маршрутизации сообщений «ТАХОнет» между запрашивающей стороной и стороной-респондентом;

e) «запрашивающая сторона» означает Договаривающуюся сторону, отправляющую запрос или уведомление «ТАХОнет», которое затем направляется соответствующей стороне-респонденту через центральный концентратор;

f) «сторона-респондент» означает Договаривающуюся сторону, которой адресован запрос или уведомление «ТАХОнет»;

g) «орган выдачи карточки», или «ОВК», означает орган, уполномоченный Договаривающейся стороной выдавать карточки тахографа и регулировать их использование;

h)' «субъект данных» означает физическое лицо, данные которого передаются через **систему электронного обмена информацией о карточках водителя «ТАХОнет»**;

h) «персональные данные» означают любую информацию, передаваемую через **систему электронного обмена информацией о карточках водителя «ТАХОнет»** и позволяющую идентифицировать субъект данных, например имя или идентификационный номер;

i) «нарушение неприкосновенности персональных данных» означает нарушение безопасности данных, которое приводит к случайному или противоправному уничтожению, утрате, изменению или несанкционированному раскрытию передаваемых, хранящихся или иным образом обрабатываемых персональных данных, или доступу к ним;

j) «автоматическая обработка» включает следующие операции при условии их полного или частичного выполнения с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, удаление, извлечение или распространение.

3. Общие обязанности

3.1 Никакая Договаривающаяся сторона не может заключать соглашения о предоставлении доступа к **системе электронного обмена информацией о карточках водителя «ТАХОнет»** от имени другой стороны или каким-либо иным образом представлять другую Договаривающуюся сторону на основании настоящего добавления. Никакая Договаривающаяся сторона не может действовать в качестве субподрядчика другой Договаривающейся стороны в операциях, указанных в настоящем добавлении.

3.2 Договаривающиеся стороны обеспечивают доступ к своему национальному регистру карточек водителей через **систему электронного обмена информацией о карточках водителя «ТАХОнет»** таким образом и на таком уровне обслуживания, как это предусмотрено в разделе 4.6 настоящего добавления.

3.3 Договаривающиеся стороны незамедлительно уведомляют друг друга в том случае, если они замечают сбои или ошибки в работе, относящиеся к сфере их ответственности, которые могут поставить под угрозу нормальное функционирование **системы электронного обмена информацией о карточках водителя «ТАХОнет»**.

3.4 Каждая сторона назначает контактных лиц по **системе электронного обмена информацией о карточках водителя «ТАХОнет»** и уведомляет об этом секретариат ЕСТР. Любое изменение, касающееся контактных лиц, должно быть доведено до сведения секретариата ЕСТР в письменном виде.

4. Испытания на подключение к **системе электронного обмена информацией о карточках водителя «ТАХОнет»**

4.1 Подключение Договаривающейся стороны к **системе электронного обмена информацией о карточках водителя «ТАХОнет»** производится после успешного завершения процедуры установления связи, интеграции и эксплуатационных испытаний в соответствии с действующими инструкциями и под контролем Европейской комиссии.

4.2 В случае непрохождения предварительных испытаний Европейская комиссия может приостановить испытательный этап. Испытания возобновляют, после того как Договаривающаяся сторона сообщит Европейской комиссии о реализации необходимых технических усовершенствований на национальном уровне, позволяющих успешно провести предварительные испытания.

4.3 Максимальная продолжительность предварительных испытаний составляет шесть месяцев.

5. Защищенная архитектура

5.1 Конфиденциальность, целостность и неотрекаемость сообщений «ТАХОнет» обеспечивается защищенной архитектурой **системы электронного обмена информацией о карточках водителя «ТАХОнет»**.

5.2 Основой защищенной архитектуры «ТАХОнет» является служба инфраструктуры открытых ключей (ИОК), которая была создана Европейской комиссией и требования которой изложены в разделах 4.8 и 4.9 настоящего добавления.

5.3 С защищенной архитектурой «ТАХОнет» взаимодействуют следующие субъекты:

а) Сертификационный орган, который отвечает за создание цифровых сертификатов, выдаваемых (после проверки запроса ~~Регистрационным органом~~ **Органом проверки запросов**) для загрузки национальными компетентными органами Договаривающихся сторон (через ~~назначенных ими доверенных курьеров~~ **онлайнный портал системы ИОК Сертификационного органа**), а также за обеспечение соответствующей технической инфраструктуры для выдачи, отмены и обновления цифровых сертификатов;

b) владелец домена, отвечающий за работу центрального концентратора, указанного в разделе 4.1 настоящего добавления, а также проверку и координацию защищенной архитектуры «ТАХОнет»;

c) ~~Регистрационный орган~~ **Орган проверки запросов**, отвечающий за **проверку подлинности личности запрашивающей организации, ее контактных лиц и доверенных курьеров. В рамках регулярных сеансов ЕГСО компетентные национальные органы смогут подавать через доверенного курьера ЕГСО запросы на сертификаты для проверки. ОИЦ будет проверять запросы на сертификаты в ходе телефонного звонка контактному лицу ЕГСО (официально назначенному компетентным органом государства-участника) в ходе сеансов ЕГСО** ~~регистрацию и утверждение запросов на выдачу, отзыв и обновление цифровых сертификатов и за проверку личности доверенных курьеров;~~

d) доверенный курьер — **физическое лицо, назначенное ответственным лицом национального органа для проверки подлинности запроса на сертификат в Орган проверки запросов и получения соответствующего сертификата от Сертификационного органа** ~~лицо, назначенное национальным органом и отвечающее за передачу открытого ключа Регистрационному органу и получение соответствующего сертификата, выдаваемого Сертификационным органом;~~

e) национальный орган Договаривающейся стороны, который:

i) создает закрытые ключи и соответствующие открытые ключи, подлежащие включению в сертификаты, выдаваемые Сертификационным органом;

ii) запрашивает у Сертификационного органа цифровые сертификаты;

iii) назначает доверенного курьера.

5.4 Сертификационный орган и ~~Регистрационный орган~~ **Орган проверки запросов** назначаются Европейской комиссией.

5.5 Любая Договаривающаяся сторона, которая подключается к **системе электронного обмена информацией о карточках водителя «ТАХОнет»**, должна направить запрос на выдачу цифрового сертификата в соответствии с разделом 4.9 настоящего добавления в целях подписания и шифрования сообщения «ТАХОнет».

5.6 Сертификат может быть отозван в соответствии с разделом 4.9 настоящего добавления.

6. Защита данных и конфиденциальность

6.1 Стороны принимают все необходимые технические и организационные меры с целью гарантировать безопасность данных «ТАХОнет», **передаваемых через систему электронного обмена информацией о карточках водителя**, и предотвращать изменение, утрату или несанкционированную обработку этих данных или доступ к ним (в частности, обеспечивать подлинность, конфиденциальность данных, отслеживаемость, целостность, доступность, неотрекаемость и сохранность сообщений).

6.2 В том случае, если одной из сторон становится известно о нарушении целостности персональных данных, она в кратчайшие сроки информирует об этом Европейскую комиссию и использует разумные и надлежащие средства для устранения этого нарушения и сведения к минимуму его возможных негативных последствий.

6.3 Стороны предоставляют субъекту данных, чьи персональные данные были получены через **систему электронного обмена информацией о карточках водителя «ТАХОнет»**, возможность:

Статья I а) потребовать подтверждение по поводу того, находятся ли персональные данные, относящиеся к этому субъекту данных, на хранении, а также получить эти данные в краткой, прозрачной, понятной и легкодоступной форме;

Статья II б) потребовать в случае необходимости исправления неточных персональных данных без неоправданных задержек;

Статья III с) потребовать в случае необходимости удаления персональных данных, если они больше не требуются соответствующей стороне или если они были обработаны незаконно или в нарушение основных принципов, изложенных в статьях 5 и 6 Конвенции о защите физических лиц при автоматизированной обработке персональных данных (далее «Конвенция»);

Статья IV d) в любое время по причинам, связанным с его или ее личными обстоятельствами, высказать возражения против обработки его или ее персональных данных какой-либо стороной.

Статья V 6.4 В случае необходимости автоматической обработки персональных данных, полученных через **систему электронного обмена информацией о карточках водителя «ТАХОнет»**, она производится в соответствии с Конвенцией.

6.5 Стороны идентифицируют любые персональные данные, переданные запрашивающей стороне через **систему электронного обмена информацией о карточках водителя «ТАХОнет»**, и предоставляют общую информацию, например такую, которая содержится на соответствующем веб-сайте, по поводу мер безопасности применительно к передаче данных другим сторонам.

6.6 Сторона-респондент передает персональные данные через **систему электронного обмена информацией о карточках водителя «ТАХОнет»** только с законной и конкретной целью оказания помощи запрашивающей стороне в выполнении настоящего Соглашения. Запрашивающая сторона не производит дальнейшую обработку персональных данных, которая несовместима с этой целью.

6.7 Сторона-респондент передает персональные данные только в соответствии с настоящим Соглашением.

6.8 Запрашивающая сторона, получающая персональные данные **через систему электронного обмена информацией о карточках водителя «ТАХОнет»**, передает эти данные третьей стороне только в том случае, если эта третья сторона является национальным компетентным органом, уполномоченным проверять или обеспечивать соблюдение продолжительности периодов работы и отдыха в соответствии с настоящим Соглашением.

6.9 Запрашивающие стороны хранят персональные данные не дольше, чем это необходимо и уместно для той цели, с которой эти данные обрабатываются. Такой срок хранения должен соответствовать действующим законам, правилам и предписаниям, регламентирующим хранение таких данных в пределах юрисдикции запрашивающей стороны.

7. Расходы

7.1 Договаривающиеся стороны несут расходы по осуществляемой ими разработке и использованию собственных систем и процедур обработки данных, которые необходимы для выполнения обязательств на основании настоящего добавления.

7.2 Услуги, указанные в разделе 4.1 настоящего добавления, предоставляются центральным концентратором бесплатно.

8. Привлечение субподрядчиков

8.1 Стороны могут передавать на подряд любые услуги, за которые они несут ответственность на основании настоящего добавления.

8.2 Привлечение субподрядчиков не освобождает данную сторону от ответственности на основании настоящего добавления, включая ответственность за обеспечение надлежащего уровня обслуживания в соответствии с разделом 4.6 настоящего добавления.

Раздел 4.1 добавления

Общие аспекты системы электронного обмена информацией о карточках водителя «ТАХОнет»

1. Общее описание

Система электронного обмена информацией о карточках водителя «ТАХОнет» — ~~электронная система обмена информацией о карточках водителя. Она~~ осуществляет маршрутизацию запросов информации от запрашивающей стороны стороне-респонденту и ответов от стороны-респондента запрашивающей стороне. Договаривающиеся стороны, которые используют систему **электронного обмена информацией о карточках водителя «ТАХОнет»**, должны подключить к этой системе свои национальные регистры карточек водителя.

2. Архитектура

~~Система обмена сообщениями «ТАХОнет»~~ **электронного обмена информацией о карточках водителя** состоит из следующих частей:

2.1 Центральный концентратор, который в состоянии получать и проверять запрос от запрашивающей стороны и обрабатывать его путем его перенаправления сторонам-респондентам. Центральный концентратор ждет ответа от каждой стороны-респондента, синтезирует их и направляет сводный ответ запрашивающей стороне.

2.2 Национальные системы сторон имеют интерфейс, позволяющий им направлять запросы в центральный концентратор и получать на них ответы. Национальные системы могут использовать собственное или коммерческое программное обеспечение для передачи сообщений в центральный концентратор и их получения из него.

3. Управление

3.1 Центральный концентратор находится в ведении Европейской комиссии, которая несет ответственность за его техническую эксплуатацию и обслуживание.

3.2 Центральный концентратор хранит данные в течение периода, не превышающего шесть месяцев, помимо данных журналов и статистических данных, определенных в разделе 4.7 настоящего добавления.

3.3 Центральный концентратор не предоставляет доступа к персональным данным, за исключением уполномоченных сотрудников Европейской комиссии в тех случаях, когда это необходимо в целях мониторинга, обслуживания и устранения неисправностей.

3.4 Каждая Договаривающаяся сторона несет ответственность за:

3.4.1 конфигурирование собственных национальных систем и управление ими, включая интерфейсы для связи с центральным концентратором;

3.4.2 установку и обслуживание ее национальной системы, включая аппаратное и программное обеспечение, будь то собственное или коммерческое;

3.4.3 надлежащую эксплуатационную совместимость ее национальной системы с центральным концентратором, включая обработку сообщений об ошибках, полученных из центрального концентратора;

3.4.4 принятие всех мер в целях обеспечения конфиденциальности, целостности и доступности информации;

3.4.5 работу национальных систем в соответствии с уровнями обслуживания, определенными в разделе 4.6 настоящего добавления.

Раздел 4.2 добавления

Функциональные возможности системы электронного обмена информацией о карточках водителя «ТАХОнет»

1. Система электронного обмена информацией о карточках водителя ~~ее~~общений «ТАХОнет» обеспечивает следующие функции:

1.1 функция «проверки выдачи карточек» (Check Issued Cards) (CIC) позволяет запрашивающей стороне направлять одной или всем сторонам-респондентам запрос на проверку выдачи карточек (Check Issued Cards Request) для выяснения того, имеет ли уже соискатель карточки карточку водителя, выданную сторонами-респондентами. Стороны-респонденты отвечают на запрос, направляя ответ по результатам проверки выдачи карточек (Check Issued Cards Response);

1.2 функция «проверки статуса карточки» (Check Card Status) (CCS) позволяет запрашивающей стороне запрашивать у стороны-респондента сведения по карточке, выданной стороной-респондентом, посредством направления ей запроса на проверку статуса карточки (Check Card Status Request). Сторона-респондент отвечает на запрос, направляя ответ по результатам проверки статуса карточки (Check Card Status Response);

1.3 функция «изменения статуса карточки» (Modify Card Status) (MCS) позволяет запрашивающей стороне уведомлять сторону-респондента посредством запроса об изменении статуса карточки (Modify Card Status Request) о том, что статус карточки, выданной стороной-респондентом, изменился. Сторона-респондент направляет ответ с подтверждением изменения статуса карточки (Modify Card Status Acknowledgement);

1.4 функция «выдачи карточки на основании водительского удостоверения» (Issued Card Driving Licence) (ICDL) позволяет запрашивающей стороне уведомить сторону-респондента — посредством запроса относительно выдачи карточки на основании водительского удостоверения (Issued Card Driving Licence Request) — о том, что карточка была выдана запрашивающей стороной по предъявлении водительского удостоверения, выданного стороной-респондентом. Сторона-респондент направляет ответ в связи с выдачей карточки на основании водительского удостоверения (Issued Card Driving Licence Response).

2. Впоследствии будут добавлены сообщения других типов, считающиеся целесообразными для обеспечения эффективного функционирования **системы электронного обмена информацией о карточках водителя «ТАХОнет»**, например уведомления об ошибках.

3. Национальные системы признают статусы карточек, перечисленные в таблице 1, при использовании любой из функций, описанных в пункте 1. Вместе с тем сторонам нет необходимости вводить административную процедуру, охватывающую использование всех перечисленных статусов.

4. Если сторона получает ответ или уведомление с указанием статуса, который не используется в ее административных процедурах, то национальная система преобразует статус, указанный в полученном сообщении, в соответствующее значение в рамках ее административной процедуры. Сторона-респондент не отклоняет сообщение, если указанный в нем статус значится в таблице 1.

5. Статус карточки, указанный в таблице 1, не должен использоваться для определения того, действительна ли карточка водителя для управления транспортным средством. Когда сторона направляет запрос в регистр национального органа, выдавшего карточку, с помощью функции CCS, ответ должен содержать специальное поле «действительна для управления». Национальные административные процедуры должны быть такими, чтобы ответы CCS всегда содержали соответствующее значение поля «действительна для управления».

Таблица 1
Статусы карточки

Статус карточки	Определение
Запрошена	ОВК получил заявку на выдачу карточки водителя. Эта информация регистрируется и заносится в базу данных с созданными ключами поиска.
Утверждена	ОВК утвердил заявку на карточку тахографа.
Отклонена	ОВК не утвердил заявку.
Персонализирована	Карточка тахографа была персонализирована.
Отправлена	Национальный орган отправил карточку водителя соответствующему водителю или учреждению, которое занимается выдачей.
Передана	Национальный орган передал карточку водителя соответствующему водителю.
Конфискована	Карточка водителя была изъята у водителя компетентным органом.
Приостановлена	Карточка водителя была временно изъята у водителя.
Отменена	ОВК решил отозвать карточку водителя. Карточка была безвозвратно аннулирована.
Возвращена	Карточка тахографа была возвращена в ОВК с указанием, что она больше не требуется.
Утеряна	ОВК получил уведомление о том, что карточка тахографа утеряна.
Похищена	ОВК получил уведомление о том, что карточка тахографа похищена. Похищенная карточка считается утерянной.
Работает неисправно	ОВК получил уведомление о том, что карточка тахографа работает неисправно.
Срок действия истек	Срок действия карточки тахографа истек.
Заменена	Карточка тахографа, которая, в соответствии с полученным сообщением, была утеряна, похищена или работала неисправно, была заменена новой карточкой. Новая карточка содержит те же данные, за исключением индекса номера замены карточки, который увеличивается на единицу.
Обновлена	Карточка тахографа была обновлена в связи с изменением административных данных или истечением срока действия. Номер новой карточки остается прежним, за исключением индекса номера обновления карточки, который увеличивается на единицу.
В процессе обмена	ОВК, который выдал карточку водителя, получил уведомление о начале процедуры ее обмена на карточку водителя, которую выдает ОВК другой стороны.
Обменена	ОВК, который выдал карточку водителя, получил уведомление о завершении процедуры ее обмена на карточку водителя, которую выдает ОВК другой стороны.

Раздел 4.3 добавления

Положения, регламентирующие обработку сообщений системой электронного обмена информацией о карточках водителя «ТАХОнет»

1. Общие технические требования

1.1 Центральный концентратор имеет синхронный и асинхронный интерфейсы для обмена сообщениями. Стороны могут выбирать наиболее подходящую для них технологию для обеспечения взаимодействия их собственных прикладных программ с концентратором.

1.2 Все сообщения, которыми обмениваются центральный концентратор и национальные системы, должны кодироваться в соответствии со стандартом UTF-8.

1.3 Национальные системы должны быть в состоянии получать и обрабатывать сообщения, содержащие знаки греческого алфавита и кириллицы.

2. Структура сообщений XML и определение схемы (XSD)
- 2.1 Общая структура сообщений XML следует формату, определенному схемами XSD, установленными в центральном концентраторе.
- 2.2 Центральный концентратор и национальные системы передают и получают сообщения, которые соответствуют схеме XSD.
- 2.3 Национальные системы должны быть в состоянии отправлять, принимать и обрабатывать все сообщения, соответствующие любой из функций, указанных в разделе 4.2 настоящего добавления.
- 2.4 Сообщения XML должны отвечать по крайней мере минимальным требованиям к содержанию, изложенным в таблице 2.

Таблица 2

Минимальные требования к содержанию сообщений XML

<i>Общий заголовок</i>		<i>В обязательном порядке</i>
Версия	Официальная версия спецификаций XML указывается с помощью пространства имен, определенного в схеме XSD сообщения и в атрибуте «Версия» элемента заголовка каждого сообщения XML. Номер версии («п.п») определяется как фиксированное значение для каждой версии файла «Определение схемы XML» (xsd).	Да
Идентификатор теста	Факультативный идентификатор для тестирования. Инициатор теста заполняет поле идентификатора, а все участники процесса перенаправляют/возвращают тот же идентификатор. В реальных условиях эксплуатации он никакой роли не играет, а если он все же указан, его не следует использовать.	Нет
Технический идентификатор	Идентификатор УУИД однозначно идентифицирует каждое индивидуальное сообщение. Отправитель создает УУИД и указывает этот атрибут. В рабочих процессах этот элемент данных не используется.	Да
Идентификатор рабочего процесса	Идентификатор рабочего процесса является УУИД и должен быть создан запрашивающей стороной. Впоследствии этот идентификатор используется во всех сообщениях в целях корреляции рабочего процесса.	Да
Отправлено в	Дата и время (UTC) отправления сообщения.	Да
Превышение времени ожидания	Это факультативный атрибут даты и времени (в формате UTC). Его значение устанавливается центральным концентратором только для перенаправленных запросов. Он указывает стороне-респонденту на время, когда интервал ожидания для запроса будет превышен. Это значение не требуется для MS2TCN_<x>_Req и всех ответных сообщений. Оно факультативно, поэтому одно и то же определение заголовка можно использовать для всех типов сообщений, независимо от того, требуется ли атрибут timeoutValue или нет.	Нет

<i>Общий заголовок</i>	<i>В обязательном порядке</i>
От	Код ISO 3166-1 Alpha 2 стороны, отправляющей сообщение, или «ЕС». Да
В адрес	Код ISO 3166-1 Alpha 2 стороны, в адрес которой отправляется сообщение, или «ЕС». Да

Раздел 4.4 добавления

Транслитерация и службы NYSIS (Система идентификации и сбора данных штата Нью-Йорк)

- Для кодирования имен всех водителей в национальном регистре используется алгоритм NYSIS, заложенный в центральном концентраторе.
- При поиске карточки посредством функции SIC в качестве основного механизма поиска используются ключи NYSIS.
- Кроме того, для получения дополнительных результатов стороны могут использовать индивидуальный алгоритм.
- В результатах поиска указывается механизм поиска, который использовался для обнаружения той или иной записи, — NYSIS или индивидуальный.
- Если сторона намерена регистрировать уведомления ICDL, то ключи NYSIS, содержащиеся в уведомлении, регистрируются как часть данных ICDL. При поиске данных ICDL сторона пользуется ключами NYSIS, которые относятся к имени заявителя.

Раздел 4.5 добавления

Требования в области безопасности

- Для обмена сообщениями между центральным концентратором и национальными системами используется протокол HTTPS.
- Для целей безопасной передачи сообщений между национальной системой и центральным концентратором национальные системы используют цифровые сертификаты, указанные в разделах 4.8 и 4.9 настоящего добавления.
- В национальных системах, как минимум, должны использоваться сертификаты с хэш-алгоритмом подписи SHA-2 (SHA-256) и длиной открытого ключа 2048 бит.

Раздел 4.6 добавления

Уровни обслуживания

- Национальные системы обеспечивают нижеследующий минимальный уровень обслуживания:
 - Они работают в круглосуточном режиме семь дней в неделю.
 - Мониторинг их работоспособности осуществляется при помощи тактового (heartbeat) сообщения, отправляемого центральным концентратором.
 - Норма их оперативной готовности составляет 98 % в соответствии со следующей таблицей (цифры округлены до ближайшей единицы):

<i>Оперативная готовность</i>	<i>означает недоступность</i>		
	в сутки	в месяц	в год
98 %	0,5 часа	15 часов	7,5 суток

Сторонам рекомендуется соблюдать нормы суточной оперативной готовности, но следует признать, что для проведения некоторых необходимых мероприятий, таких как обслуживание системы, ее работа может быть приостановлена на период более

30 минут. Вместе с тем ежемесячные и ежегодные нормы оперативной готовности являются обязательными.

1.4 Национальные системы должны реагировать как минимум на 98 % запросов, направленных им в течение одного месяца.

1.5 Они должны отвечать на запросы в течение периода до 10 секунд.

1.6 Общая продолжительность времени до превышения периода ожидания (время, в течение которого запрашивающая сторона может ждать ответ) не должна превышать 20 секунд.

1.7 Национальные системы должны быть в состоянии соблюдать норму обслуживания запросов на уровне шести сообщений в секунду.

1.8 Национальные системы не должны направлять запросы в **центральный** концентратор «ТАХОнет» с частотой более двух запросов в секунду.

1.9 Каждая национальная система должна быть в состоянии справляться с возможными техническими проблемами в центральном концентраторе или национальных системах других сторон. К числу таких проблем, в частности, относятся:

- a) потеря связи с центральным концентратором;
- b) отсутствие ответа на запрос;
- c) получение ответа после истечения предусмотренного времени ожидания ответа на сообщение;
- d) получение посторонних сообщений;
- e) получение недействительных сообщений.

2. Центральный концентратор должен:

2.1 обеспечивать норму оперативной готовности на уровне 98 %;

2.2 направлять национальным системам уведомление о любых ошибках либо с помощью ответного сообщения, либо с помощью специального сообщения об ошибке. В свою очередь в национальных системах, получающих эти сообщения, должна быть предусмотрена процедура их передачи на более высокий уровень для принятия надлежащих мер по устранению указанной ошибки.

3. Эксплуатационно-техническое обслуживание

Стороны при помощи веб-приложения уведомляют другие стороны и Европейскую комиссию о любых плановых работах по обслуживанию, как минимум, за одну неделю до их начала, если это возможно с технической точки зрения.

Раздел 4.7 добавления

Данные журналов и статистические данные, собираемые в центральном концентраторе

1. В целях обеспечения конфиденциальности данные, собираемые в статистических целях, должны быть анонимными. Использование данных, позволяющих идентифицировать конкретную карточку, водителя или водительское удостоверение, в статистических целях не допускается.

2. Данные журналов обеспечивают учет всех операций для целей мониторинга и отладки и могут использоваться для подготовки статистических данных об этих операциях.

3. Персональные данные хранятся в журналах не более шести месяцев. Статистическая информация хранится бессрочно.

4. Статистические данные для отчетности включают данные, касающиеся:
 - a) запрашивающей стороны;
 - b) стороны-респондента;
 - c) типа сообщения;
 - d) кода статуса ответа;
 - e) даты и времени сообщений;
 - f) времени ожидания ответа.

Раздел 4.8 добавления

Общие положения, касающиеся цифровых ключей и сертификатов «ТАХОнет»

1. Генеральный директорат Европейской комиссии по информатике (ДИГИТ) предоставляет в распоряжение Договаривающихся сторон ЕСТР, подключающихся к **системе электронного обмена информацией о карточках водителя «ТАХОнет»** (далее именуемых «национальными органами») через «eDelivery», службу ИОК¹ (именуемую «службой ИОК ФОЕ»).

2. Процедура запроса и отзыва цифровых сертификатов, а также подробные условия их использования определены в разделе 4.9 настоящего добавления.

3. Использование сертификатов

3.1 После выдачи сертификата национальный орган² должен использовать сертификат только в рамках системы **электронного обмена информацией о карточках водителя «ТАХОнет»**. Сертификат может использоваться для:

- a) аутентификации происхождения данных;
- b) кодирования данных;
- c) надежного выявления случаев нарушения целостности данных.

3.2 Любое использование сертификата, не разрешенное в явном виде в качестве одного из вариантов разрешенного использования, запрещено.

4. Договаривающиеся стороны:

a) обеспечивают защиту своего закрытого ключа от несанкционированного использования;

b) воздерживаются от передачи или раскрытия закрытого ключа третьим сторонам, даже если последние действуют в качестве их представителей;

c) обеспечивают конфиденциальность, целостность и доступность закрытых ключей, которые были созданы и находятся на хранении и в использовании **в системе «ТАХОнет»**;

d) воздерживаются от дальнейшего использования закрытого ключа по истечении срока действия или отзыва сертификата, помимо просмотра зашифрованных данных (например, для расшифровки сообщений электронной почты). Ключи, срок действия которых истек, либо уничтожаются, либо хранятся таким образом, который исключает возможность их использования;

e) предоставляют ~~Регистрационному органу~~ **Органу проверки запросов** идентификационные данные тех уполномоченных представителей, которым разрешается направлять требование об отзыве сертификатов, выданных для данной

¹ ИОК (инфраструктура открытых ключей) — это набор ролей, правил, процедур и систем, необходимых для создания, распространения и отзыва цифровых сертификатов и управления ими.

² Идентифицируется значением атрибута «O=» в уникальном имени субъекта выданного сертификата.

организации (требования об отзыве включает пароль отзыва и данные о событиях, которые обусловили необходимость отзыва);

f) предотвращают неправомерное использование закрытого ключа, направляя требование об отзыве связанного с ним сертификата открытого ключа в случае нарушения безопасности закрытого ключа или данных активации закрытого ключа;

g) несут ответственность и соблюдают обязательство требовать отзыва сертификата в случаях, предусмотренных политикой сертификации (ПС) и регламентом сертификационной практики (РСП) Сертификационного органа;

h) незамедлительно уведомлять ~~Регистрационный орган~~ **Орган проверки запросов** об утере, краже или возможном нарушении безопасности любых ключей ЕСТР, используемых в рамках системы **электронного обмена информацией о карточках водителя «ТАХОнет»**.

5. Ответственность

Без ущерба для ответственности Европейской комиссии в случае нарушения любых требований, установленных применимым законодательством, или в тех случаях, когда она не может быть исключена в соответствии с этим законодательством, Европейская комиссия не несет ответственности или обязательств в отношении:

a) содержания сертификата, ответственность за которое несет исключительно владелец сертификата. Проверка точности содержания сертификата возлагается на его владельца;

b) использования сертификата его владельцем.

Раздел 4.9 добавления

Описание службы ИОК для системы электронного обмена информацией о карточках водителя «ТАХОнет»

1. Введение

ИОК (инфраструктура открытых ключей) — это набор ролей, правил, процедур и систем, необходимых для создания, распространения и отзыва цифровых сертификатов и управления ими³. Служба «eDelivery» ИОК ФОЕ обеспечивает выдачу цифровых сертификатов, используемых для обеспечения конфиденциальности, целостности и неотрекаемости информации, передаваемой между точками доступа (ТД), и управление этими сертификатами.

Служба «eDelivery» ИОК работает на базе сертификационного органа (СО) Trust Center Services TeleSec Shared Business («Траст Центр Сервисез ТелеСек Шэрд Бизнес»), на который распространяется политика сертификации (ПС) и регламент сертификационной практики (РСП) СО TeleSec Shared-Business-CA компании «**Дойче телеком секьюрити, «Т-Системз Интернэшнл ГмБХ» (Deutsche Telekom Security GmbH⁴)**».

Служба ИОК выдает сертификаты, которые могут использоваться для обеспечения безопасности различных бизнес-процессов внутри и вне компаний, организаций, государственных органов и учреждений, которым требуется средний уровень безопасности для подтверждения подлинности, целостности и достоверности конечного субъекта.

³ https://ru.wikipedia.org/wiki/Инфраструктура_открытых_ключей.

⁴ Актуальную версию ПС и РСП можно загрузить по адресу <https://www.telesec.de/en/sbca-en/support/download-area/>.

2. Процедура запроса сертификата
- 2.1 Роли и обязанности
- 2.1.1 «Организация» или «национальный орган», запрашивающие сертификат
- 2.1.1.1 Национальный орган запрашивает сертификаты ~~в контексте проекта «ТАХОнет».~~
- 2.1.1.2 Национальный орган:
- a) запрашивает сертификаты в службе ИОК ФОЕ;
 - b) создает закрытые ключи и соответствующие открытые ключи, подлежащие включению в сертификаты, выдаваемые Сертификационным органом;
 - c) загружает сертификат после утверждения;
 - d) подписывает и отправляет обратно ~~Регистрационному органу~~ **Органу проверки запросов**:
 - i) идентификационную форму контактных лиц и доверенных курьеров,
 - ii) подписанную индивидуальную доверенность⁵.
- 2.1.2 Доверенный курьер
- 2.1.2.1 Национальный орган назначает доверенного курьера, **если это еще не сделано для ЕГСО; назначенный доверенный курьер должен быть одним и тем же лицом для системы электронного обмена информацией о карточках водителя и ЕГСО.**
- 2.1.2.2 Доверенный курьер:
- a) **удостоверяет запросы на сертификат перед Органом проверки запросов в ходе уже налаженного и хорошо известного процесса очной идентификации и регистрации для сеансов подписания ЕГСО; и передает открытый ключ Регистрационному органу в процессе очной идентификации и регистрации;**
 - b) **получает/загружает соответствующий сертификат из системы ИОК Сертификационного органа, после того как сертификат был создан и стал доступен. Регистрационного органа**
- 2.1.3 Владелец домена
- 2.1.3.1 Владелец домена является ГД МОТР.
- 2.1.3.2 Владелец домена:
- a) проверяет и координирует работу ~~ее~~ **«ТАХОнет» системы электронного обмена информацией о карточках водителя** и защищенной архитектуры ~~«ТАХОнет»~~, включая проверку процедур выдачи сертификатов;
 - b) управляет работой центрального концентратора ~~«ТАХОнет»~~ и координирует деятельность сторон в части функционирования **системы электронного обмена информацией о карточках водителя «ТАХОнет»**;
 - c) проводит вместе с национальными органами испытания для подключения к **системе электронного обмена информацией о карточках водителя «ТАХОнет».**

⁵ Доверенность — это юридический документ, которым организация наделяет Европейскую комиссию в лице назначенного ею должностного лица, ответственного за службу ИОК ФОЕ, полномочиями запрашивать создание сертификата от ее имени у сертификационного органа TeleSec Shared Business компании **«Дойче телеком секьюрити, ГмбХ» «Т-Системз Интернэшнл ГмбХ»**. См. также пункт 6.

2.1.4 ~~Регистрационный орган~~ **Орган проверки запросов**

2.1.4.1 ~~Функции Регистрационного органа~~ **Органа проверки запросов** выполняет Объединенный исследовательский центр (ОИЦ).

2.1.4.2 ~~Регистрационный орган~~ **Орган проверки запросов** отвечает за **проверку подлинности запрашивающей организации, личности ее контактных лиц и доверенных курьеров. Орган проверки запросов проверяет запросы на сертификаты для системы электронного обмена информацией о карточках водителя в рамках валидации путем телефонного звонка контактному лицу ЕГСО (официально назначенному компетентным органом государства-участника) в ходе сеансов ЕГСО** ~~проверку личности доверенного курьера, регистрацию и утверждение запросов на выдачу, отзыв и обновление цифровых сертификатов.~~

2.1.4.3 ~~Регистрационный орган~~ **Орган проверки запросов:**

- a) присваивает национальному органу уникальный идентификатор;
- b) удостоверяет подлинность национального органа, личность его контактных лиц и доверенных курьеров;
- c) взаимодействует со службой поддержки ФОЕ в связи с вопросами подлинности национального органа, личности его контактных лиц и доверенных курьеров;
- d) информирует национальный орган об утверждении или отклонении запроса на сертификат.

2.1.5 Сертификационный орган

2.1.5.1 Сертификационный орган отвечает за обеспечение технической инфраструктуры для обработки запросов, выдачи и отзыва цифровых сертификатов.

2.1.5.2 Сертификационный орган:

- a) обеспечивает техническую инфраструктуру, необходимую для обработки запросов национальных органов на выдачу сертификатов;
- b) утверждает или отклоняет запросы на выдачу сертификата;
- c) связывается с ~~Регистрационным органом~~ **Органом проверки запросов** для проверки подлинности запрашивающей организации, когда это необходимо.

2.2 Выдача сертификатов

2.2.1 Выдача сертификатов производится в соответствии со следующими этапами:

- a) этап 1: идентификация доверенного курьера;
- b) этап 2: создание запроса на сертификат;
- c) этап 3: Регистрация в **РФ Органе проверки запросов**;
- d) этап 4: создание сертификата;
- e) этап 5: публикация сертификата;
- f) этап 6: принятие сертификата.

2.2.2 Этап 1: Идентификация доверенного курьера

Для идентификации доверенного курьера:

- a) ~~Регистрационный орган~~ **Орган проверки запросов** направляет национальному органу идентификационную форму контактных лиц и доверенных курьеров⁶ **(та же, что идентификационная форма ЕГСО). Эта форма включает также**

⁶ См. пункт 5.

К этой форме прилагается доверенность, которая подписывается организацией (компетентным органом по ЕСТР).

b) Национальный орган направляет обратно заполненную форму и подписанную доверенность ~~Регистрационному органу~~ **Органу проверки запросов**;

c) ~~Регистрационный орган~~ **Орган проверки запросов** подтверждает факт получения и правильного заполнения формы;

d) ~~Регистрационный орган~~ **Орган проверки запросов** представляет обновленный экземпляр списка контактных лиц и доверенных курьеров владельцу домена.

2.2.3 Этап 2: Создание запроса на сертификат

2.2.3.1 Запрос и получение сертификата производится на том же компьютере и с помощью того же веб-браузера.

2.2.3.2 Для создания запроса на сертификат:

a) Организация переходит на веб-интерфейс пользователя для запроса сертификата с помощью универсального указателя ресурса URL <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> и вводит ~~имя пользователя «sbca/CEF_eDelivery.europa.eu» и пароль «digit.333»~~ **идентификационные данные (имя пользователя/пароль), полученные от системы ИОК Сертификационного органа для пользовательского портала.**

b) Организация выбирает позицию «request» («Запрос») в левой части панели, а затем позицию «CEF_TACHOnet» в выпадающем списке.

c) Для завершения процесса Организация вносит в форму запроса на сертификат информацию, указанную в таблице 3, и нажимает на кнопку «Next (soft-PSE)».

Таблица 3

Подробные сведения о полях, подлежащих заполнению

Поле, подлежащее заполнению	Описание
Страна	C = код страны , местоположение владельца сертификата, проверенное по открытой директории; Ограничения: 2 знака в соответствии с ISO 3166-1, alpha-2, с учетом регистра; примеры: DE, BE, NL Отдельные случаи: UK (для Великобритании), EL (для Греции)
Организация/Компания (O)	O = название организации владельца сертификата
Главный домен (OU1)	OU=CEF_eDelivery.europa.eu
Область ответственности (OU2)	OU=CEF_TACHOnet
Департамент (OU3)	Обязательное значение согласно «ОБЛАСТИ ОТВЕТСТВЕННОСТИ» При запросе сертификата содержание необходимо проверить по списку допущенных значений («белый список»). Если информация не соответствует списку, то запрос не проходит.

Поле, подлежащее заполнению	Описание
	<p>Формат: OU=<TYPE>-<GTC_NUMBER>,</p> <p>где «<TYPE>» заменяется на AP_PROD: точка доступа в эксплуатационной среде, <GTC_NUMBER> соответствует GTC_OID-1.3.130.0.2018.xxxxxx, а «Ares(2018)xxxxxx» — это номер GTC для проекта «TAXOnet».</p> <p>Например: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx</p>
Имя (CN)	Поле должно быть пустым.
Фамилия (CN)	<p>Значение в этом поле начинается с «GRP:», за которым следует общее имя (common name).</p> <p>Формат: CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER></p> <p>Например: GRP:CEF_TACHOnet_AP_PROD_BE_001</p>
Эл. почта	E=CEf-EDELIVERY-SUPPORT@ec.europa.eu
Эл. почта 1 (SAN)	Поле должно быть пустым.
Эл. почта 2 (SAN)	Поле должно быть пустым.
Эл. почта 3 (SAN)	Поле должно быть пустым.
Адрес	Поле должно быть пустым.
Улица	Должен быть указан официальный адрес организации владельца сертификата (используется для доверенности)
Номер дома	Должен быть указан официальный адрес организации владельца сертификата (используется для доверенности)
Почтовый индекс	<p>Должен быть указан официальный адрес организации владельца сертификата (используется для доверенности)</p> <p>Внимание: если почтовый индекс НЕ является 5-значным, оставить поле «Почтовый индекс» пустым и указать почтовый индекс в поле «Город».</p>
Город	<p>Должен быть указан официальный адрес организации владельца сертификата (используется для доверенности)</p> <p>Внимание: если почтовый индекс НЕ является 5-значным, оставить поле «Почтовый индекс» пустым и указать почтовый индекс в поле «Город».</p>
Номер телефона	Поле должно быть пустым.
Идентификационные данные	Адрес электронной почты должен совпадать с адресом, используемым при регистрации уникального идентификатора.

Поле, подлежащее заполнению	Описание
	+ Должно быть указано имя лица, представляющего организацию (используется для доверенности) + № в реестре коммерческих организаций (обязательно указывать только для частных организаций) Зарегистрировано в местном суде (требуется только для частных организаций в Германии и Австрии)
Пароль отзыва	Обязательное поле, значение выбирается стороной, запрашивающей сертификат
Пароль отзыва (повторный ввод)	Обязательное поле, значение повторно вводится стороной, запрашивающей сертификат

d) Выбранная длина ключа — 2048 бит (высший уровень).

e) Организация отмечает ссылочный номер для получения сертификата.

f) Служба поддержки ФОЕ проверяет новые запросы на сертификаты и действительность информации, внесенной в запрос на сертификат.

g) Служба поддержки ФОЕ проверяет правильность формата информации, указанной в запросе.

h) Если одна из проверок в пункте 5 или 6 выше не пройдена успешно, Служба поддержки ФОЕ отправляет на адрес электронной почты, указанный в «Идентификационных данных» формы запроса, электронное письмо с владельцем домена в копии, в котором организации предлагается начать процесс заново. Непринятый запрос на сертификат аннулируется.

i) Служба поддержки ФОЕ направляет ~~Регистрационному органу~~ **Органу проверки запросов** электронное письмо относительно действительности запроса. Электронное письмо содержит:

1) название организации, указанное в поле «Организация (O)» запроса на сертификат;

2) данные сертификата, включая имя точки доступа, для которой должен быть выдан сертификат, указанное в поле «Фамилия (CN)» запроса на сертификат;

3) ссылочный номер сертификата;

4) адрес организации, адрес ее электронной почты и имя представляющего ее лица.

2.2.4 Этап 3: Проверка в **Органе проверки запросов** ~~Регистрационном органе~~ (~~Утверждение сертификата~~ **Проверка запроса на сертификат**)

2.2.4.1 Доверенный курьер или контактное лицо назначает встречу с **Органом проверки запросов** ~~Регистрационным органом~~ посредством обмена электронными сообщениями, и сообщает идентификационные данные доверенного курьера, который прибудет на личную встречу.

2.2.4.2 Организация готовит пакет документов, включающий:

a) заполненную и подписанную доверенность;

b) копию действительного паспорта доверенного курьера, который прибудет на личную встречу; ~~Эта копия должна быть подписана одним из контактных лиц организации, идентифицированных на этапе 1;~~

c) бумажный экземпляр запроса на сертификат, подписанный одним из контактных лиц организации.

2.2.4.3 ~~Регистрационный орган~~ **Орган проверки запросов** принимает доверенного курьера после установления его личности по прибытии в здание. ~~Регистрационный орган~~ **Орган проверки запросов** производит очную регистрацию запроса на сертификат, в целях которой он:

- a) производит идентификацию и аутентификацию доверенного курьера;
- b) сравнивает внешность доверенного курьера с предъявленным им паспортом;
- c) проверяет действительность паспорта, предъявленного доверенным курьером;
- d) сверяет проверенный паспорт, предъявленный доверенным курьером, с копией действительного паспорта доверенного курьера, ~~подписанного одним из идентифицированных контактных лиц организации. Подпись проверяется посредством сверки с оригиналом «идентификационной формы доверенного курьера и контактных лиц»;~~
- e) проверяет заполненную и подписанную доверенность;
- f) проверяет бумажный экземпляр запроса на сертификат ~~и сравнивает предоставленную в нем подпись с оригиналом «идентификационной формы доверенного курьера и контактных лиц»;~~
- g) связывается по телефону с контактным лицом подписывающей стороны, чтобы еще раз проверить личность доверенного курьера и содержания запроса на сертификат.

2.2.4.4 ~~Регистрационный орган~~ **Орган проверки запросов** подтверждает Службе поддержки ФОЕ, что национальный орган действительно уполномочен осуществлять эксплуатацию компонентов, для которых он запрашивает сертификаты, и что соответствующий процесс очной регистрации прошел успешно. Подтверждение отправляется по электронной почте сообщением, защищенным сертификатом «CommiSign», к которому прилагается отсканированная копия проверенных документов, которые были предъявлены во время очной встречи, и подписанного проверочного списка для этапов процесса, выполненных ~~Регистрационным органом~~ **Органом проверки запросов**.

2.2.4.5 Если ~~Регистрационный орган~~ **Орган проверки запросов** подтверждает действительность запроса, то процесс продолжается в соответствии с положениями пунктов 2.2.4.6 и 2.2.4.7. В противном случае в выдаче сертификата будет отказано, о чем будет проинформирована организация.

2.2.4.6 Служба поддержки ФОЕ утверждает запрос на сертификат и уведомляет ~~Регистрационный орган~~ **Орган проверки запросов** об утверждении запроса.

2.2.4.7 **Служба поддержки ФОЕ** ~~Регистрационный орган~~ уведомляет организацию о том, что сертификат можно получить через **систему ИОК Сертификационного органа** (пользовательский портал).

2.2.5 Этап 4: Создание сертификата

Сертификат создается после утверждения запроса на его выдачу.

2.2.6 Этап 5: Публикация и получение сертификата

2.2.6.1 После утверждения запроса на сертификат **Служба поддержки ФОЕ** уведомляет **Орган проверки запросов** об утверждении сертификата и сообщает организации, что сертификат может быть получен. ~~Регистрационный орган~~ **получает сертификат и передает копию доверенному курьеру.**

2.2.6.2 Организация получает уведомление Регистрационного органа о том, что сертификаты могут быть получены.

2.2.6.23 Организация переходит на пользовательский портал по адресу <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> и входит в систему с помощью идентификационных данных (имя пользователя/пароль), полученных

от системы ИОК Сертификационного органа для пользовательского портала — под именем пользователя «sbea/CEF_eDelivery.europa.eu» и паролем «digit.333».

2.2.6.34 Организация нажимает на кнопку «fetch» («Получить») в левой части экрана и указывает ссылочный номер, отмеченный в процессе оформления запроса на сертификат.

2.2.6.45 Организация устанавливает сертификаты, нажав на кнопку «install» («Установить»).

2.2.6.56 Сертификат устанавливается в точке доступа. Поскольку установка зависит от конкретной реализации, организации следует обратиться к своему поставщику точки доступа, чтобы получить описание этого процесса.

2.2.6.67 Для установки сертификата в точке доступа необходимо выполнить следующие шаги:

- a) экспортировать закрытый ключ и сертификат,
- b) создать хранилище ключей и хранилище доверенных сертификатов,
- c) установить хранилище ключей и хранилище доверенных сертификатов в точке доступа.

3. Процедура отзыва сертификата

3.1 Организация представляет запрос на отзыв через **систему ИОК Сертификационного органа** (пользовательский портал).

3.2 Отзыв сертификата производится Службой поддержки ФОЕ.

4. Общие положения и условия, касающиеся службы ИОК ФОЕ

4.1 Справочная информация

В качестве поставщика решения «eDelivery», которое является одним из компонентов механизма финансирования «Фонд объединения Европы», ДИГИТ предоставляет в распоряжение Договаривающихся сторон ЕСТР службу ИОК⁷ («служба ИОК ФОЕ»). Служба ИОК ФОЕ используется национальными органами («конечными пользователями»), являющимися участниками системы **электронного обмена информацией о карточках водителя «ТАХОНет»**.

ДИГИТ является клиентом ИОК решения TeleSec Shared-Business-CA («SBCA»), эксплуатацию которого осуществляет доверенный центр группы **«Дойче телеком секьюрити, ГмбХ» «Т-Системз Интернэшнл ГмбХ» («Т-Системз»⁸)**. ДИГИТ играет роль ведущего регистратора домена «CEF_eDelivery.europa.eu» SBCA. В этом качестве ДИГИТ в рамках домена «CEF_eDelivery.europa.eu» создает поддомены для каждого проекта, использующего службу ИОК ФОЕ.

В настоящем документе представлена подробная информация об условиях использования поддомена **системы электронного обмена информацией о карточках водителя «ТАХОНет»**. ДИГИТ выполняет функцию субрегистратора этого поддомена. В этом качестве он выдает, отзывает и обновляет сертификаты для данного проекта.

4.2 Оговорка об ограничении ответственности

Европейская комиссия не несет никакой ответственности или обязательств в отношении содержания сертификата, которые возлагаются исключительно на его

⁷ ИОК (инфраструктура открытых ключей) — это набор ролей, правил, процедур и систем, необходимых для создания, распространения и отзыва цифровых сертификатов и управления ими.

⁸ Доверенная роль оператора доверенного центра, базирующегося в доверенном центре **«Дойче телеком секьюрити, ГмбХ2 «Т-Системз»**, состоит также в выполнении функций внутреннего регистрационного органа органа проверки запросов.

владельца. Ответственность за проверку точности содержания сертификата несет его владелец.

Европейская комиссия не несет никакой ответственности или обязательств в отношении использования сертификата его владельцем, являющимся сторонним юридическим лицом вне Европейской комиссии.

Данная оговорка не имеет целью ограничить ответственность Европейской комиссии в случае нарушения любых требований, установленных применимым законодательством, или исключить ее ответственность в тех случаях, когда она не может быть исключена в соответствии с этим законодательством.

4.3 Разрешенные/запрещенные виды использования сертификатов

4.3.1 Разрешенные виды использования сертификатов

После выдачи сертификата владелец⁹ сертификата использует его только в рамках системы **электронного обмена информацией о карточках водителя «TAXOnet»**. В этом контексте сертификат может использоваться для:

аутентификации происхождения данных;

кодирования данных;

надежного выявления случаев нарушения целостности данных.

4.3.2 Запрещенные виды использования сертификатов

Любое использование сертификата, не разрешенное в явном виде в качестве одного из вариантов разрешенного использования, запрещено.

4.4 Дополнительные обязанности владельца сертификата

Подробные положения и условия для SBCA определены «**Дойче телеком секьюрити, ГмбХ**» «Т-Системз» в политике сертификации (ПС) и регламенте сертификационной практики (PCП) службы SBCA¹⁰. В настоящий документ включены спецификации и рекомендации по безопасности, касающиеся технических и организационных аспектов, и описывается деятельность оператора доверенного центра, выполняющего роли сертификационного органа (CO) и регистрационного органа (PO) **органа проверки запросов**, а также делегированной третьей стороны ~~регистрационного органа (PO) органа проверки запросов~~.

Запросить сертификат могут только субъекты, уполномоченные участвовать в системе **электронного обмена информацией о карточках водителя «TAXOnet»**.

Что касается принятия сертификата, то применяется пункт 4.4.1 политики сертификации и регламента сертификационной практики (ПС/PCП) службы SBCA; кроме того, условия использования и положения, представленные в настоящем документе, считаются принятыми организацией, которой выдан сертификат («O»), при его первом использовании.

Что касается публикации сертификата, то применяются положения пункта 2.2 ПС/PCП службы SBCA.

Все владельцы сертификатов соблюдают следующие требования:

- 1) они обеспечивают защиту своего закрытого ключа от несанкционированного использования;
- 2) они воздерживаются от передачи или раскрытия закрытого ключа третьим сторонам, даже если последние действуют в качестве их представителей;
- 3) они воздерживаются от дальнейшего использования закрытого ключа по истечении срока действия или отзыва сертификата, помимо просмотра

⁹ Идентифицируется значением атрибута «O» в уникальном имени субъекта выданного сертификата.

¹⁰ Актуальную версию ПС/PCП службы SBCA «**Дойче телеком секьюрити, ГмбХ**» «Т-Системз» см. по адресу <https://www.telesec.de/en/sbca-en/support/download-area/>.

зашифрованных данных (например, для расшифровки сообщений электронной почты);

4) владелец сертификата отвечает за копирование или перенаправление ключа конечному субъекту или субъектам;

5) владелец сертификата должен обязать конечного субъекта/всех конечных субъектов соблюдать настоящие условия и положения, включая ПС/РСП службы SBCA, при работе с закрытым ключом;

6) владелец сертификата должен предоставить идентификационные данные тех уполномоченных представителей, которым разрешается запрашивать отзыв сертификатов, выданных организации, с подробным описанием событий, которые обусловили необходимость отзыва, и пароль отзыва;

7) для сертификатов, связанных с группами лиц и функциями и/или юридическими лицами, после выхода лица из группы конечных субъектов (например, прекращение трудовых отношений) владелец сертификата должен предотвращать неправомерное использование закрытого ключа путем отзыва сертификата;

8) владелец сертификата несет ответственность и должен потребовать отзыва сертификата при обстоятельствах, указанных в пункте 4.9.1 ПС/РСП службы SBCA;

- в случае обновления или повторного создания ключей для сертификатов применяется пункт 4.6 или 4.7 ПС/РСП службы SBCA;
- в случае внесения изменений в сертификат применяется пункт 4.8 ПС/РСП службы SBCA;
- в случае отзыва сертификата применяется пункт 4.9 ПС/РСП службы SBCA.

5. Идентификационная форма контактных лиц и доверенных курьеров (идентификационная форма ЕГСО — образец)

Я, нижеподписавшийся(ая), *[имя и адрес представителя организации]*, удостоверяю, что нижеследующая информация будет использоваться в связи запросом, созданием и получением цифровых сертификатов открытого ключа для точек доступа «ТАХОнет» в порядке обеспечения конфиденциальности, целостности и неотречаемости сообщений «ТАХОнет»:

Данные контактных лиц:

— Контактное лицо № 1	— Контактное лицо № 2
— Фамилия:	— Фамилия:
— Имя:	— Имя:
— Мобильный телефон:	— Мобильный телефон:
— Телефон:	— Телефон:
— Эл. почта:	— Эл. почта:
— Образец собственноручной подписи: —	— Образец собственноручной подписи: — — —

Данные доверенных курьеров:

— Доверенный курьер № 1	— Доверенный курьер № 2
— Фамилия:	— Фамилия:
— Имя:	— Имя:
— Мобильный телефон:	— Мобильный телефон:
— Эл. почта:	— Эл. почта:
— Страна выдачи паспорта:	— Страна выдачи паспорта:
— Номер паспорта:	— Номер паспорта:
— Дата истечения срока действия паспорта:	— Дата истечения срока действия паспорта:

Компетентное министерство Договаривающейся стороны ЕСТР

в лице:

* настоящим удостоверяет, что данная форма заявки на представление политики компетентного органа Договаривающейся стороны компетентным органом этой Договаривающейся стороны является подлинной, а приложения к ней являются действительными;

* настоящим разъясняет, что назначенный и утвержденный компетентный орган Договаривающейся стороны будет осуществлять свою деятельность в рамках

добавления 1В к ЕСТР и документа «Политика Европейского главного сертификационного центра для системы цифровых тахографов» («Политика ЕГСО»),

и/или

добавления 1С к ЕСТР и документа «Умный тахограф — Политика Европейского корневого центра сертификации и политика инфраструктуры симметричных ключей» («Политика ЕГСО второго поколения»),

и/или

добавления 4 к ЕСТР и политики сертификации (ПС) и регламента сертификационной практики (РСП) TeleSec Shared-Business-CA (политика ИОК для системы электронного обмена информацией о карточках водителя «ТАХОнет»).

1. Идентификационные данные компетентного органа Договаривающейся стороны¹¹

- a. **Официальное название организационной структуры:**
- b. **Адрес организационной структуры:**
- c. **Имя должным образом назначенного представителя организационной структуры:**
- d. **Контактное лицо (если отличается от указанного в пункте с.¹²):**
- e. **Адрес электронной почты:**
- f. **Почтовый адрес:**
- g. **Номер(а) телефона(ов) и/или факса:**

2. Идентификационные данные доверенного курьера (лица, передающего запросы на сертификаты/ключи безопасности ЕГСО и/или запросы на сертификаты для системы «ТАХОнет»-электронного обмена информацией о карточках водителя, и получающего ключи безопасности от ЕГСО¹³):

- a. **Имя:**
- b. **Почтовый адрес:**
- c. **Номер телефона и/или факса:**

3. Подтверждение согласия и подпись

Настоящим я подтверждаю свое согласие с вышеуказанным, подписывая данную форму заявления и ознакомившись

с добавлением 1В к ЕСТР и политикой ЕГСО,

и/или

с добавлением 1С к ЕСТР и политикой ЕГСО второго поколения,

и/или

¹¹ Просьба ОБРАТИТЬ ВНИМАНИЕ, что об изменениях в данных необходимо сообщать непосредственно в ЕГСО.

¹² ПРИЛОЖИТЬ письмо лица, указанного в пункте 1.с, с распоряжениями для лица, указанного в пункте 1.d., включая копию пропуска лица, указанного в пункте d., в здание организации, которая назначена в качестве компетентного органа Договаривающейся стороны.

¹³ ПРИЛОЖИТЬ письмо о назначении лица, указанного в пункте 1.d., в качестве лица, указанного в пункте 2, и копию документа, удостоверяющего его/ее личность; эти данные будут включены в документы на хранении ЕГСО.

добавлением 4 к ЕСТР и политикой ИОК для системы «ТАХОнет» электронного обмена информацией о карточках водителя.

Я также признаю, что ЕГСО аннулирует заявки при наличии свидетельств того, что

- формы или приложения к ним были выданы на основании неточной или ложной информации;
- содержащаяся в них информация устарела.

Настоящим я подтверждаю, что информация, указанная в данной форме заявления и приложениях к нему и предоставленная в адрес ЕГСО, является правильной, точной и полной.

На обработку данных, указанных в этой форме, распространяется декларация конфиденциальности, регулирующая защиту персональных данных. С этой декларацией можно ознакомиться на интернет-сайте ЕС по адресу: <https://ec.europa.eu/dpo-register/detail/DPR-EC-00406>. Просьба ознакомиться с этой декларацией до заполнения и отправки настоящей формы.

Место, дата, штамп или печать организации:

Подпись уполномоченного представителя:

6. Документы

6.1 Индивидуальная доверенность (образец)

Ниже представлен образец индивидуальной доверенности, которая должна быть подписана и предъявлена доверенным курьером в ходе очной регистрации в РЭ-Органе проверки запросов.

*Please print the text of this document on your letterhead, add your company stamp and have it signed by the administrative contact or admin-c of the domain.
The power of attorney must be signed by an authorized representative of the organization (principal).*

The Shared-Business-CA customer will then submit this document together with the order document to the T-Systems International GmbH Trust Center.

Individual power of attorney / Power of attorney granted to one person

I, *[name and address of the end-user]*, empower as an authorized person of this organization *

[name of the company receiving the certificate]

(e. g. sample company, sample authority, to be registered in the O-field of the certificate *)

following company and/or person:

Company: **European Commission**
Address: **DG DIGIT, 28 rue Belliard, 1000 Brussels**
Represented by Mr/Mrs/Ms: **Adrien FERIAL**

On my behalf, by complying with all and any regulations and formalities (particularly Certificate Policy (CP) / Certification Practice Statement (CPS)), for authorisation to manage (i.e. issue, revoke, renew) X.509v3-certificates, including the complete key-material, issued by the certification authority „TeleSec Shared-Business-CA“, in respect of the domain as above mentioned.

This power of attorney relates to issuing and management of the following certificate types (the applicable type has to be marked):

- user¹: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client
- server²: e.g. identity of web server, TLS/SSL client server authentication
Please enter additionally the country, organization, locality, state or province name of the server:

- eMail-Gateway³: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

- The power of attorney is valid until further notice, but up to a **maximum of 27 months**² or **maximum of 36 months**^{1,3} from date of issuance.
- The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month**² months or **maximum of 36 months**^{1,3} from date of issuance.

Please note that a time limit on the power of attorney can cause that a request for certificate order, renewal or revocation may not be possible because the validity period of the authorization has been exceeded!

Place, date, company stamp or seal of the organisation (principal)

Signature of the authorized representative

6.2 Бумажный бланк запроса на сертификат (образец)

Ниже приведен образец бумажного бланка запроса на сертификат, который должен быть подписан и предъявлен доверенным курьером в ходе очной регистрации в РӨ-Органе проверки запросов.

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

Please reproduce the certificate data information provided by CEF Support Team acknowledging the completeness of the electronic certificate request, e.g.:

Certificate data	
Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OiD-1.3.130.0.2018.xxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu

Insert reference number (e.g. 776002)

please fill in

Trusted courier #1
Name:
First names:
Mobile phone:
Email:
Passport issuing country:
Passport number:
Passport validity end date:

7. Глоссарий

Основные термины, используемые в разделах настоящего добавления, определены в разделе «Определения ФОЕ» на едином цифровом веб-портале ФОЕ (CEF Digital):

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions>.

Основные сокращения, используемые в настоящем описании предложения компонента, раскрыты в глоссарии ФОЕ на едином цифровом веб-портале ФОЕ (CEF Digital):

<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?spaceKey=CEFDIGITAL&title=CEF+Glossary>.

7.2 Услуги, указанные в разделе 4.1 настоящего добавления, предоставляются центральным концентратором бесплатно.

8. Привлечение субподрядчиков

8.1 Стороны могут передавать на подряд любые из услуг, за которые они несут ответственность на основании настоящего добавления.

8.2 Привлечение субподрядчиков не освобождает сторону от ответственности на основании настоящего добавления, включая ответственность за обеспечение надлежащего уровня обслуживания в соответствии с разделом 4.6 настоящего добавления.
