Экономический и Социальный Совет

Distr.: General
12 December 2019
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 третья сессия
Женева, 24 февраля 2020 года
Пункт 4 предварительной повестки дня
Система «ТАХОнет»

Пересмотренное новое добавление к Европейскому соглашению, касающемуся работы экипажей транспортных средств, производящих международные автомобильные перевозки (ЕСТР)

Добавление 4

Технические требования к системе «ТАХОнет»* **

Представлено Австрией

Настоящий документ, первоначально представленный Австрией в качестве страны, председательствующей в Европейском союзе, содержит проект текста возможного нового приложения к Соглашению ЕСТР, касающегося системы «ТАХОнет». Он был пересмотрен с целью отразить изменения, предложенные на двадцать второй сессии.

* Настоящий документ воспроизводится в том виде, в каком он был представлен.

** Изменения к настоящему документу выделены перечеркнутым шрифтом в случае исключенного текста и жирным шрифтом в случае нового текста.

Новое добавление к ЕСТР

Добавление 4

Технические требования к системе «TAXOнет»

1. Область применения и цель

1.1 В настоящем добавлении излагаются положения и условия, касающиеся подключения Договаривающихся сторон ЕСТР к системе «TAXOнет» по линии службы «eDelivery».

1.2 Договаривающиеся стороны, которые подключаются к системе «TAXOнет» по линии системы «eDelivery», соблюдают положения, изложенные в настоящем добавлении.

2. Определения

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

b) «eDelivery» означает службу, которая дает возможность передавать соответствующие данные с помощью электронных средств между третьими сторонами, предоставляющими доказательства, имеющие отношение к переданным данным, в том числе доказательства факта направления и получения этих данных и их защиты от риска несанкционированного изменения;

c) «TAXOнет» означает систему электронного обмена информацией о карточках водителей между Договаривающимися сторонами, установленную Европейской комиссией;

d) «центральный концентратор» означает информационную систему, дающую возможность маршрутизации сообщений между запрашивающей стороной и стороной-респондентом;

e) «запрашивающая сторона» означает Договаривающую сторону, направляющую запрос «TAXOнет» или соответствующее уведомление, которое затем направляется соответствующей стороне-респонденту через центральный концентратор;

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

g) «орган выдачи карточки» или «ОВК» означает субъект, уполномоченный выдавать карточки тахографа и регулировать их использование~~.~~**;**

h)' «субъект данных» означает физическое лицо, данные которого являются предметом обмена данными по сети «TAXOнет»;

h) «личные данные» означают любую информацию, обмен которой осуществляется по сети «TAXOнет» и которая позволяет идентифицировать субъект данных, например имя или идентификационный номер;

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

j) «автоматическая обработка» включает следующие операции, если она осуществляется в целом или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, стирание, извлечение или распространение.

3. Общие обязанности

3.1 Никакая Договаривающаяся сторона не может заключать соглашения о предоставлении доступа к системе «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 посредство «ТАХОнет» таким образом и на таком уровне услуг, которые предусмотрены в подразделе добавления 4.6.

3.3 Договаривающиеся стороны незамедлительно уведомляют друг друга в том случае, если они замечают сбои в работе или ошибки в части их ответственности, которые могут поставить под угрозу нормальное функционирование «ТАХОнет».

3.4 Каждая сторона указывает данные о контактных лицах по «ТАХОнет» секретариату ЕСТР. Любое изменение, касающееся контактных лиц, должно быть доведено до сведения секретариата ЕСТР в письменном виде.

4. Испытания на подключение к «ТАХОнет»

4.1 Подключение той или иной Договаривающейся стороны к «ТАХОнет» производится после успешного завершения процедуры подключения, интеграции и проверки эксплуатационных характеристик в соответствии с действующими инструкциями и под надзором Европейской комиссии.

4.2 В случае неспособности пройти предварительные испытания Европейская комиссия может временно отложить этап испытаний. Испытание возобновляют, после того как данная Договаривающаяся сторона сообщит Европейской комиссии о внесении необходимых технических улучшений на национальном уровне, позволяющих обеспечить успешное проведение испытаний на эксплуатационные характеристики.

4.3 Максимальная продолжительность предварительных испытаний составляет шесть месяцев.

5. Доверительная архитектура

5.1 Конфиденциальность, целостность и отказоустойчивость сообщений «ТАХОнет» обеспечиваются за счет доверительной архитектуры системы «ТАХОнет».

5.2 Доверительная архитектура «ТАХОнет» строится на основе соответствующих положений службы инфраструктуры сертификации открытых ключей (ПКИ), учрежденной Европейской комиссией, требования которой изложены в подразделах добавления 4.8 и 4.9.

5.3 В работе доверительной архитектуры «ТАХОнет» принимают участие следующие субъекты:

a) Сертификационный орган, который отвечает за создание цифровых сертификатов, которые выдаются Регистрационным органом национальным компетентным органам Договаривающихся сторон

(через посредство доверенных стран, которые назначены ими), а также за создание соответствующей технической инфраструктуры, отвечающей за выдачу, аннулирование и возобновление цифровых сертификатов;

b) владелец домена, отвечающий за работу центрального концентратора, указанного в подразделе добавления 4.1, и легализацию и координацию доверительной инфраструктуры «ТАХОнет»;

c) регистрационный орган, отвечающий за регистрацию и утверждение запросов на выдачу, отмену и возобновление цифровых сертификатов и за проверку идентичности доверенных стран;

d) доверенный курьер – лицо, назначенное национальным органом, отвечающим за передачу открытых ключей Регистрационному органу и получение соответствующего сертификата, создаваемого Сертификационным органом;

e) национальный орган от 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 назначаются Европейской комиссией.

5.5 Любая Договаривающаяся сторона, которая подключается к системе «ТАХОнет», должна направить запрос на выдачу цифрового сертификата в соответствии с подразделом 4.9 добавления в целях подписания и шифрования соответствующего сообщения «ТАХОнет».

5.6 Соответствующее свидетельство может быть отозвано в соответствии с подразделом добавления 4.9.

6. Защита и конфиденциальность данных

6.1 Стороны принимают в соответствии с законодательными актами, регламентирующими защиту данных на международном и национальном уровнях, и в частности с Конвенцией о защите физических лиц при автоматизированной обработке персональных данных, все необходимые технические и организационные меры с целью гарантировать безопасность данных «ТАХОнет» и предотвращать изменение, утрату или несанкционированную обработку этих данных или доступ к таким данным (в частности, их аутентичность, конфиденциальность, отслеживаемость, целостность, доступность и отказоустойчивость и безопасность сообщений).

~~6.2 Каждая сторона обеспечивает защиту своих собственных национальных систем от неправомерного использования, внедрения злонамеренных кодов, вирусов, взлома компьютеров, нарушений и незаконной фальсификации данных и от других сопоставимых действий третьих сторон. Стороны соглашаются прилагать разумные с коммерческой точки зрения усилия во избежание передачи каких либо вирусов, вредоносных программ с таймером времени, вирусных программ самотиражирования или аналогичных элементов или любых иных приемов программирования, которые могут вызвать сбой в работе компьютерных систем другой стороны.~~

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

6.3 **Стороны дают субъекту данных, персональные данные которого были получены по сети «ТАХОнет», возможность:**

a) получить подтверждение по поводу того, хранятся ли персональные данные, относящиеся к указанному субъекту данных, в соответствующем файле данных, а также направить ему сообщение о таких данных в краткой, прозрачной, понятной и легкодоступной форме;

b) обеспечить в случае необходимости исправление неточных персональных данных без неоправданных задержек;

c) обеспечить в случае необходимости удаление персональных данных, если они этой стороне больше не нужны 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»);

d) возразить в любое время по причинам, связанным с его или ее конкретной ситуацией, против обработки персональных данных, которые касаются его или ее, какой-либо стороной.

6.4 **В случае необходимости автоматической обработки персональных данных, полученных по сети «ТАХОнет», она производится в соответствии с Конвенцией.**

6.5 **Стороны идентифицируют любые персональные данные, переданные запрашивающей стороне по сети «ТАХОнет», и предоставляют общую информацию, например такую, которая содержится на соответствующем веб-сайте, по поводу мер предосторожности, применимых к передаче другим сторонам.**

6.6 **Сторона-респондент передает персональные данные по сети «ТАХОнет» только с законной и конкретной целью, каковой является оказание помощи запрашивающей стороне в выполнении настоящего Соглашения. Запрашивающая сторона не производит дальнейшую обработку персональных данных, которая несовместима с этими целями.**

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

6.8 **Запрашивающая сторона, получающая персональные данные по сети «ТАХОнет», передает персональные данные третьей стороне только в том случае, если эта третья сторона является национальным органом, управомоченным проверять или обеспечивать соблюдение продолжительности работы и отдыха в соответствии с настоящим Соглашением.**

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

7. Расходы

7.1 Договаривающиеся стороны несут расходы, связанные с собственными разработками и с использованием своих систем данных и процедур, которые необходимы для соблюдения обязательств на основании настоящего добавления.

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

8. Передача работы на субподряд

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

8.2 Передача такой работы на субподряд не освобождает данную сторону от ответственности на основании настоящего добавления, в том числе от ответственности за надлежащий уровень услуг в соответствии с подразделом добавления 4.6.

Подраздел добавления 4.1
Общие аспекты «ТАХОнет»

1. Общее описание

«ТАХОнет» – электронная система обмена информацией о карточках водителя. Она осуществляет маршрутизацию запросов «ТАХОнет» на представление информации из запрашивающей стороны стороне-респонденту, а также ответов из стороны-респондента запрашивающей стороне. Договаривающиеся стороны, которые являются участниками системы «ТАХОнет», должны подключить к этой системе свои национальные регистры, содержащие карточки водителей.

2. Архитектура

Система сообщений «ТАХОнет» состоит из следующих компонентов:

2.1 Центральный концентратор, который получает запрос из запрашивающей стороны, подтверждает его получение и обрабатывает его в целях препровождения ответа запрашивающим сторонам. Центральный концентратор ждет ответ каждой стороны-респондента, сводит эти ответы воедино и направляет сводный ответ запрашивающей стороне.

2.2 Национальные системы сторон, которые оснащены соответствующим интерфейсом, способны как направлять ответы на центральный концентратор, так и получать предназначенные им ответы. Национальные системы могут использовать собственное или коммерческое программное обеспечение для передачи или получения сообщений на центральный концентратор и из него.

3. Управление

3.1 Центральный концентратор находится в ведении Европейской комиссии, которая несет ответственность за техническую работу и эксплуатационно-техническое обслуживание центрального концентратора.

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

3.3 Центральный концентратор не предоставляет доступ к персональным данным, за исключением данных об уполномоченных сотрудниках Европейской комиссии, если это необходимо в целях мониторинга, эксплуатационно-технического обслуживания и выявления неисправностей.

3.4 Каждая Договаривающаяся сторона несет ответственность за:

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

3.4.2 установку и эксплуатационно-техническое обслуживание своей национальной системы, включая аппаратное оборудование и программное обеспечение, будь то собственное или коммерческое;

3.4.3 правильную эксплуатационную совместимость своей 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 национальной системы в соответствии с уровнем обслуживания, определенным в подразделе добавления 4.6.

Подраздел добавления 4.2
Функциональные возможности «ТАХОнет»

1. Система сообщений «ТАХОнет» обеспечивает следующие функциональные возможности:

1.1 функция «проверки выданных карточек» (Check Issued Cards) (CIC): дает возможность запрашивающей стороне направлять запрос на проверку выданных карточек одной или всем запрашивающим сторонам в целях выяснения, имеет ли уже предъявитель карточки соответствующую карточку водителя, выданную ему сторонами-респондентами. Стороны-респонденты отвечают на полученный запрос посредством направления соответствующего ответа в связи с проверкой выданных карточек (Check Issued Cards Response);

1.2 функция «проверки статуса карточки» (Check Card Status) (CCS): дает возможность запрашивающей стороне направлять запрос на предоставление подробных данных, касающихся той или иной карточки, выданной этой стороной, посредством направления этой стороной соответствующего запроса на проверку статуса выданной карточки (Check Card Status Request); сторона-респондент отвечает на полученный запрос посредством направления соответствующего ответа в связи с проверкой статуса карточек (Card Status Response);

1.3 функция «изменения статуса карточки» (Modify Card Status) (MCS): дает возможность запрашивающей стороне уведомлять сторону-респондента на основании запроса относительно изменения статуса карточки о том, что статус карточки, выданной этой стороной, 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 License) (ICDL): она дает возможность запрашивающей стороне уведомить сторону-респондента на основании запроса относительно выдачи карточки на основании водительского удостоверения 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 включаться другие сообщения, которые, как считается, позволят повысить эффективность работы системы «ТАХОнет», например уведомление об ошибках.

3. Национальные системы признают статус карточек, перечисленных в таблице 1, в случае использования любой из функций, описанных в пункте 1. Вместе с тем сторонам нет нужды осуществлять какую-либо процедуру, которая предполагала бы использование всех статусов, перечисленных выше.

4. Когда та или иная сторона получает ответ или уведомление с указанием статуса, который в ее административных процедурах не используется, национальная система придает статусу, указанному в сообщении, тот уровень, который соответствует ее административной процедуре. Сообщение не будет отклоняться страной-респондентом до тех пор, пока указанный статус сообщения значится в таблице 1.

5. Для того чтобы установить, действует ли карточка водителя для управления транспортным средством, статус карточки, указанный в таблице 1, не используется. В тех случаях, когда та или иная сторона просматривает регистр национального органа, выдающего карточки, используя функцию CCS, ответ будет содержать выделенное для этой цели поле «действительна для управления». Национальные административные процедуры должны быть такими, чтобы ответы CCS во всех случаях содержали позицию «действительна для управления».

Таблица 1
Статус карточек

Статус карточек	*Определение*
Заявка	ОВК получил заявку на выдачу карточки водителя. Эта информация регистрируется и хранится в базе данных с помощью созданных ключей 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.
Изъята	ОВК решил изъять карточку водителя. Карточка была аннулирована.
Возвращена	Карточка тахографа была возвращена в ОВК с указанием, что она более не нужна.
Потеряна	ОВК получил уведомление, что карточка тахографа потеряна.
Похищена	ОВК получил уведомление, что карточка тахографа похищена. Похищенная карточка считается утраченной.
Работает неисправно	ОВК получил уведомление, что карточка тахографа работает неисправно.
Срок действия истек	Срок действия карточки тахографа истек.

Статус карточек	*Определение*
Заменена	Карточка тахографа, которая, в соответствии с полученным сообщением, была потеряна, похищена или плохо работала, была заменена новой карточкой. Данные на новой карточке те же, за исключением индекса замены номера карточки, который был увеличен на единицу.
Возобновлена	Карточка тахографа была возобновлена в связи с изменением административных данных или истечением срока действия. Номер карточки на новой карточке остался тем же, за исключением индекса номера возобновления, который был увеличен на единицу.
В процессе замены	ОВК, который выдал карточку водителя, получил уведомление о начале процедуры замены этой карточки водителя на карточку водителя другой стороны, выданной ОВК.
Обменена	ОВК, который выдал карточку водителя, получил уведомление о завершении процедуры замены этой карточки водителя на карточку водителя другой стороны, выданной ОВК.

Подраздел добавления 4.3

Положения, регламентирующие обработку сообщений системой «ТАХОнет»

1. Общие технические требования

1.1 Центральный концентратор оснащен синхронными и асинхронными интерфейсами для обмена сообщениями. Стороны могут выбирать наиболее подходящую для них технологию, позволяющую им использовать свои собственные прикладные программы в целях взаимодействия с концентратором.

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

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

2. Структура XML-сообщений и определение схемы (XSD)

2.1 Общая структура XML-сообщений следует формату, определенному схемами XSD, установленными в центральном концентраторе.

2.2 Центральный концентратор и национальные системы передают и получают сообщения, которые соответствуют XSD-схеме.

2.3 Национальные системы способны направлять, получать и обрабатывать все сообщения, соответствующие любой из функциональных возможностей, указанных в подразделе добавления 4.2.

2.4 XML-сообщения должны включать по крайней мере минимальные требования, изложенные в таблице 2.

Таблица 2
Минимальные требования к содержанию XML-сообщений

Общий заголовок		*В обязательном порядке*
Версия	Официальная версия спецификаций XML уточняется с помощью пространства имен, определенного в XSD-сообщении и в атрибуте версии элемента заголовка любого XML-сообщения. Номер версии («n.m») определяется в качестве фиксированного значения в каждом выпуске файла «Определение схемы XML» (xsd).	Да
Идентификатор теста	Идентификатор теста – факультативный. Инициатор теста заполняет идентификаторы, и все участники документооборота отправляют/ возвращают тот же идентификатор. В процессе осуществления операций на него не следует обращать внимания, а в том случае, если он будет все же указан, его не следует использовать.	Нет
Технический идентификатор	Идентификатор UUID однозначно идентифицирует каждое индивидуальное сообщение. Отправитель создает соответствующий UUID и заполняет этот атрибут. Этот элемент данных ни в каком делопроизводстве не используется.	Да
Идентификатор рабочего процесса	UUID – идентификатор рабочего процесса, который должен создаваться запрашивающей стороной. Впоследствии этот идентификатор используется во всех сообщениях в целях корреляции рабочего процесса.	Да
Направлен	Дата и время (UTC), когда было направлено сообщение.	Да
Тайм-аут	Это – факультативный атрибут даты и времени (в формате UTC). Это значение будет устанавливаться центральным концентратором в случае переданных запросов. Этот атрибут указывает стороне-респонденту, когда истекает время ожидания. Это значение не требуется в случае «MS2TCN_<x>_Req» и всех ответных сообщений. Оно носит факультативный характер, вследствие чего можно использовать то же определение заголовка для всех типов сообщений независимо от того, требуется атрибут времени ожидания или нет.	Нет
С	Код «ISO 3166-1 Alpha 2» стороны, направляющей запрос, или «EU».	Да
до	Код «ISO 3166-1 Alpha 2» стороны, которой направляется запрос, или «EU».	Да

Подраздел добавления 4.4

Службы транслитерации и системы NYSIIS (Система идентификации и сбора и анализа данных штата Нью-Йорк)

1. Для кодирования фамилий всех водителей в национальном регистре используется алгоритм NYSIIS, заложенный в центральном концентраторе.

2. В процессе поиска той или иной карточки посредством функции CIC в качестве основного механизма поиска используются ключи NYSIIS.

3. В дополнение к этому для вывода на дисплей дополнительных результатов стороны могут использовать индивидуальный алгоритм.

4. Результаты поиска покажут механизм поиска, который использовался для обнаружения той или иной записи – NYSIIS или индивидуальный.

5. Если какая-либо сторона намерена зарегистрировать уведомления ICDL, то в этом случае ключи NYSIIS, содержащиеся в уведомлении, регистрируются в качестве данных ICDL. В процессе поиска данных ICDL сторона пользуется ключами NYSIIS, которые относятся к в фамилии заявителя.

Подраздел добавления 4.5

Требования к безопасности

1. Для обмена сообщениями между центральным концентратором и национальными системами используется протокол HTTPS.

2. Для целей безопасной передачи сообщений между национальными системами и центральным концентратором национальные системы пользуются цифровыми сертификатами, указанными в подразделах добавления 4.8 и 4.9.

3. Национальные системы применяют, как минимум, сертификаты, использующие подпись на основе хеш-алгоритма SHA-2 (SHA-256) и открытый 2048-битный ключ шифрования.

Подраздел добавления 4.6

Уровни обслуживания

1. Национальные системы обеспечивают нижеследующий минимальный уровень обслуживания:

1.1 Они доступны 24 часа в сутки, 7 дней в неделю.

1.2 Их доступность контролируется сообщением такта состояния, выдаваемого центральным концентратором.

1.3 Нормы их доступности составляют 98% в соответствии со следующей таблицей (цифры округлены до ближайшей значимой единицы):

	Нормы недоступности		
Доступность	ежесуточно	ежемесячно	ежегодно
98%	0,5 часа	15 часов	7,5 дня

Сторонам рекомендуется соблюдать нормы ежесуточной доступности, однако при этом признается, что некоторые необходимые виды деятельности, такие как эксплуатационно-техническое обслуживание, предполагает необходимость простоя продолжительностью более 30 минут. Вместе с тем ежемесячные и ежегодные нормы доступности являются обязательными.

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

1.5 Они должны отвечать на запросы не позже чем через 10 секунд.

1.6 Общая продолжительность тайм-аута (время, в течение которого запрашивающая сторона может ждать ответ) не должна превышать 20 секунд.

1.7 Они должны быть в состоянии соблюдать норму обслуживания на уровне шести сообщений в секунду.

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

1.9 Каждая национальная система должна быть в состоянии справляться с потенциальными техническими проблемами центрального концентратора или национальных систем в других сторонах. Это включает, в частности, следующие моменты:

a) потеря связи с центральным концентратором;

b) отсутствие реакции на запрос;

c) получение ответа после истечения предусмотренного времени ожидания ответа на сообщение;

d) получение посторонних сообщений;

e) получение недостоверных сообщений.

2. Центральный концентратор должен:

2.1 обеспечивать норму доступности на уровне 98%;

2.2 направлять национальным системам уведомление о любых ошибках либо с помощью ответа на сообщение, либо с помощью специального сообщения об ошибке. В свою очередь национальные системы должны получать эти специальные сообщения об ошибках и быть оснащены функцией разгрузки нарастания рабочего процесса, позволяющей принимать надлежащие меры по устранению указанных ошибок.

3. Эксплуатационно-техническое обслуживание

Стороны уведомляют другие стороны и Европейскую комиссию о любых плановых работах по эксплуатационно-техническому обслуживанию через посредство веб-приложения, как минимум, за неделю до начала этих работ, если это возможно с технической точки зрения.

Подраздел добавления 4.7

Система регистрации и статистика по данным, собранным в центральном концентраторе

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

2. Система регистрации информации должна позволять отслеживать все операции по мониторингу и отладке системы статистических данных, касающихся этих операций.

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

4. Статистические данные, используемые для целей 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.

Подраздел добавления 4.8

Общие положения, касающиеся цифровых ключей и сертификатов «ТАХОнет»

1. Генеральный директорат по информатике Европейской комиссии (ДИГИТ) оказывает услуги ПКИ[1] (именуемые «услуги СЕФ ПКИ») Договаривающимся сторонам ЕСТР, связанные с системой «ТАХОнет» (и как следствие, с национальными органами) через посредство службы «eDelivery».

2. Процедура запроса и отмены цифровых сертификатов, а также детальные положения и условия их использования определены в подразделе добавления 4.9.

3. Использование сертификатов:

3.1 После выдачи сертификата национальный орган использует данный сертификат только в контексте «ТАХОнет»[2]. Этот сертификат можно использовать в целях:

a) аутентификации происхождения данных;

b) кодирования данных;

c) надежного выявления случаев нарушения целостности данных.

3.2 Любое использование, которое однозначно не разрешается в качестве допустимого вида использования данного сертификата, запрещено.

4. Договаривающиеся стороны:

a) обеспечивают защиту своего закрытого ключа от несанкционированного использования;

b) воздерживаются от передачи или предания огласке закрытого ключа третьим сторонам, даже в качестве их представителей;

c) обеспечивают конфиденциальность, целостность и доступность закрытых ключей, которые созданы, хранятся и используются в системе «ТАХОнет»;

d) воздерживаются от дальнейшего использования закрытого ключа по истечении срока действия или аннулирования сертификата, помимо просмотра зашифрованных данных (например, для расшифровки сообщений электронной почты); ключи, срок действия которых истек, либо уничтожаются, либо сохраняются с помощью таких способов, которые предотвращают возможность их использования;

e) предоставляют Регистрационному органу идентификационные данные тех уполномоченных представителей, которым разрешается направлять требование в целях аннулирования сертификатов, выданных данной организации (требование в целях аннулирования включает пароль на данное требование и данные о событиях, которые обусловили необходимость отмены);

[1] ПКИ (Инфраструктура сертификации открытых ключей) представляет собой набор ролей, принципов, процедур и систем, необходимых для создания, управления, распределения и отмены цифровых сертификатов.

[2] Идентифицируется по значению атрибута «O=» в отличительном определении сути выданного сертификата.

f) предотвращают злоупотребление открытым ключом, направляя требование аннулировать соответствующий сертификат на открытый ключ в случае нарушения частного ключа или данных, позволяющих активировать частный ключ;

g) несут ответственность и соблюдают обязательство требовать аннулирования сертификата в обстоятельствах, предусмотренных принципами сертификации (ПС) и утвержденной практикой сертификации (УПС) Сертификационного органа;

h) незамедлительно уведомляют Регистрационный орган в случае потери, хищения или потенциального нарушения любых ключей ЕСТР, используемых в контексте «ТАХОнет».

5. Обязательства

Без ущерба для обязательств Европейской комиссии в случае нарушения любого требования, закрепленного в применимом национальном законе, или обязательства в вопросах, которые нельзя исключить на основании этого закона, Европейская комиссия не несет материальной или моральной ответственности 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.

Подраздел добавления 4.9

Описание услуг ПКИ для системы «ТАХОнет»

1. Введение

ПКИ (Инфраструктура сертификации открытых ключей) представляет собой набор ролей, принципов, процедур и систем, необходимых для создания, управления, распределения и отмены цифровых сертификатов[3]. Система услуг СЕФ ПКИ службы «eDelivery» дает возможность выдачи и организации цифровых сертификатов, используемых в целях обеспечения конфиденциальности, целостности и отказоустойчивости информации, которой обмениваются пункты доступа (ПД).

Система услуг ПКИ службы «eDelivery» строится на базе Центра управления безопасностью «ТелеСек Шэард Бизнес СА» (Сертификационный орган), в случае которого применяются принципы сертификации (ПС)/утвержденная практика сертификации (УПС) «ТелеСек Шэард Бизнес СА» компании «Т-Системз Интернэшнл ГмбХ»[4].

Система услуг ПКИ выдает сертификаты, которые подходят для защиты различных бизнес-процессов как на уровне, так и вне компаний, организаций, государственных органов и учреждений, которым требуется соответствующий уровень безопасности информационной среды в целях подтверждения аутентичности, добросовестности и благонадежности конечного субъекта.

[3] https://en.wikipedia.org/wiki/Public_key_infrastructure.

[4] Самую последнюю версию ПС и УПС можно скачать 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», запрашивающая или запрашивающий сертификат

2.1.1.1 Национальный орган запрашивает сертификат по линии проекта «ТАХОнет».

2.1.1.2 Национальный орган:

a) запрашивает сертификаты в службе СЕФ ПКИ;

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

c) скачивает сертификат после утверждения;

d) подписывает и отправляет обратно Регистрационному органу:

i) идентификационную форму контактных лиц и доверенных курьеров,

ii) подписанную индивидуальную доверенность[5].

2.1.2 Доверенный курьер

2.1.2.1 Национальный орган назначает доверенного курьера.

2.1.2.2 Доверенный курьер:

a) передает открытый ключ Регистрационному органу в процессе очной идентификации и регистрации;

b) получает соответствующий сертификат у Регистрационного органа.

2.1.3 Владелец домена

2.1.3.1 Владельцем домена является ГД МОТР.

2.1.3.2 Владелец домена:

a) подтверждает и координирует работу сети «ТАХОнет» и доверительную архитектуру «ТАХОнет», включая подтверждение процедур выдачи сертификатов;

b) управляет работой центрального концентратора «ТАХОнет» и координирует деятельность сторон в части функционирования системы «ТАХОнет»;

c) проводит вместе с национальными органами тесты системы связи с «ТАХОнет.

2.1.4 Регистрационный орган

2.1.4.1 Функции Регистрационного органа выполняет Центр совместных исследований (ЦСИ).

2.1.4.2 Регистрационный орган несет ответственность за проверку идентичности доверенного курьера на предмет регистрации и утверждения запросов на выдачу, отмену и возобновление цифровых сертификатов.

[5] Доверенность – правовой документ, на основании которого организация уполномочивает и разрешает Европейской комиссии, представленной назначенным ею должностным лицом, ответственным за услуги СЕФ ИПК, обращаться с запросом на составление сертификата от имени компании «Т-Системз Интернэшнл ГмбХ ТелеСек Шэард Бизнес СА». См. также пункт 6.

2.1.4.3 Регистрационный орган:

a) присваивает национальному органу уникальный идентификатор;

b) подтверждает идентичность национального органа, его контакты и доверенных курьеров;

c) поддерживает связи со службой поддержки СЕФ в части аутентичности национального органа, его контактов и доверенных курьеров;

d) информирует национальный орган по вопросам утверждения или изъятия сертификата.

2.1.5 Сертификационный орган

2.1.5.1 Сертификационный орган несет ответственность за обеспечение технической инфраструктуры, необходимой для обработки запросов, выдачи и аннулирования цифровых сертификатов.

2.1.5.2 Сертификационный орган:

a) обеспечивает техническую инфраструктуру, необходимую для обработки запросов на выдачу сертификатов национальными органами;

b) утверждает или отклоняет запросы на выдачу сертификата;

c) поддерживает связи с Регистрационным органом в части проверки, в случае необходимости, идентичности запрашивающей Организации.

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 РО;

d) **Этап 4:** Создание сертификата;

e) **Этап 5:** Публикация сертификата;

f) **Этап 6:** Принятие сертификата.

2.2.2 Этап 1: Идентификация доверенного курьера;

В случае идентификации доверенного курьера осуществляется следующий процесс:

a) Регистрационный орган направляет национальному органу идентификационную форму контактных лиц и доверенных курьеров[6]. Эта форма включает также доверенность (PoA), которая подписывается организацией (Орган ЕСТР);

b) национальный орган направляет обратно заполненную форму и подписанную доверенность Регистрационному органу;

c) Регистрационный орган подтверждает факт получения и правильного заполнения этой формы;

d) Регистрационный орган представляет обновленную копию списка контактных лиц и доверенных курьеров владельцу домена.

[6] См. пункт 5.

2.2.3 Этап 2: Создание запроса на сертификат;

2.2.3.1 Запрос и загрузка сертификата производится на том же компьютере и с помощью той же поисковой системы.

2.2.3.2 В случае идентификации доверенного курьера осуществляется следующий процесс:

a) Организация переходит на веб-интерфейс пользователя в целях запроса сертификата с помощью универсального указателя ресурса URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en:, и вносит имя пользователя **«sbca/CEF_eDelivery.europa.eu»** и пароль **«digit.333»**;

b) Организация выбирает мышкой позицию «request» с левой стороны панели и выбирает в выпадающем меню позицию «CEF_TACHOnet»;

c) в порядке завершения этого процесса Организация вносит в форму на запрос сертификата информацию, содержащуюся в таблице 3, выбрав мышкой позицию «Next (soft-PSE)»;

Таблица 3
Полные данные для каждого требуемого поля

Требуемые поля	*Описание*
Страна	**C = Код страны,** местоположение владельца сертификата, проверенное по общедоступному каталогу Ограничения: 2 знака в соответствии с ISO 3166-1, alpha-2, с учетом регистра; примеры: DE, BE, NL Конкретные случаи: UK (для Великобритании), EL (для Греции)
Организация/Компания (O)	**O = Название Организации владельца сертификата**
Основной домен (OU1)	**OU = CEF_eDelivery.europa.eu**
Область ответственности (OU2)	**OU = CEF_TAXOnet**
Департамент (OU3)	Обязательное значение согласно «ОБЛАСТИ ОТВЕТСТВЕННОСТИ» При запросе сертификата содержание необходимо проверить по точному списку («белый список»). Если информация не соответствует списку, то запрос не проходит Формат: **OU = <TYPE>-<GTC_NUMBER>**, где «<TYPE>» заменяют на AP_PROD: пункт доступа в рабочей среде и где <GTC_NUMBER> соответствует **GTC_OID-1.3.130.0.2018.xxxxxx,** а «Ares(2018)xxxxxx» соответствует номеру GTC для проекта «TAXOнет» Например: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Имя (CN)	Эта графа должна быть незаполненной

Требуемые поля	*Описание*
Фамилия (CN)	Должна начинаться с «GRP:», после чего идет обычное название Формат: **CN = GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Например: GRP:CEF_TAXOnet_AP_PROD_BE_001
Эл. почта	**E = CEF-EDELIVERY-SUPPORT@ec.europa.eu**
Эл. почта 1 (SAN)	Эта графа должна быть незаполненной
Эл. почта 2 (SAN)	Эта графа должна быть незаполненной
Эл. почта 3 (SAN)	Эта графа должна быть незаполненной
Адрес	Эта графа должна быть незаполненной
Улица	Должен быть указан официальный адрес организации владельца сертификата. (используется для доверенности)
Номер улицы	Должен быть указан официальный адрес организации владельца сертификата. (используется для доверенности)
Почтовый код	Должен быть указан официальный адрес организации владельца сертификата. (используется для доверенности) **Внимание**: Если почтовый код НЕ 5-значный почтовый код, следует оставить эту графу незаполненной и проставить почтовый код в графе «Город»
Город	Должен быть указан официальный адрес организации владельца сертификата. (используется для доверенности) **Внимание**: Если почтовый код НЕ 5-значный почтовый код, следует оставить эту графу незаполненной и проставить почтовый код в графе «Город»
Номер телефона	Эта графа должна быть незаполненной
Данные идентификации	Адрес электронной почты должен быть тем же, что и адрес, использованный для регистрации уникального идентификатора + Должна быть указана фамилия лица, представляющего организацию. (используется для доверенности) + **Коммерческий регистр №** (обязательное указание только для частных организаций)

Требуемые поля	*Описание*
	Внесено по решению местного суда (требуется только для частных организаций в Германии и Австрии)
Аннулирование пароля	Обязательная графа, выбранная лицом, направившим запрос
Аннулирование пароля (повтор)	Обязательная графа, выбранная лицом, направившим запрос (повтор)

d) выбранная длина ключа должна составлять 2048 (высший разряд);

e) Организация регистрирует исходный номер для загрузки сертификата;

f) Группа поддержки СЕФ проверяет новые запросы на сертификаты и выясняет, действительна ли информация, занесенная в сертификат;

g) Группа поддержки СЕФ проверяет запрос с целью убедиться в том, что информация занесена в него в правильном формате;

h) если одна из проверок дает отрицательные результаты, Группа поддержки СЕФ направляет сообщение по электронной почте по адресу электронной почты, указанному в графе формы запроса «Identification data» (Идентификационные данные), с копией владельцу домена, в котором данной организации предлагается еще раз повторить этот процесс с начала. Запрос на сертификат, который не прошел, аннулируется;

i) Группа поддержки СЕФ направляет сообщение по электронной почте Регистрационному органу по поводу обоснованности этого запроса. В это электронное сообщение включают следующие данные:

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

2) дата сертификата, включая название AP (пункт доступа), где должен быть выдан сертификат, указанное в графе «Last Name (CN)» (Фамилия (CN));

3) исходный номер сертификата;

4) адрес организации, адрес ее электронной почты и фамилия лица, которое ее представляет.

2.2.4 Этап 3: Регистрация в Регистрационном органе (утверждение сертификата)

2.2.4.1 Доверенный курьер или контактное лицо назначает встречу в Регистрационном органе посредством обмена электронными сообщениями, позволяющими идентифицировать доверенного курьера, который проведет очную встречу.

2.2.4.2 Организация готовит пакет документации, состоящий из:

a) заполненной и подписанной доверенности;

b) копии действительного паспорта доверенного курьера, который проведет очную встречу. Эта копия должна быть подписана одним из контактных лиц организации, идентифицированных на этапе 1;

c) бумажного экземпляра запроса на сертификат, подписанного одним из контактных лиц организации.

2.2.4.3 Регистрационный орган принимает доверенного курьера после проверки его идентичности в приемной здания. Регистрационный орган производит очную регистрацию запроса на сертификат посредством:

a) идентификации и подтверждения аутентичности доверенного курьера;

b) проверки физической внешности по паспорту, предъявленному доверенным курьером;

c) проверки срока действия паспорта, предъявленного доверенным курьером;

d) сверки подтвержденного паспорта, предъявленного доверенным курьером, с копией действительного паспорта доверенного курьера, подписанного одним из идентифицированных контактных лиц организации. Подпись подтверждается посредством сверки с оригиналом «идентификационной формы доверенного курьера и контактных лиц»;

e) сверки заполненной и подписанной доверенности;

f) сверки бумажного варианта запроса на сертификат и проставленной в нем подписи с оригиналом «идентификационной формы доверенного курьера и контактных лиц»;

g) предложения подписавшему контактному лицу еще раз проверить идентичность доверенного курьера и содержание запроса на сертификат.

2.2.4.4 Регистрационный орган подтверждает Группе поддержки СЕФ, что национальный орган действительно уполномочен производить действия, на которые он запрашивает сертификаты, и что соответствующий очный процесс регистрации произведен успешно. Это подтверждение направляется надежной электронной почтой с использованием сертификата «CommiSign» с приложенной отсканированной копией подтвержденного в ходе очной встречи пакета документов и подписанного контрольного списка функциональных проверок, проведенных Регистрационным органом.

2.2.4.5 Если Регистрационный орган подтверждает законность запроса, то процесс его удовлетворения осуществляется в соответствии с пунктами 2.2.4.6 и 2.2.4.7. В противном случае запрос о выдаче сертификата будет отклонен, и запрашивающая организация будет соответствующим образом проинформирована.

2.2.4.6 Группа поддержки СЕФ утверждает запрос на сертификат и уведомляет Регистрационный орган об утверждении сертификата.

2.2.4.7 Регистрационный орган уведомляет организацию, что сертификат можно получить через портал пользователя.

2.2.5 Этап 4: Создание сертификата;

Сертификат создается после утверждения запроса на его выдачу.

2.2.6 Этап 5: Публикация сертификата и его загрузка

2.2.6.1 После утверждения запроса на сертификат 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.

2.2.6.3 Организация переходит на портал пользователя по адресу https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: и входит в систему под именем пользователя **«sbca/CEF_eDelivery.europa.eu»** и вводит пароль **«digit.333»**.

2.2.6.4 Организация выбирает мышкой позицию «fetch» с левой стороны и указывает исходный номер, зарегистрированный в ходе процесса прохождения заявки на сертификат.

2.2.6.5 Организация инсталлирует сертификаты, выбрав мышкой кнопку «install».

2.2.6.6 Сертификат инсталлируется в пункте доступа. Поскольку с точки зрения осуществления этот процесс носит специфичный характер, организация обращается к провайдеру своего пункта доступа с просьбой дать описание этого процесса.

2.2.6.7 В целях инсталляции сертификата в пункте доступа необходимо предпринять следующие шаги:

a) экспортировать закрытый ключ и сертификат,

b) создать хранилище ключей и хранилище доверенных сертификатов,

c) инсталлировать в пункте доступа хранилище ключей и хранилище доверенных сертификатов.

3. Процедура запроса сертификата

3.1 Организация представляет запрос на аннулирование через веб-портал пользователя.

3.2 Процесс аннулирования сертификата осуществляет Группа поддержки СЕФ.

4. Общие положения и условия предоставления услуги СЕФ ПКИ

4.1 Контекст

В своем качестве системного интегратора структурного элемента системы «eDelivery» Европейского механизма взаимодействий ДИГИТ оказывает услуги ПКИ[7] («услуги СЕФ ПКИ») Договаривающимся сторонам ЕСТР. Услуги СЕФ ПКИ используются национальными органами (конечными пользователями), участвующими в системе «ТАХОнет».

ДИГИТ является арендатором системы ПКИ в Группе «ТелеСек Шэард Бизнес СА солюшн» («SBCA»), которая действует в Центре сертификации Группы «Т-Системз Интернэшнл ГмбХ» («Т-Системз»[8]). ДИГИТ играет роль ведущего регистратора домена SBCA «CEF_eDelivery.europa.eu». В этом качестве ДИГИТ создает в рамках домена «CEF_eDelivery.europa.eu» соответствующие субдомены для каждого проекта, который пользуется услугами СЕФ ПКИ.

В настоящем документе содержится детальная информация о положениях и условиях субдомена системы «ТАХОнет». ДИГИТ выполняет функцию субрегистратора этого субдомена. В этом качестве он выдает, аннулирует и возобновляет сертификаты этого проекта.

[7] ПКИ (Инфраструктура сертификации открытых ключей) представляет собой набор ролей, принципов, процедур и систем, необходимых для создания, управления, распределения и отмены цифровых сертификатов.

[8] Доверенная роль оператора Центра сертификации, расположенного в Группе «Т-Системз», состоит также в решении задачи, возложенной на внутренний регистрационный орган.

4.2 Отказ от ответственности

Европейская комиссия не берет на себя какой бы то ни было материальной или моральной ответственности за содержание сертификата, которая возлагается исключительно на владельца сертификата. Ответственность за проверку точности содержания сертификата возлагается на его владельца;

Европейская комиссия не берет на себя какой бы то ни было материальной или моральной ответственности за использование сертификата его владельцем, который является третьим субъектом права вне Европейской комиссии.

Данный отказ от ответственности не имеет целью ограничить ответственность Европейской комиссии в нарушение любых требований, закрепленных в применимом национальном законодательстве, или снять с себя ответственность в тех вопросах, которые нельзя исключить из сферы действия этого законодательства.

4.3 Разрешенные/запрещенные виды использования сертификатов

4.3.1 Разрешенные виды использование сертификатов

После выдачи сертификата национальный орган использует данный сертификат только в контексте «TAXOнет»[9]. В этом контексте данный сертификат может использоваться для:

- аутентификации происхождения данных;
- кодирования данных;
- надежного выявления случаев нарушения целостности данных.

4.3.2 Запрещенные виды использования сертификатов

Любое использование, которое однозначно не разрешается в качестве допустимого вида использования данного сертификата, запрещено.

4.4 Дополнительные обязательства владельца сертификата

Детальные положения и условия SBCA определены Группой «Т-Системз» в принципах сертификации (CP)/положении о практике сертификации (CPS) службы SBCA10. В данном документе включены технические требования и руководящие принципы регулирования технических и организационных аспектов и описываются виды деятельности оператора Сертификационного центра в роли Сертификационного органа (CA) и Регистрационного органа (RA), а также уполномоченной третьей стороны Регистрационного органа (RA).

Обращаться с запросом на сертификат могут только те субъекты, которые принимают участие в работе системы «TAXOнет».

Что касается признания сертификата, то в данном случае применяются принципы сертификации и положение о практике сертификации SBCA (CP/CPS), указанные в пункте 4.4.1. Кроме того, условия использования и соответствующие положения, описанные в настоящем документе, считаются признанными той организацией, которой был выдан сертификат («O=») в самом начале.

[9] Идентифицируется по значению атрибута «O=» в отличительном определении сути выданного сертификата.

[10] Самая последняя версия SBCA CP/CPS Группы «Т-Системз» доступна по адресу: **https://www.telesec.de/en/sbca-en/support/download-area/**.

Что касается публикации сертификата, то в этом случае применяются требования SBCA CP/CPS, указанные в пункте 2.2.

Все владельцы сертификатов соблюдают следующие требования:

1) обеспечивают защиту своего закрытого ключа от несанкционированного использования;

2) воздерживаются от передачи или предания огласке закрытого ключа третьим сторонам, даже в качестве представителей;

3) воздерживаются от дальнейшего использования закрытого ключа по истечении срока действия или аннулирования сертификата, помимо просмотра зашифрованных данных (например, для расшифровки сообщений электронной почты);

4) владелец сертификата несет ответственность за копирование или передачу ключа конечному субъекту или субъектам;

5) владелец сертификата должен обязать конечного субъекта/ всех конечных субъектов соблюдать настоящие положения и условия, включая SBCA CP/CPS, регламентирующие использование закрытого ключа;

6) владелец сертификата должен представить идентификационные данные тех уполномоченных представителей, которым разрешается направлять требование в целях аннулирования сертификатов, выданных данной организации, с указанием подробной информации о событиях, которые обусловили необходимость аннулирования этого сертификата, а также аннулирования пароля;

7) в случае сертификатов, относящихся к группам лиц и функциям и/или юридическим лицам, после того как соответствующее лицо уходит из группы конечных субъектов (например, в случае прекращения трудовых отношений), владелец сертификата должен предотвратить злоупотребление открытым ключом посредством соответствующего аннулирования сертификата;

8) владелец сертификата несет ответственность и требует аннулировать сертификат в обстоятельствах, указанных в пункте 4.9.1 SBCA CP/CPS.

В случае возобновления или изменения ключа к сертификатам, применяется пункт 4.6 или 4.7 SBCA CP/CPS.

В случае внесения поправки в сертификат применяется пункт 4.8 SBCA CP/CPS.

В случае отмены сертификата применяется пункт 4.9 SBCA CP/CPS.

5. Форма идентификации контактных лиц и доверенных курьеров (образец).

Я, *[фамилия и адрес представителя организации]***, удостоверяю, что нижеследующая информация будет использоваться в связи запросом, созданием и получением сертификатов на открытый цифровой ключ к пунктам доступа к системе «ТАХОнет» в порядке обеспечения конфиденциальности, целостности и отказоустойчивости сообщений «ТАХОнет»:**

Информация о контактных лицах:

– **Контактное лицо № 1**	– **Контактное лицо № 2**
– Фамилия:	– Фамилия:
– Имя	– Имя
– Сотовый телефон:	– Сотовый телефон:
– Телефон:	– Телефон:
– Электронная почта:	– Электронная почта:
– Образец собственноручной подписи: –	– Образец собственноручной подписи: – – –

Информация о доверенных курьерах:

– **Доверенный курьер № 1**	– **Доверенный курьер № 2**
– Фамилия:	– Фамилия:
– Имя	– Имя
– Сотовый телефон:	– Сотовый телефон:
– Электронная почта:	– Электронная почта:
– Страна выдачи паспорта:	– Страна выдачи паспорта:
– Номер паспорта:	– Номер паспорта:
– Дата истечения срока действия паспорта:	– Дата истечения срока действия паспорта:

Место, дата, штамп или печать Организации:
Подпись уполномоченного представителя:

6. Документы

6.1 Индивидуальная доверенность (образец)

Образец индивидуальной доверенности, которая должна быть подписана и предъявлена доверенным курьером в ходе очной регистрации в RAO, приводится ниже:

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):

☒ user [1]: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server [2]: 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-Gateway [3]: 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)

Образец бумажного бланка запроса на сертификат, который должен быть подписан и предъявлен доверенным курьером в ходе очной регистрации в RAO, приводится ниже:

Просьба напечатать текст настоящего документа на фирменном бланке, проставить штамп вашей организации и передать на подпись уполномоченному представителю вашей организации.

Бумажный бланк запроса на сертификат «TAXOnet»

Я, ***[фамилия и адрес представителя организации]***, удостоверяю, что нижеследующая информация будет использоваться в связи запросом, созданием и получением сертификатов на открытый цифровой ключ к пунктам доступа в системе «TAXOnet» в порядке обеспечения конфиденциальности, целостности и отказоустойчивости сообщений «TAXOnet»:

Просьба воспроизвести информацию с данными сертификата, представленную Группой поддержки СЕФ, подтверждающей полноту электронного запроса на сертификат, например:

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

Исходный номер запроса на сертификат: *включить исходный номер (например, 776002)*
Идентификация доверенного курьера, прибывающего на очную регистрацию запроса: *просьба заполнить*

Доверенный курьер № 1
Фамилия:
Имя (имена):
Сотовый телефон:
Эл. почта:
Страна выдачи паспорта:
Номер паспорта:
Дата истечения действия паспорта:

Место, дата, штамп или печать Организации:

Подпись уполномоченного представителя:

7. Глоссарий

Основные термины, использованные в настоящем разделе добавления, определены в разделе определений СЕФ на едином цифровом веб-портале СЕФ:

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

Основные акронимы, использованные в данном описании предложенного компонента, определены в глоссарии СЕФ на едином цифровом веб-портале СЕФ:

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

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

8. Передача работы на субподряд

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

8.2 Такого рода субподряд не освобождает стороны от ответственности в соответствии с положениями настоящего добавления, включая ответственность за обеспечение надлежащего уровня обслуживания в соответствии с подразделом добавления 4.6.