**Техническое задание**

напредоставление права использования программного обеспечения на условиях простой (неисключительной) лицензии в целях получения пользователями квалифицированных сертификатов ключей проверки электронных подписей

## 1. Назначение документа

Настоящий документ содержит Техническое задание на предоставление права использования программного обеспечения на условиях простой (неисключительной) лицензии для взаимодействия с Удостоверяющим центром по созданию ключей электронной подписи

**2. Термины и определения, использующиеся в Техническом задании**

|  |  |
| --- | --- |
| Термин / Сокращение | Описание / Определение / Расшифровка |
| Лицензиар | Правообладатель программного обеспечения или иное лицо, имеющее право предоставлять право использования программного обеспечения на законных основаниях. |
| Лицензиат | Лицо (сторона договора) получившее право использования программного обеспечения на условиях простой (неисключительной) лицензии. |
| ИС | Информационная система |
| Информационная система Удостоверяющего центра | Автоматизированная информационная система, обеспечивающая регистрацию пользователей в Удостоверяющем центре и выполнение сервисных операций в процессе создания и выдачи пользователям квалифицированных сертификатов ключей проверки электронных подписей. |
| ПО | Программное обеспечение, которое обеспечивает взаимодействие Лицензиата (пользователей) с Удостоверяющим центром в процессе создания ключей электронной подписи и получения квалифицированных сертификатов ключей проверки электронных подписей. |
| Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) | Сертификат ключа проверки электронной подписи, соответствующий требованиям установленным Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи и являющийся в связи с этим официальным документом.  |
| Ключ проверки электронной подписи (ключ проверки ЭП) | Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. |
| Ключевой носитель | Электронное защищенное USB-устройство, предназначенное для хранения ключей электронной подписи и (опционально) квалифицированных сертификатов ключей проверки электронных подписей (USB-токены компаний Актив,  Аладдин Р.Д., ISBC и др.) |
| Криптопровайдер | Независимый программный модуль (Cryptography Service Provider, CSP), реализующий стандартный криптографический интерфейс компании Microsoft - CryptoAPI 2.0. |
| Пользователь | Определенный Лицензиатом потребитель услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей. |
| Уполномоченный сотрудник | Сотрудник Лицензиата/(организации), ответственный за информационную безопасность Лицензиата/ (организации) и выступающий от имени Лицензиата/ (всех остальных работников организации). Имеет действующий квалифицированный сертификат, выданный Удостоверяющим центром и наделён Лицензиатом/(организацией) полномочиями взаимодействовать от его имени с Удостоверяющим центром по вопросам идентификации пользователей, а также вопросам создания, выдачи, отзыва квалифицированных сертификатов пользователей при помощи сервиса автоматизированного взаимодействия, предоставленного ему Лицензиаром. |
| Сервис автоматизированного взаимодействия | Сервис является частью информационной системы Удостоверяющего центра, расположен на web-сайте Лицензиара и позволяет осуществлять дистанционное взаимодействие между уполномоченным сотрудником Лицензиата/ (организации) и Удостоверяющим центром для контроля и обработки поданных пользователями заявок. |
| Сертификат ключа проверки электронной подписи (сертификат) | Электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. |
| АРМ | Автоматизированное рабочее место |
| СКЗИ | * 1. Средства криптографической защиты информации – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
 |
| СМЭВ | Система межведомственного электронного взаимодействия  |
| ТЗ |  Техническое задание |
| Удостоверяющий центр (УЦ) | Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».  |
| ФСБ | Федеральная служба безопасности России |
| Электронная подпись (ЭП) | Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. |

**3. Предмет закупки**

Предоставление Лицензиаром права использования программного обеспечения на условиях простой (неисключительной) лицензии Лицензиату для взаимодействия с Удостоверяющим центром по созданию ключей электронной подписи, для внутрикорпоративного использования, / для использования в государственной / муниципальной / корпоративной информационной системе <название ИС>, с записью на ключевой носитель;

Организация взаимодействия Лицензиата (пользователей/ ( уполномоченного сотрудника организации) с Лицензиаром путем удаленного доступа к ПО на сайте, обеспечивающему передачу в УЦ заявок на создание ключей электронной подписи и создание сертификатов / самостоятельное создание пользователями ключей электронной подписи и передачу в УЦ запросов на сертификаты формата PKCS#10, передачу в УЦ регистрационных данных пользователей, формирование необходимых документов в процессе регистрации пользователей в УЦ, прием из УЦ созданных сертификатов, а также их учет;

Оказание Лицензиаром услуги на предоставление сервиса автоматизированного взаимодействия Лицензиату/ (уполномоченному сотруднику организации) с Удостоверяющим центром, функционал которого предоставляется лицу, ответственному за информационную безопасность Лицензиата/ (организации) и выступающему от имени Лицензиата/ (пользователей). Доступ к сервису автоматизированного взаимодействия осуществляется уполномоченным сотрудником Лицензиата/(организации) на web-сайте Лицензиара путём настраивания ролевой модели управления взаимодействием между пользователями, уполномоченным сотрудником Лицензиата/(организации) и Удостоверяющим центром;

Оказание услуг технической и методической поддержки Лицензиату (пользователям) по вопросам использования программного обеспечения в режиме 8х5 с 09:00 до 18:00, в рабочие дни Лицензиата/24x7х365 по телефонам «горячей линии» и электронной почте в течение срока действия контракта;

Оказание дополнительных услуг по настройке рабочего места владельца сертификата в режиме 8х5: с 09:00 до 18:00, в рабочие дни Лицензиата.

**4. Цель предоставления прав и оказания услуг**

Обеспечение Лицензиата правом использования ПО на условиях простой (неисключительной) лицензии в целях получения Лицензиатом (пользователями) квалифицированных сертификатов с записью на ключевые носители в количестве 400 штук для нужд <наименование Лицензиата> / для работы в информационной системе <наименование ИС>.

Срок предоставления прав использования программного обеспечения - 12 (двенадцать) календарных месяцев с даты предоставления доступа.

Территорией использования программного обеспечения является Российская Федерация.

**5. Место исполнения**

Доступ к программному обеспечению осуществляется через web-интерфейс на web-

Процедура выдачи сертификатов должна осуществляться через информационную систему УЦ для создания сертификатов, с возможностью контроля процесса создания сертификатов.

**6. Сроки исполнения**

В течение 10 (десяти) рабочих дней со дня получения заявки от Лицензиата (пользователя) Лицензиар обязуется предоставить право использования ПО Лицензиату (пользователю) путем активации доступа к функциональным возможностям ПО на сервере Лицензиара, что подтверждается предоставлением пользователям уникального имени (логина) и пароля для использования ПО. Одна лицензия на ПО позволяет пользователю получить 1 (один) квалифицированный сертификат ключа проверки электронной подписи.

Квалифицированные сертификаты ключей проверки электронной подписи должны быть созданы и переданы Лицензиату (пользователю) посредством ИС УЦ в течение 10 (десяти) рабочих дней с момента получения Лицензиаром от Лицензиата заявки на создание сертификата и предоставления достоверных сведений и документов, необходимых для создания сертификатов. Заявка имеет силу для сторон как в случае ее передачи Лицензиару путем вручения документа, так и при ее передаче в электронном виде средствами компьютерной и иной связи.

Заявки на создание сертификатов поступают от Лицензиата в течение срока действия контракта (партиями или по одной) по мере необходимости, в общем количестве, не превышающем N шт.

Срок действия квалифицированного сертификата ключа проверки электронной подписи, создаваемого УЦ, должен составлять 12 месяцев с момента его создания.

**7. Состав закупки**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование**  | **Кол-во лицензий, ед.** |
| 1 | Право использования ПО на условиях простой (неисключительной) лицензии в целях получения пользователями квалифицированных сертификатов ключей проверки электронных подписей для *физического лица* (срок действия сертификата - 12 месяцев). | 400 лицензий |

**8. Требования к Удостоверяющему центру, привлекаемому Лицензиаром для создания ключей электронной подписи и для создания и выдачи квалифицированных сертификатов ключей проверки электронной подписи**

 **8.1. Нормативно-правовые требования к Удостоверяющему центру**

Лицензиар должен обеспечить участие/привлечение аккредитованного Удостоверяющего центра, отвечающего следующим требованиям:

* УЦ на весь срок действия сертификата по условиям контракта должен иметь действующую лицензию ФСБ России, выданную в соответствии с Постановлением Правительства Российской Федерации от 16 апреля 2012 года № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» и Федеральным законом от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
* Удостоверяющий центр должен быть аккредитован в соответствии с требованиями, установленными Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и состоять в реестре аккредитованных Удостоверяющих центров в на портале <http://e-trust.gosuslugi.ru/CA>.
* Удостоверяющий центр должен выполнять требования Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и иных нормативных документов по защите персональных данных (ПДн) и должен быть включен в реестр операторов, осуществляющих обработку персональных данных.

**8.2. Требования к программно-аппаратному комплексу Удостоверяющего центра**

Квалифицированные электронные подписи, обеспечивающие юридическую значимость электронного документооборота Лицензиата, формируются с использованием квалифицированных сертификатов, создаваемых и выдаваемых аккредитованным УЦ.

Программно-аппаратный комплекс (ПАК) УЦ, обеспечивающий выполнение целевых функций, должен быть сертифицирован на соответствие требованиям ФСБ России к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27.12.2011г. № 796, и требованиям к информационной безопасности удостоверяющих центров, установленным для класса не ниже КС2 / КС3.

Программно-аппаратный комплекс УЦ для создания квалифицированных сертификатов должен обеспечивать:

* управление сертификатами в соответствии с международными стандартами и рекомендациями ITU-T **Х.509 v.3,** IETF **RFC 5280,** RFC 7091, RFC 4491, **RFC 5652 (CMS), PKCS#10;**
* поддержку российских криптографических алгоритмов **ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012;**
* выполнение следующих базовых функций:
* создание ключей УЦ;
* формирование корневых сертификатов УЦ;
* регистрация пользователей УЦ;
* регистрация и обработка запросов на создание сертификатов формата PKCS#10;
* контроль уникальности ключей электронной подписи в запросах на сертификаты;
* подтверждение владения пользователем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в запросе формата PKCS#10, в соответствии с «Правилами подтверждения владения ключом», утвержденными Приказом ФСБ России от 20.04.2021 г. №154;
* создание сертификатов пользователей по запросам формата PKCS#10;
* выдача сертификатов ключей электронной подписи в электронной форме и в форме документов на бумажных носителях;
* аннулирование сертификатов;
* формирование и публикация списка отозванных сертификатов;
* обеспечение доступа к реестру квалифицированных сертификатов, созданных Удостоверяющим центром, в соответствии с Приказом Министерства связи и массовых коммуникаций Российской Федерации от 22.08.2017г. № 436;
* передача в ЕСИА сведений о выданных квалифицированных сертификатах;
* возможность создания по заявкам Лицензиата (Пользователей) ключей электронной подписи (с гарантией сохранения их в тайне) в формате любого сертифицированного ФСБ России средства ЭП, поддерживающего интерфейс MS Crypto API 2.0 или PKCS#11 v.2.30;
* предоставление владельцам выданных сертификатов актуальной информации о статусе сертификатов посредством Сервиса службы актуальных статусов сертификатов (служба OCSP); служба OCSP должна обеспечивать:
* возможность проверки статуса сертификата в режиме реального времени;
* соответствие стандартам RFC 2560 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)»;
* предоставление Сервиса службы штампов времени (служба TSA); cлужба TSA должна обеспечивать:
* удостоверение времени создания и/или подписания электронного документа;
* соответствие стандартам RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).

**8.3. Требования к информационной системе Удостоверяющего центра**

Информационная система Удостоверяющего центра должна обеспечивать следующий функционал взаимодействия:

* оповещения– отправка уведомлений о ходе регистрации заявок на электронную почту пользователям информационной системы УЦ;
* формирование реестра выданных сертификатов – обеспечивается функциональность в части ведения реестра всех созданных сертификатов пользователям, в том числе с возможностью его выгрузки на внешние запоминающие устройства;
* взаимодействие через СМЭВ с государственными информационными ресурсами - обеспечивается запрос, получение, проверка и/или подтверждение достоверности документов и сведений, представленных пользователем в заявке на создание квалифицированного сертификата, при этом реализуются следующие возможности:
* проверка в автоматизированном режиме и получение из информационных ресурсов ФНС сведений о соответствии ИНН заявителя – физического лица его паспортным данным при подаче заявок на получение сертификата;
* проверка в автоматизированном режиме и получение из информационных ресурсов ПФР сведений о соответствии фамильно–именной группы (ФИО) заявителя – физического лица и его СНИЛС при подаче заявок на получение сертификата;
* проверка в автоматизированном режиме и получение из информационных ресурсов МВД сведений о статусе действительности паспорта гражданина РФ;
* хранение входящих и исходящих квитанций при взаимодействии с сервисом СМЭВ;
* информационная система удостоверяющего центра должна поддерживать ролевую модель управления доступом к возможностям системы;
* учет сформированных запросов на сертификаты и выданных сертификатов;
* отслеживание статуса заявок и срока действия выданных сертификатов;
* протоколирование действий пользователя и процессов, связанных с созданием сертификатов.

 **8.4. Требования к сервису автоматизированного взаимодействия**

Сервис автоматизированного взаимодействия является частью информационной системы Удостоверяющего центра и должен обеспечивать Лицензиату/ (уполномоченному сотруднику организации) возможность контролировать и обрабатывать поданные пользователями заявки:

* создавать заявки на получение услуг удостоверяющего центра
* отслеживать подачу заявок на сертификаты пользователями
* проверять статус заявки и сертификата
* проводить идентификацию пользователей, включая проверку данных, используя специализированные сервисы СМЭВ
* редактировать данные, указанные в запросах на создание сертификатов
* управлять уведомлениями о ходе регистрации заявок
* выгружать отчеты по заявкам в удобном формате.

 По запросу Лицензиата/(уполномоченного сотрудника организации) сервис автоматизированного взаимодействия должен обеспечивать возможность формирования отчетов о полученных заявках и выданных сертификатах в виде таблицы со следующим набором полей:

* номер заявки на создание ключа электронной подписи и сертификата;
* дата размещения заявки;
* реквизиты организации - заявителя;
* ФИО владельца сертификата – физического лица;
* контактные данные владельца сертификата;
* cтатус заявки;
* статус сертификата;
* серийный номер сертификата;
* срок действия сертификата.

**9. Требования к закупаемому программному обеспечению**

Программное обеспечение, а также расширения функционала программного обеспечения, должны обеспечивать взаимодействие Лицензиата (пользователей) с информационной системой Удостоверяющего центра в процессе создания и выдачи сертификатов и обладать следующим функционалом:

*-* регистрация пользователей – создание учетных записей пользователей информационной системы УЦ;

- авторизация пользователей – аутентификация и авторизация пользователя информационной системы УЦ;

- регистрация и обработка заявок – выполнение порядка последовательности действий по созданию сертификатов;

Доступ пользователей к программному обеспечению осуществляется через web-интерфейс на web-сайте Лицензиара.

Право использования ПО Лицензиату (пользователю) предоставляется путем активации доступа к функциональным возможностям ПО на сервере правообладателя (Лицензиара), что подтверждается предоставлением пользователям уникального имени (логина) и пароля для использования ПО. Одна лицензия на ПО позволяет пользователю получить 1 (один) квалифицированный сертификат ключа проверки электронной подписи.

ПО должно обеспечивать взаимодействие пользователей с Удостоверяющим центром (службами регистрации в пунктах обслуживания Удостоверяющего центра) в процессе создания ключей электронной подписи и получения квалифицированных сертификатов без необходимости посещения пункта обслуживания Удостоверяющего центра, путем предоставления удобного web-интерфейса взаимодействия Лицензиата и Лицензиара.

ПО может иметь возможность адаптации элементов графического интерфейса личных кабинетов под требования Лицензиата.

Посредством ПО должно обеспечиваться выполнение следующей функциональности:

* подача заявок на генерацию ключей электронной подписи и создание сертификатов;
* возможность самостоятельной генерации пользователем ключей электронной подписи и передача в УЦ запросов на сертификаты формата PKCS#10;
* подача заявок на прекращение действия сертификатов;
* передача регистрационных данных пользователей и скан-копий документов, необходимых для создания сертификатов;
* прием из УЦ созданных сертификатов и их запись на ключевой носитель (опционально);
* возможность автоматизированного приема и обработки как самоподписанных запросов на сертификаты, так и запросов на сертификаты, подписанных действующим ключом электронной подписи пользователя / уполномоченного сотрудника организации.

 **10. Требования к СКЗИ на рабочих местах пользователей**

Ключи электронных подписей и запросы на сертификаты должны создаваться с использованием сертифицированных ФСБ России средств криптографической защиты информации и иметь совместимость с криптопровайдером, используемым у Лицензиата, а именно СКЗИ VipNet CSP или VipNet PKI Client.

Для обеспечения криптографических преобразований на рабочем месте пользователя должно использоваться свободно распространяемое на территории РФ сертифицированное СКЗИ, реализующее функции средства ЭП.

СКЗИ должно обеспечивать поддержку создания ключей электронной подписи для алгоритмов ГОСТ Р 34.10-2012.

СКЗИ должно обеспечивать поддержку операционных систем на базе ОС Windows.

 **11. Требования к ключевому носителю**

В качестве ключевых носителей должны использоваться устройства, разрешенные эксплуатационной документацией сертифицированного СКЗИ или средства ЭП, используемых для создания ключей электронной подписи.

Ключевой носитель (Рутокен / JaCarta PRO / JaCarta PKI / JaCarta LT / Рутокен ЭЦП 2.0 / JaCarta ГОСТ / JaCarta-2 ГОСТ / ESMART Token ГОСТ) предоставляется Лицензиаром/ Лицензиатом.

 **12. Требования к квалифицированным сертификатам и порядку их создания**

 **12.1. Структура и состав квалифицированных сертификатов определяется:**

* Требованиями Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;
* Приказом ФСБ России №795 от 27 декабря 2011 года «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
* Регламентом создания сертификатов - Удостоверяющего центра, который должен иметь аккредитацию Министерства связи и массовых коммуникаций Российской Федерации в соответствии с требованиями Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;
* Международными стандартами и рекомендациями ITU-T X.509 v.3, IETF RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile), RFC 4491 (Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile).

Квалифицированные сертификаты должны:

* содержать поля, обязательные для заполнения в соответствии с приказом ФСБ России №795 от 27 декабря 2011 года «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи» и требованиями Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;
* включать следующие обязательные значения в расширениях:

«Использование ключа» - цифровая подпись, неотрекаемость, шифрование ключей, шифрование данных;

«Улучшенный ключ» - проверка подлинности клиента (1.3.6.1.5.5.7.3.2); защищенная электронная почта (1.3.6.1.5.5.7.3.4);

* «Тип идентификации при выдаче сертификата» (IdentificationKind) - при личном присутствии (0) / с использованием квалифицированной ЭП (1) / с использованием загранпаспорта нового поколения (2);
* допускаться для внутрикорпоративного использования, / для использования в государственной / муниципальной / корпоративной информационной системе <название ИС>.

 **12.2. Порядок создания квалифицированных сертификатов**

Регистрация в ПО пользователей и создание для них сертификатов должны обеспечиваться в автоматизированном режиме на основе запросов, формируемых по заявкам зарегистрированных пользователей и отправляемых в УЦ вместе с регистрационными данными через ПО.

Автоматизированный режим регистрации запросов и создания сертификатов на основе регистрационных данных, поступающих в УЦ посредством ПО пользователей (уполномоченных сотрудников организации), возможен только в том случае, если процедура идентификации и проверка регистрационных данных владельцев сертификатов выполняется в полном соответствии с требованиями Федерального закона № 63-ФЗ «Об электронной подписи».

Бизнес-процесс использования ПО с целью получения пользователями сертификатов состоит из основных этапов:

1. Настройка АРМ уполномоченного сотрудника Лицензиата/(организации) для взаимодействия с Удостоверяющим центром.

 Уполномоченный сотрудник Лицензиата/(организации) при помощи ПО получает в Удостоверяющем центре квалифицированный сертификат ключа проверки электронной подписи. Лицензиар подготавливает и выдаёт доступ к сервису автоматизированного взаимодействия уполномоченному сотруднику Лицензиата/ (организации) для контроля и обработки заявок пользователей.

2. Получение пользователями при помощи ПО квалифицированных сертификатов в Удостоверяющем центре.

Лицензиар предоставляет Лицензиату (пользователям) право использования ПО для получения квалифицированных сертификатов. При помощи ПО пользователи при их обращении в Удостоверяющий центр Лицензиара получают квалифицированные сертификаты при условии предоставления всех необходимых для создания сертификата достоверных сведений и документов.

3. Техническое сопровождение.

 Техническое сопровождение выданных пользователям квалифицированных сертификатов осуществляется в течение 12 месяцев с момента создания сертификата в Удостоверяющем центре.

 **13. Требования и условия предоставления оказываемых услуг Удостоверяющего центра**

Удостоверяющий центр реализует целевые функции по созданию и выдаче сертификатов в соответствии с требованиями законодательства Российской Федерации, в том числе, в соответствии с требованиями Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи», Федерального закона от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Оказание услуг должно осуществляться в соответствии с Регламентом УЦ и Регламентом взаимодействия Удостоверяющего центра и Доверенного лица при выдаче пользователям квалифицированных сертификатов ключей проверки электронных пользователей.

Регламент взаимодействия Удостоверяющего центра и Доверенного лица при выдаче пользователям квалифицированных сертификатов ключей проверки электронных пользователей должен соответствовать требованиям настоящего Технического задания и контракта.

 **14. Требования к характеристикам услуг**

Выдаваемые квалифицированные сертификаты должны соответствовать требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» и требованиям пункта 12 настоящего Технического задания, в частности:

* Удостоверяющий центр должен обеспечивать создание квалифицированных сертификатов в соответствии с ГОСТ 34.10-2012.
* должна быть обеспечена возможность управления статусом созданных сертификатов в течение всего срока их действия.
* в течение всего срока действия сертификатов Удостоверяющий центр должен обеспечивать предоставление владельцам выданных сертификатов актуальной информации о статусе их сертификатов посредством Сервиса службы актуальных статусов сертификатов (OCSP).

 **15. Требования к техническому сопровождению**

В рамках технического сопровождения сотрудники Лицензиара оказывают консультирование специалистов Лицензиата по вопросам использования ПО, использования, установки и настройки сертификатов, выданных Удостоверяющим центром, а также по вопросам, связанным с получением услуг и использованием средств ЭП. Техническое сопровождение должно быть включено в лицензионное вознаграждение.

Техническое сопровождение включает:

* консультирование должно оказываться по электронной почте и телефону;
* горячая линия Лицензиара должна работать в режиме 8х5 09:00 до 18:00, в рабочие дни Лицензиата / 24х7х365: круглосуточно, без выходных дней.

В рамках технического сопровождения Лицензиар также может оказывать дополнительные услуги по согласованию с Лицензиатом:

* удаленная настройка рабочего места владельца сертификата, которая включает в себя установку и настройку средств электронной подписи с использованием технологий удалённого доступа;
* удаленная расширенная настройка рабочего места владельца сертификата, которая включает в себя установку и настройку рабочего места для работы на порталах государственных и муниципальных информационных систем, электронных торговых площадках и др.

 **16. Гарантийные обязательства**

Удостоверяющий центр обязан обеспечить гарантийное сопровождение выданных квалифицированных сертификатов в течение 1 года, начиная со дня, следующего за днем создания ключей и сертификатов, в соответствии с требованиями ТЗ. Гарантийное сопровождение должно оказываться в режиме 24х7х365: круглосуточно, без выходных дней.

Гарантийное сопровождение сертификатов включает:

* аннулирование сертификатов – не более 12 часов с момента поступления необходимых сведений от Лицензиата (пользователей);
* ведение реестра выданных и аннулированных сертификатов в соответствии с требованиями Приказа Министерства связи и массовых коммуникаций Российской Федерации от 22.08.2017 г. № 436 «Об утверждении Порядка формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров». Актуализация реестра должна производиться Удостоверяющим центром с периодичностью не менее 1 раза в день;
* проверку по обращениям Лицензиата электронных подписей, созданных с использованием сертификатов, выданных Удостоверяющим центром;
* консультирование пользователей по вопросам, связанным с получением услуг и использованием средств ЭП;
* выполнение иных функций Удостоверяющего центра в соответствии с Регламентом УЦ.

 **17. Нормативная, правовая и методическая база**

1. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».
2. Приказ ФСБ России №795 от 27 декабря 2011 года «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».
3. Приказ ФСБ России № 796 от 27.12.2011г. «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».
4. Приказ ФСБ России от 20.04.2021 г. №154 «Правила подтверждения владения ключом».
5. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 22.08.2017г. № 436 «Об утверждении Порядка формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».
6. Федеральный закон от 27.07.2006 г. № 152-ФЗ
«О персональных данных».
7. ГОСТ Р 34.10-2012. «Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
8. ГОСТ Р 34.11–2012 «Национальный стандарт Российской Федерации. Информационная технология. Информационная технология. Криптографическая защита информации. Функция хэширования».
9. Федеральный закон от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
10. Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».