**Техническое задание к закупке № 24060209023**

**на оказание услуг по предоставлению права использования программы для ЭВМ,**

**предназначенной для взаимодействия Заказчика с Удостоверяющим центром**

**для нужд ЧУЗ «Клиническая больница «РЖД-Медицина» г. Оренбург»**

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Наименование | Единица изм. | Кол-во |
| 1 | Оказание услуг по сопровождению деятельности администратора КЦР с выдачей сертификатаадминистратора КЦР по тарифному плану «Корпоративный» | шт | 1 |
| 2 | Лицензия на право использования СКЗИ "КриптоПро CSP" в составе сертификата ключа администратораКЦР | шт | 1 |
| 3 | Право использования программы для ЭВМ "АС "Кабинет УЦ" за использование при выпуске одного сертификата на физическое лицо | шт | 1000 |

Целью оказания Услуг является организация взаимодействия Заказчика с УЦ для получения Заказчиком и пользователями Заказчика СКПЭП, а также техническая поддержка Пользователей Заказчика в течение срока действия выданного СКЭП.

Сроки оказания Услуг: с момента заключения договора и до 31 декабря 2024года.

1.Состав услуг

Услуги оказываются на основании Договора и Технического задания. Состав, характеристики, качество и порядок оказания Услуг определяются настоящим Техническим заданием.

В рамках выполнения технического задания Исполнитель предоставляет Заказчику:

* неисключительное право использования КЦР;
* обеспечение доступа Заказчика в КЦР;
* оказание технической и методической поддержки Пользователей по вопросам использования КЦР, СКЗИ и ЭП сроком на 12 мес. с момента выдачи СКПЭП;
* услуги Удостоверяющего центра, указанные в п. 4.5.

2.1. После настройки КЦР и до 31 декабря 2024г. Администратор КЦР начинает использовать КЦР для взаимодействия с УЦ, направляя в УЦ заявки на выдачу СКПЭП, а Пользователи Заказчика получают в КЦР выданные УЦ СКПЭП.

2.2. Администратор КЦР при направлении заявок на выдачу СКПЭП самостоятельно контролирует содержание данных заявки, которые должны будут входить в состав обязательных полей СКПЭП. Состав данных заявки должен соответствовать требованиям, установленным в соответствии с Федеральным законом №63-ФЗ от 6 апреля 2011 г. «Об электронной подписи».

2.3. Выпуск сертификатов осуществляется посредством личного кабинета УЦ. Перевыпуск сертификата возможен после подписания заявления на выдачу сертификата с помощью действующего, в личном кабинете УЦ.

2.4. После получения СКПЭП в течение 12 месяцев Пользователи Заказчика получают техническую поддержку Исполнителя, согласно требованиям, установленным в п. 5. Технического задания.

 Объём оказываемых Услуг

Исполнитель должен предоставить неисключительное право использования программы, предназначенной для взаимодействия с УЦ в процессе выдачи СКПЭП, в объеме, позволяющем Заказчику получить в УЦ СКПЭП в количестве 101, в том числе:

* исполнитель выдает СКПЭП Администратора КЦР в количестве \_\_1\_\_ шт.;
* право использования программы для ЭВМ «АС «Кабинет УЦ» за использование при выпуске одного сертификата на физическое лицо в количестве 100 шт;

**Предоставить лицензии на право использования СКЗИ:**

* Лицензия на право использования СКЗИ «КриптоПро CSP» в составе сертификата ключа администратора КЦР в количестве 1 шт.

2. Основные требования к оказываемым Услугам

2.1. Требования к СКПЭП и ЭП

СКПЭП должны:

- соответствовать требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- соответствовать приказу ФСБ России от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;

- соответствовать криптографическим алгоритмам, определенным стандартами ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.

2.1.1. Требования к единой структуре сертификата ключа проверки электронной подписи.

СКПЭП должен представляет собой электронный документ, подписанный электронной подписью уполномоченного лица удостоверяющего центра, структура и содержание которого определяются:

- Федеральным законом Российской Федерации от 06.04.2011 № 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»;

- международными рекомендациями RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».

СКПЭП должен содержать:

- обязательные поля СКПЭП;

- расширения СКПЭП.

2.1.2. Требования к составу и содержанию расширений СКПЭП

В состав расширений СКПЭП должны входить следующие расширения:

- расширение «Использование ключа» (обязательное поле), поле должно содержать набор областей использования ключа: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных;

- расширение «Улучшенный ключ», поле должно содержит набор областей использования ключа. Набор областей должен включать следующие области:

проверка подлинности клиента (1.3.6.1.5.5.7.3.2);

защищенная электронная почта (1.3.6.1.5.5.7.3.4);

пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6).

- расширение «Идентификатор ключа субъекта» должно содержать идентификатор ключа владельца СКПЭП;

- расширение «Идентификатор ключа центра сертификатов», расширение должно содержать идентификатор ключа уполномоченного лица УЦ;

- расширение «Политики сертификата», расширение должно включать сведения о классе средств ЭП владельца СКПЭП;

- расширение «Точки распространения списков отзыва», расширение должно содержать URL-адрес точек распространения списков отозванных сертификатов по протоколу «http».

2.2. Требования к КЦР

Для организации приема и обработки запросов на выдачу СКПЭП, Исполнитель должен подключить ресурсы Заказчика к КЦР.

Внедрение КЦР необходимо Заказчику для автоматизации взаимодействия с УЦ Исполнителя и сокращения сроков получения СКПЭП.

2.2.1. КЦР должен располагать следующей функциональностью:

- разграничение доступа Администратора КЦР и Пользователей Заказчика к КЦР;

- предоставлять веб-интерфейс для выполнения операций по управлению жизненным циклом СКПЭП;

- возможность просмотра списка запросов на СКПЭП и списка выданных СКПЭП;

- возможность создания запроса на выдачу СКПЭП;

- возможность удаления запроса на СКПЭП;

- возможность редактирования данных при формировании запроса на выдачу СКПЭП, включаемых в СКПЭП;

- возможность контроля соответствия требованиям и ограничениям:

соответствие по формату полей;

соответствие скан-копиям документов,

проверка действительности документов по реквизитам (паспорт, СНИЛС);

- возможность печати заявления на выдачу сертификата ЭП;

- возможность скачивания бумажной копии СКПЭП;

- возможность скачивания открытого ключа СКПЭП;

- возможность загрузки/просмотра скан-копий документов;

- возможность ввода реквизитов скан-копий документов;

- возможность распознавания скан-копий документов;

- возможность генерации закрытого ключа в режиме ФКН (функционального ключевого носителя с защитой канала);

- возможность просмотра информации о выдаваемом СКПЭП;

- возможность уведомления Пользователей и Администраторов КЦР об изменениях статусов запроса на выдачу СКПЭП (по e-mail или СМС);

Предоставление инструкций по работе в КЦР. Уведомление об изменениях в КЦР (по email).

Выделенный номер технической поддержки.

Поддержка работы с КриптоПро CSP и ViPNet CSP.

2.2.2. Необходимая функциональность КЦР для Администратора КЦР:

- вход по логину и паролю (с обязательной двухфакторной аутентификацией по СМС – коду);

- вход по СКПЭП;

- возможность просмотра списка заявок на выдачу СКПЭП, списка выданных СКПЭП для пользователя;

- возможность просмотра баланса предоплаченных сертификатов;

- возможность создания заявки на перевыпуск сертификата юридического лица с реквизитами физического лица;

- возможность привязки заявки на сертификат физического лица к организации;

- возможность редактирования данных о Пользователе, обратившемся за СКПЭП;

- возможность загрузки/просмотра скан-копий документов (паспорт, СНИЛС, заявление на выдачу СКПЭП);

- возможность просмотра подробной истории действий по заявке;

- возможность выгрузки списка СКПЭП в Excel;

- возможность создания запросов на управление жизненным циклом СКПЭП в электронном виде и отправка их в УЦ;

- возможность формирования описи документов для отправки в УЦ;

- возможность отклонения и редактирования заявки, одобренной в УЦ;

- возможность оставлять заметки/комментарии к заявке;

- возможность поиска по данным заявки (ИНН, ФИО, по тексту заметки).

Возможность просмотра информации о месте установки СКПЭП:

- реестр ПК (до ветки реестра);

- ключевой носитель (до серийного номера);

- usb –носитель (до модели файловой системы);

- управление экспортируемостью сертификата до его выпуска.

- возможность уведомления администратора об окончании срока действия сертификата в самом сервисе.

2.2.3. Необходимая функциональность КЦР для Пользователей:

- вход по логину и паролю (с подтверждением доступа к персональным данным через СМС – код или действующий сертификат);

- вход по СКПЭП;

- возможность загрузки/просмотра скан-копий документов (паспорт, СНИЛС, заявление на выдачу СКПЭП);

- возможность подписи заявления на выдачу СКПЭП действующим СКПЭП пользователя;

- возможность оставлять заметки/комментарии к заявке;

- возможность ознакомления с информацией, содержащейся в СКПЭП под расписку, в соответствии с ФЗ№ 63 от 06.04.2011;

- возможность установки выпущенного СКПЭП на ключевой носитель;

- возможность просмотра списка своих заявок на выдачу СКПЭП, списка выданных СКПЭП;

- возможность копирования сертификата на рабочем месте пользователя посредством криптопровайдера;

- возможность проверки на соответствие требованиям используемых типов ключевых носителей.

- возможность уведомления пользователей об окончании срока действия сертификатов по еmail

4.2.3 Функциональность КЦР для проверки готовности АРМ Пользователя для работы

В КЦР должна быть функциональность, позволяющая проверить готовность АРМ Пользователя для работы с выдачей предупреждающего уведомления о необходимости установки программных компонент, недостающих для корректной работы с КЦР, СКЗИ, ключами ЭП и ЭП. Пользователю должна быть предоставлена возможность выбора действий по установке, позволяющая осуществить:

- настройку АРМ Пользователя и браузера для работы с СКПЭП;

- исправление расположения временной папки операционной системы АРМ Пользователя;

- отключение конфликтных служб с операционной системой АРМ Пользователя;

- отключение конфликтных надстроек браузера;

- отключение конфликтных программ в автозагрузке операционной системы АРМ Пользователя;

- изменение режима кеширования страниц браузера;

- установка корневых сертификатов УЦ;

- установка драйверов ключевых носителей;

- запуск службы «Автоматическое обновление» операционной системы;

- установка необходимого пакета обновлений операционной системы и браузера;

- запуск необходимых служб операционной системы;

- регистрация OID сертификатов для УЦ;

- установка сертификатов в хранилище «Личное» с ключевых носителей;

- возможность локальной загрузки на АРМ Пользователя необходимых компонентов для работы с СКПЭП;

- возможность уменьшения объема загружаемых файлов за счет анализа локально размещенных на рабочей станции установочных файлов и установленных программ;

- возможность самостоятельного выбора пользователем необходимых для установки компонентов.

Сервис должен функционировать в:

- ОС: Windows 8/10/2012 (32 или 64 бит);

- Интернет браузер: GoogleChrome, Opera, MozillaFirefox, Яндекс.Браузер.

 4.2.6 Требование к средствам криптографической защиты информации

Средства криптографической защиты информации должны обеспечивать:

- авторизацию и обеспечение юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии со стандартами ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-2012);

- аутентичность, конфиденциальность и имитозащиту соединений TLS;

- контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;

- управление ключевыми элементами системы в соответствии с регламентом средств защиты;

- реализацию протокола EAP/TLS;

- внешний интерфейс СКЗИ для обеспечения работы с функциональным ключевым носителем (ФКН), согласования ключей для использования в реализациях протокола IPSec, работы с другими приложениями.

Требования к действующим алгоритмам:

- алгоритм выработки значения хэш-функции должен быть реализован в соответствии с требованиями ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

- алгоритмы формирования и проверки электронной подписи должны быть реализованы в соответствии с требованиями ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

- при генерации закрытых и открытых ключей должна быть обеспечена возможность генерации с различными параметрами в соответствии ГОСТ Р 34.10-2012;

4.2.7 Требования к размеру ключей электронной подписи

- длина ключей электронной подписи:

закрытый ключ должен быть 256 бит,

открытый ключ должен быть 512 бит при использовании алгоритма ГОСТ Р 34.10-2012.

- длина ключей, используемых при шифровании:

закрытый ключ должен быть 256 бит,

открытый ключ должен быть 512 бит на базе алгоритма ГОСТ Р 34.10-2012,

симметричный ключ - 256 бит.

- длина ключей, используемых при шифровании:

закрытый ключ должен быть 256 бит,

открытый ключ должен быть 512 бит на базе алгоритма ГОСТ Р 34.10-2012,

симметричный ключ должен быть 256 бит.

 4.2.8 Требования к поддержке устройств хранения персональной ключевой и парольной информации

Средство криптографической защиты информации должно поддерживать работу с устройствами хранения персональной ключевой и парольной информации с USB-интерфейсом.

 4.2.9 Требования к сертификации.

Средство криптографической защиты информации должно иметь действующий сертификат соответствия требованиям ФСБ России к шифровальным (криптографическим) средствам класса не ниже КС1 и может использоваться для криптографической защиты информации (в том числе защиты TLS-соединений), не содержащей сведений, составляющих государственную тайну.

 3. Требования к типу лицензии

Заказчику должны быть предоставления неисключительные права в составе СКПЭП на использования СКЗИ сроком действия равным сроку СКПЭП.

 4.4 Требования к услугам удостоверяющего центра

В состав услуг УЦ, предоставляемых Исполнителем Заказчику, должны входить:

- выдача СКПЭП с информацией о сроке действия, с объектными идентификаторами;

- ограничение срока действия СКПЭП – 12 мес (если иное не предусмотрено законодательством);

- возможность создания ключа электронной подписи и ключа проверки электронной подписи Пользователем;

- прекращение действия СКПЭП;

- ведение реестра СКПЭП, обеспечение его актуальности и сохранности;

- проверка и обеспечение уникальности ключей проверки электронной подписи в реестре сертификатов;

- организацию и обеспечение исполнения требований к СКПЭП и электронной подписи согласно п. 4.1 ТЗ;

- удостоверение времени создания и/или подписания электронного документа,

- соответствие следующим стандартам: RFC 3161 Internet X.509 Public Key

Infrastructure. Time-Stamp Protocol (TSP).

- возможность проверки статуса СКПЭП в режиме реального времени,

работу по протоколу RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP).

 Требования к оказанию услуг

4.5 Требования к оказанию услуг УЦ

УЦ оказывает услуги в порядке и в сроки, установленные Регламентом (порядком) оказания услуг, публикуемым на общедоступном сайте УЦ в сети Интернет.

УЦ выполняет все функции и осуществляет все действия, предусмотренные 63-ФЗ.

№ п/п Состав услуг Время выполнения Период предоставления услуг

1. Выдача СКПЭП Не более 3 рабочих дней с момента предоставления пользователем Заказчика необходимых документов В режиме 24х7х365:

круглосуточно, без выходных дней

2 Ведение реестра СКПЭП Актуализация с периодичностью не менее, чем 1 раз в день. В режиме 24х7х365:

круглосуточно, без выходных дней

3 Аннулирование СКПЭП Не более 12 часов с момента поступления заявления на отзыв по форме, установленной Регламентом (порядком) оказания услуг УЦ В режиме 24х7х365:

круглосуточно, без выходных дней

4 Оказание услуг по сопровождению деятельности администратора КЦР с выдачей сертификата администратора КЦР по тарифному плану «Корпоративный»

4.1 Техническая поддержка Согласно пункту 5 настоящего ТЗ. В режиме 24х7х365:

круглосуточно, без выходных дней

4.2 Изготовление квалифицированного Сертификата Администратора на уполномоченное лицо Заказчика сроком действия один год. Выпуск сертификата Администратора сроком на 1 год по месту нахождения Исполнителя или Заказчика (согласно условиям ТЗ). В режиме 8х5х365:

в рабочие дни Исполнителя

4.3 Сопровождение Сертификата Администратора. Возможность производить смену и отзыв (прекращение действия) Сертификата в течение срока действия этого Сертификата (не более трех раз). Срок действия каждого вновь выданного Сертификата в рамках настоящих услуг ограничивается сроком действия первого Сертификата

 В режиме 8х5х365:

в рабочие дни Исполнителя

4.4 Ускоренная проверка формы заявки на выпуск сертификата Администратора Проверка всех фактов соответствия сведений в Заявлении на выдачу Сертификата в течение 2 часов с момента представления всех необходимых документов

 В режиме 8х5х365:

в рабочие дни Исполнителя

4.5 Возможность назначения неограниченного количества дополнительных Администраторов с доступом по логину и паролю для работы в АС «Кабинет УЦ» на время действия Сертификата Администратора с возможностью настройки различных прав по использованию «АС «Кабинет УЦ» В режиме 8х5х365:

в рабочие дни Исполнителя

5 Требования к оказанию услуг технической поддержки

5.1.1 Общие положения

Услуги технической поддержки оказываются Исполнителем.

Исполнитель в рамках технического сопровождения должен организовать горячую линию для обращений Заказчика:

- горячая линия Исполнителя должна обеспечивать Заказчику возможность оперативно получать консультации по вопросам использования, установки и настройки СКПЭП, выданных Исполнителем, в рамках областей их применения;

- горячая линия должна работать круглосуточно, без выходных дней, в режиме 24х7х365;

- при необходимости и с согласия Заказчика консультации должны оказываться при помощи технологий удалённого доступа.

5.1.2 Требования к оказанию услуг по телефону

Исполнитель должен обеспечить единую точку входа для телефонных обращений Заказчика. Номер телефона должен принадлежать пулу адресов ТфОП населенного пункта размещения Заказчика или префиксу 8-800.

Исполнитель должен обеспечивать уровень обслуживания не ниже 80/90 (ожидание ответа у 80% обращений абонентов составляет не более 90 секунд).

Исполнитель должен обеспечить соединение Заказчика с консультантом Исполнителя со следующими количественными характеристиками (с момента соединения с консультантом Исполнителя):

- консультант Исполнителя должен поднимать трубку звонящего телефона не позднее пятого звонка (не более чем через 10 секунд). Консультант Исполнителя должен представиться (фамилия, имя);

- каждое обращение Заказчика должно фиксироваться:

должна производиться аудиозапись каждого обращения Заказчика,

в случае если, проблему не удалось решить сразу, Заказчику должен сообщаться номер обращения, либо внутренний номер консультанта Исполнителя и сроки решения проблемы.

Заявки от Заказчика, требующие для решения привлечения дополнительных специалистов Исполнителя, должны переводиться на соответствующие отделы сразу после обращения. Информация о ходе решения должна быть сообщена Заказчику не позднее суток с момента его последнего обращения.

Консультант Исполнителя должен доводить решение проблемы Заказчика до логического завершения (Заказчик подтверждает решение проблемы).

5.1.3 Требования к оказанию услуг через веб-сайт (Онлайн-консультант)

Онлайн-консультант должен располагаться на сайте Исполнителя, каждый ответ от специалиста Исполнителя должен содержать ФИО консультанта.

5.1.4 Требования к оказанию услуг по почте

Исполнитель должен обеспечить единую точку входа для обращений по электронной почте.

Обработка почты должна вестись в режиме 24/7/365.

Ответ Исполнителя должен отправляться не позднее 2-х часов с момента поступления письма Заказчика. Если решение требует привлечения дополнительных сотрудников Исполнителя, то в ответе должен быть указан номер обращения и сроки решения проблемы.

Каждый ответ от специалиста Исполнителя должен содержать всю контактную информацию: ФИО, телефон, внутренний номер, должность.

Ответ на официальный письменный запрос Заказчика по почте должен предоставляться не позднее чем через 30 календарных дней с момента поступления обращения.

6 Требования к Исполнителю

Исполнитель должен иметь лицензию Федеральной службы безопасности Российской Федерации на осуществление разработки, производства, распространения 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, при условии наличия в данной действующей лицензии следующих работ (видов деятельности), предусмотренных пунктами: 12, 15, 20, 21, 24, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, являющихся приложением к Положению, утвержденному Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313;

Исполнитель должен являться УЦ и быть аккредитован требованиям 63-ФЗ.

Исполнитель должен выполнять требования 152-ФЗ и иных нормативных документов по защите ПДн и должен быть включен в реестр операторов, осуществляющих обработку персональных данных.

Исполнитель должен заключить с Заказчиком лицензионный/сублицензионный договор на передачу права использования программы для ЭВМ.

Программное обеспечение должно содержаться в Едином реестре российских программ для ЭВМ и баз данных.

Предоставление Услуг должно осуществляться в соответствии с регламентом УЦ, Договора и Технического задания.

**Начальная максимальная цена договора, порядок формирования цены:** **136 200** (сто тридцать шесть тысяч двести) рублей **00** копеек с НДС

Порядок формирования цены договора: Стоимость услуг включает в себя все затраты, издержки и иные расходы Исполнителя, в том числе сопутствующие, связанные с исполнением настоящего Договора.

Форма оплаты - безналичный расчет производится Заказчиком путем перечисления денежных средств на расчетный счет Исполнителя.

Срок и порядок оплаты оказанных услуг: в течение 15 (пятнадцати) календарных дней с даты оказания услуг и получения Заказчиком оригинального комплекта документов подписанного со стороны Исполнителя: счета на оплату, актов оказания услуг (2 экз.).