**Техническое задание**

**на оказание услуг по изготовлению квалифицированных сертификатов ключей проверки электронной подписи**

1. **Термины и определения**

|  |  |
| --- | --- |
| Термин / Сокращение | Описание / Определение / Расшифровка |
| Заказчик | Частное учреждение здравоохранения "Клиническая больница "РЖД-Медицина" города Самара" |
| 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. |
| Исполнитель | Организация, оказывающая услуги по созданию ключей, изготовлению сертификатов ключей проверки электронных подписей и выполнению иных функций, предусмотренных настоящим Техническим заданием и условиями контракта |
| Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) | Сертификат ключа проверки электронной подписи, соответствующий требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» и иным принимаемым в соответствии с ним нормативно правовым актам, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи |
| 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) 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 | Потребитель услуг по созданию и выдаче сертификатов ключей проверки электронных подписей |
| Сертификат ключа проверки электронной подписи (сертификат) | Электронный документ или документ на бумажном носителе, выданный УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи |
| СКЗИ | 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 |
| ТЗ | Техническое задание |
| Удостоверяющий центр (УЦ) | Юридическое лицо или индивидуальный предприниматель, 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 |

1. **Объект закупки**
* оказание услуг Удостоверяющего центра (далее – УЦ) по формированию ключей электронной подписи, а также изготовлению и выдаче квалифицированных сертификатов ключей проверки электронных подписей (далее - сертификаты), соответствующих требованиям приказа ФСБ России от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи", Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;
* организация удаленного взаимодействия пользователей с Исполнителем (обслуживающим персоналом УЦ) в процессе оказания услуг посредством сервисов информационной системы УЦ, обеспечивающих возможность формирования заявок на изготовление ключей электронной подписи и сертификатов / самостоятельной генерации пользователями ключей электронной подписи и запросов на сертификаты формата PKCS#10, передачу в УЦ регистрационных данных пользователей, выдачу пользователям сертификатов, изготовленных на основании сформированных заявок / запросов на сертификаты, и учет выданных сертификатов.
1. **Наименование, цели и объем оказываемых услуг, требования к оказанию услуг.**
	1. **Цель оказания услуг:**

 Обеспечение Заказчика ключами электронной подписи и квалифицированными сертификатами в максимальном количестве 160 штук для оформления электронных больничных листов и работе в системе Фонда социального страхования.

* 1. **Место оказания услуг:**
* Процедура выпуска сертификатов должна осуществляться через информационную систему УЦ Исполнителя с возможностью контроля процесса создания сертификатов.
* Правила предоставления услуги должно определяться в соответствии с Регламентом оказания Удостоверяющим центром услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей (далее - Регламент УЦ) и условиями договора.
	1. **Сроки исполнения:**
* Квалифицированные сертификаты ключей проверки электронной подписи должны быть изготовлены и переданы Заказчику в течение 10 (десяти) рабочих дней с момента получения от Заказчика заявки на изготовление и предоставления Исполнителю документов, необходимых для изготовления сертификатов. Заявка имеет силу для сторон как в случае ее передачи исполнителю путем вручения документа, так и при ее передаче в электронном виде средствами компьютерной и иной связи.
* Заявки на изготовление сертификатов поступают от Заказчика в течение срока действия договора (партиями или по одной) по мере необходимости, в общем количестве, не превышающем 160 шт.
* Срок действия квалифицированного сертификата ключа проверки электронной подписи, создаваемого УЦ, должен составлять 12 месяцев с момента его изготовления.
	1. **Состав услуг:**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование**  | **Характеристики**  | **Кол-во,ед.** |
| 1 | Изготовление сертификата ключа проверки электронной подписи для *юридического лица* (срок действия сертификата - 12 месяцев). | Сертификат должен быть изготовлен на юридическое лицо и должен содержать:- наименование и регистрационные данные юридического лица,- ФИО уполномоченного представителя ЮЛ, его СНИЛС.  | не более 160 |
| 3 | Срок изготовления и выдачи сертификата ключа проверки электронной подписи  | Не более 10 рабочих дней с момента предоставления Заказчиком необходимых документов Исполнителю. | В режиме 8х5:с 09:00 до 18:00, в рабочие дни Заказчика |
| 4 | Гарантийное сопровождение, включающее в себя:- ведение реестра выданных и аннулированных сертификатов ключей проверки электронной подписи;- аннулирование сертификата ключа проверки электронной подписи;- выполнение иных функций Удостоверяющего центра в соответствии с Регламентом УЦ. | Актуализация с периодичностью не менее 1 раза в день.Не более 12 часов с момента поступления необходимых сведений от Заказчика. | В режиме 24х7х365:круглосуточно, без выходных дней |
| 5 | Техническая поддержкапо телефонам «горячей линии» и электронной почте | Консультирование по вопросам установки и настройки средств электронной подписи, а также использования сертификатов, выданных Исполнителем. | В режиме 8х5:с 09:00 до 18:00, в рабочие дни Заказчика / 24x7х362: круглосуточно, без выходных дней |

 **4. Требования к программно-аппаратному комплексу и информационной системе Удостоверяющего центра**

 **4.1. Требования к Удостоверяющему центру**

 Квалифицированные электронные подписи, обеспечивающие юридическую значимость электронного документооборота Заказчика, формируются с использованием квалифицированных сертификатов, создаваемых аккредитованным УЦ Исполнителя в рамках оказания услуг по изготовлению и выдаче квалифицированных сертификатов.

Программно-аппаратный комплекс УЦ, обеспечивающий выполнение целевых функций, должен быть сертифицирован ФСБ России в соответствии с порядком, установленным законодательством Российской Федерации, по классу не ниже, чем КС3 / КС2.

Программно-аппаратный комплекс УЦ для изготовления 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, ГОСТ Р 34.11-94;**
* выполнение следующих базовых функций:
* генерация ключей УЦ;
* формирование корневых сертификатов УЦ;
* регистрация пользователей УЦ;
* регистрация и обработка запросов на изготовление сертификатов формата PKCS#10;
* контроль уникальности ключей электронной подписи в запросах на сертификаты;
* формирование 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, изданных Удостоверяющим центром, в соответствии с Приказом Министерства связи и массовых коммуникаций Российской Федерации от 22.08.2017г. № 436;
* возможность формирования по заявкам 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 TSP); cлужба TSP должна обеспечивать:
* удостоверение времени создания и/или подписания электронного документа;
* соответствие стандартам RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).

Информационная система Удостоверяющего центра должна обеспечивать удобный интерфейс взаимодействия (Web-интерфейс) с пользователями в процессе оказания услуг по изготовлению и выдаче сертификатов.

 **4.2. Требования к информационной системе Удостоверяющего центра, обеспечивающей взаимодействие с пользователями**

* Интерфейс взаимодействия информационной системы Удостоверяющего центра должен обеспечивать следующую функциональность:
* *авторизация пользователей* – аутентификация и авторизация пользователя информационной системы УЦ;
* *регистрация и обработка заявок* – выполнение порядка последовательности действий̆ по выпуску сертификатов;
* *оповещения* – отправка уведомлений о ходе регистрации заявок на электронную почту пользователям информационной системы УЦ (уведомления об авторизации пользователя, о формировании пользователем запроса на сертификат, о необходимости пройти верификацию, о завершении заявки.) Письма должны приходить как пользователю, так и ответственному сотруднику;
* *формирование реестра выданных сертификатов* – обеспечивается функциональность в части ведения реестра всех созданных сертификатов по сотрудникам организации, в том числе с возможностью его выгрузки на внешние запоминающие устройства;
* Информационная система Удостоверяющего центра должна обеспечивать взаимодействие пользователей̆ (сотрудников организации / ответственного сотрудника организации) с Удостоверяющим центром (службами регистрации в пунктах обслуживания Исполнителя) в процессе создания ключей̆ электронной̆ подписи и получения квалифицированных сертификатов без необходимости посещения пункта обслуживания Исполнителя, путем предоставления удобного Web-интерфейса взаимодействия организации и Исполнителя.
* Интерфейс взаимодействия должен быть реализован в виде системы Личных кабинетов, которые, в зависимости от настройки, могут предоставляться как персонально каждому сотруднику организации, так и лицу, ответственному за информационную безопасность организации и выступающему от имени всех остальных сотрудников.
* Через Личные кабинеты информационной̆ системы УЦ должно обеспечиваться выполнение следующей функциональности:
* подача заявок на генерацию ключей̆ электронной̆ подписи и изготовление сертификатов;
* возможность самостоятельной генерации пользователем ключей̆ электронной̆ подписи и передача в УЦ запросов на сертификаты формата PKCS#10;
* передача регистрационных данных пользователей и скан-копий документов, необходимых для изготовления сертификатов;
* прием из УЦ изготовленных сертификатов и их запись на ключевой носитель (опционально);
* учет сформированных запросов на сертификаты и выданных сертификатов;
* отслеживание статуса заявок и срока действия выпущенных сертификатов;
* протоколирование действий пользователя и процессов, связанных с изготовлением сертификатов.
* По запросу Заказчика информационная система Удостоверяющего центра должна обеспечивать возможность формирования отчетов о полученных заявках и выпущенных сертификатах в виде таблицы со следующим набором полей:
* номер заявки на изготовление ключа электронной подписи и сертификата;
* дата размещения заявки;
* реквизиты организации - заявителя;
* ФИО владельца сертификата – сотрудника организации;
* контактные данные владельца сертификата;
* статус заявки;
* статус сертификата;
* серийный номер сертификата;
* срок действия сертификата.
	1. **Требования к СКЗИ на рабочих местах пользователей**
* Ключи электронных подписей и запросы на сертификаты должны изготавливаться с использованием сертифицированных ФСБ России средств криптографической защиты информации и иметь совместимость с криптопровайдером, используемым у Заказчика, а именно «Крипто Про CSP».
* 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 генерации ключей электронной подписи для алгоритмов ГОСТ Р 34.10-2012.
* СКЗИ должно обеспечивать поддержку операционных систем на базе ОС Windows.
	1. **Требования к ключевому носителю**

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

 Ключевой носитель предоставляется Заказчиком.

* 1. **Порядок изготовления сертификатов**

 Регистрация в УЦ пользователей и изготовление 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 Личные кабинеты информационной системы УЦ.

 Автоматизированный режим регистрации запросов и формирования сертификатов на основе регистрационных данных, поступающих в УЦ через Личные кабинеты Пользователей (сотрудников организации) / ответственных сотрудников организации, возможен только в том случае, если процедура удостоверения личности и проверка регистрационных данных владельцев сертификатов выполняется в полном соответствии с требованиями Закона № 63-ФЗ.

* 1. **Требования к безопасности**

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.

* 1. **Требования к техническому сопровождению**

В рамках технического сопровождения Исполнитель оказывает консультирование специалистов Заказчика по вопросам использования, установки и настройки сертификатов, выданных Исполнителем, а также по вопросам, связанным с получением услуг и использованием средств ЭП:

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

 Исполнитель обязан обеспечить гарантийное сопровождение выданных квалифицированных сертификатов в течение 1 года, начиная со дня, следующего за днем выпуска ключей и сертификатов, в соответствии с требованиями ТЗ.

Гарантийное сопровождение сертификатов включает:

* аннулирование сертификатов;
* ведение реестра выданных и аннулированных сертификатов в соответствии с требованиями Приказа 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»;
* проверку по обращениям Заказчика электронных подписей, сформированных с использованием сертификатов, выданных Исполнителем;
* консультирование пользователей по вопросам, связанным с получением услуг и использованием средств ЭП.