Приложение 1

к извещению об осуществлении закупки

**Описание объекта закупки**

**1.** **Предмет муниципального контракта**: оказание услуг по передаче неисключительных прав на использование программного обеспечения «КриптоПро».

**2.** **Требования к предоставляемым услугам:**

2.1. Срок оказания услуг сопровождения программного обеспечения - не менее 12 (двенадцати) месяцев с даты подписания Заказчиком документа о приёмке, предусмотренного муниципальным контрактом.

2.2. Тип поставки программного обеспечения - электронный.

2.3. Во исполнение требований пункта 1 части 1 статьи 12 Федерального закона Российской Федерации от 04 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности» и постановления 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)» Исполнитель должен иметь действующую лицензию ФСБ России на распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств.

**3. Перечень предоставляемых услуг:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Код ОКПД2/ КТРУ | Наименование услуг | Характеристика предоставляемых услуг | Кол-во |
| 1 | 58.29.50.000 | Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение | Лицензия на право использования средства криптографической защиты информации "КриптоПро CSP" версии 5.0R2 на одном рабочем месте, бессрочно. Эквивалент не предусмотрен в соответствии с приказом ФНС России от 27.03.2024 №ЕД-7-26/245@, в связи с принятием Федерального закона от 31.07.2023 №389-ФЗ "О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и о приостановлении действия абзаца второго пункта 1 статьи 78 части первой Налогового кодекса Российской Федерации" | 5 штук |

Предоставляемые услуги включены в поз. 146 приложения 1 к постановлению Правительства Российской Федерации от 23.12.2024 № 1875 «О мерах по предоставлению национального режима при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок товаров, работ, услуг отдельными видами юридических лиц».

**4. Требования к программному обеспечению.**

4.1. Средство криптографической защиты информации должно быть сертифицировано ФСБ России по требованиям:

• к средствам электронной подписи;

• к шифровальным (криптографическим) средствам защиты конфиденциальной информации, по классу КС1, КС2.

4.2. Применяемое средство криптографической защиты информации (средство электронной подписи) должно обеспечивать применение электронной подписи (ЭП) и шифрования в соответствии с нормами действующего законодательства Российской Федерации и осуществлять выполнение следующих основных функций:

- генерацию и управление ключевой информацией;

- формирование электронной подписи в соответствии с ГОСТ Р 34.10-2012 и ГОСТ 34.10-2018;

- подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2012;

- подсчет значения хеш-функции в соответствии с ГОСТ Р 34.11-2012 и ГОСТ 34.11-2018;

- шифрование и расшифрование данных в соответствии с ГОСТ 34.12-2018 и ГОСТ 34.13-2018;

- формирование ключей электронной подписи и ключей проверки электронной подписи, а также ключей шифрования;

- идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений;

- реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов.

4.3. Требования к реализации программного интерфейса встраивания.

Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP).

Встраивание средства криптографической защиты информации (средства электронной подписи) в прикладную информационную систему должно предусматривать возможность:

- Применения в операционных системах семейства Microsoft Windows интерфейса функций CAPICOM, Certificate Enrollment Control, Certificate Enrollment API, Certificate Services;

- вызова функций средства криптографической защиты информации (средства электронной подписи);

- применения в стандартном прикладном программном обеспечении операционных систем семейства Microsoft Windows MS Outlook Express; MS IE; MS IIS; Outlook, и т.д. (для поддержки MS Office Word, Excel может требоваться дополнительное ПО от разработчика средство криптографической защиты информации (средство электронной подписи)).

4.4. Требования к алгоритмам, сертификатам открытых ключей и поддерживаемым форматам криптографических сообщений.

Применяемое средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 34.12-2018 и ГОСТ 34.13-2018 с учетом RFC 4357 «Additional Cryptographic Algorithms for Use with ГОСТ 34.12-2018 и ГОСТ 34.13-2018, GOST R 34.10-2012, and GOST R 34.11-2012 Algorithms», ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2018, ГОСТ Р 34.10-2018.

Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 «Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile» с учетом RFC 4491, GOST R 34.10-2012, ГОСТ Р 34.11-2012 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».

Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать формат криптографических сообщений согласно RFC 3852 «Cryptographic Message Syntax (CMS)» с учетом RFC 4490 «Using the ГОСТ 34.12-2018 и ГОСТ 34.13-2018, ГОСТ Р 34.11-2012, GOST R 34.10-2012 Algorithms with Cryptographic Message Syntax (CMS)», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 34.12-2018 и ГОСТ 34.13-2018, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS».

Применяемое средство криптографической защиты информации (средство электронной подписи) должно поддерживать возможность создания форматов криптографических сообщений типа CAdES в соответствии с ETSI TS 101 733 (Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)):

- формата CAdES-BES;

- формата CAdES–T;

- формата СAdES-X Long Type 1,

а также формата XML DSign для формирования электронной подписи в XML при встраивании в прикладные информационные системы с использованием программных библиотек (SDK) от разработчика средства криптографической защиты информации (средство электронной подписи). Отдельные компоненты таких программных библиотек могут лицензироваться дополнительно.

4.5. Требования к составу.

Комплектация исполнения средства криптографической защиты информации (средства электронной подписи) должна включать:

- Модуль сетевой аутентификации TLS, обеспечивающий реализацию сетевого протокола TLS с использованием российских криптографических стандартов (возможности модуля TLS определяются типом лицензии на средство криптографической защиты информации (средство электронной подписи));

- модуль реализации набора протоколов IPsec с использованием отечественных криптографических алгоритмов, включая библиотеки IKE, ESP, AH (лицензируется отдельно);

- модуль Winlogon для аутентификации пользователей в домене Microsoft Windows (лицензируется отдельно);

- модуль, обеспечивающий реализацию криптографических операций в Java-приложениях, посредством использования средства криптографической защиты информации (средства электронной подписи) (лицензируется отдельно);

- приложение командной строки обеспечивающее формирование запросов на создание сертификатов, хэширование, шифрование и расшифрование файлов, создание и проверку электронной подписи файлов, в том числе в формате криптографических сообщений типа CAdES (лицензируется отдельно);

- модуль построения защищенного TLS-канала между произвольными серверами и рабочими местами пользователей с установленным средством криптографической защиты информации (средством электронной подписи), реализует прием (инкапсуляцию) незащищенного трафика от произвольного приложения или службы на клиентском компьютере (рабочем месте), его шифрование и дальнейшую передачу по протоколу TLS с последующем расшифровыванием на удаленном компьютере.

4.6. Функциональные требования.

Средство криптографической защиты информации (средство электронной подписи) должно предоставлять программный интерфейс для выполнения следующих основных функций:

- формирование электронной подписи на рабочем месте пользователя;

- подтверждение подлинности электронной подписи на рабочих местах пользователей;

- подсчет значения хеш-функции данных на рабочих местах пользователей;

- шифрование и расшифрование данных на рабочем месте пользователя;

- формирование ключей электронной подписи и ключей проверки электронной подписи на рабочем месте пользователя;

- поддержка аппаратных средств визуализации подписываемой информации, включая форматы подписи таких аппаратных устройств (типа Рутокен PinPad).

Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать выполнение следующих сервисных функций:

- установка личных сертификатов и ключей проверки электронной подписи на рабочем месте с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;

- копирование и удаление ключей электронной подписи;

- установка, изменение и удаление пароля на доступ к закрытому ключу.

- создание и проверка электронной подписи в формате CMS (присоединенной и отсоединенной) с использованием графического интерфейса пользователя;

- Установка параметров работы в режиме «Облачного провайдера», включая определение сетевых адресов подключения, установку сертификатов ключей проверки электронной подписи, хранящихся в «облачном токене».

4.7. Требования к общесистемному программному обеспечению.

Средство криптографической защиты информации (средство электронной подписи) должно включать варианты исполнений, функционирующих в среде следующих операционных систем:

- Windows XP/7/8/8.1/10 (x86, x64);

- «Альт 8 СП» Рабочая станция / релиз 8 (x86, x64);

Red Hat Enterprise Linux Desktop;

Apple Mac OS X;

Red Hat Enterprise Linux Workstation.

4.8. Требования к поддерживаемым ключевым носителям.

Средство криптографической защиты информации (средство электронной подписи) должно поддерживать следующие носители:

1. Пассивные носители, предназначенные для хранения ключей электронной подписи и их передачи в операционную систему с установленным средством криптографической защиты информации (средством электронной подписи) для создания электронной подписи и выполнения прочих операций.

2. Активные носители, предназначенные для хранения неизвлекаемых ключей электронной подписи без возможности их передачи в операционную систему с установленным средством криптографической защиты информации (средством электронной подписи).

3. Функциональные ключевые носители, предназначенные для хранения неизвлекаемых ключей электронной подписи с защитой канала связи с ключевым носителем с помощью протокола выработки общего ключа с аутентификацией на основе пароля – протокола SESPAKE.

4. Сетевые программно-аппаратные комплексы для централизованного хранения неизвлекаемых ключей и создания электронной подписи («облачный токен»).

4.9. Требования к поддерживаемым стандартным приложениям и службам операционных систем.

Средство криптографической защиты информации (средство электронной подписи) должно поддерживаться следующими стандартными приложениями и службами операционных систем:

- Клиент электронной почты - Microsoft Outlook (из состава Microsoft Office 2003/2007/2010/2013/2016);

- Клиент электронной почты - Microsoft Outlook Express в составе Internet Explorer/Microsoft Edge, Почта Windows Mail, Live Mail;

- Microsoft Word, Excel из состава Microsoft Office 2003/2007/2010/2013/2016 (c помощью специализированного плагина от производителя средства криптографической защиты информации (средства электронной подписи) для Microsoft Office – лицензируется отдельно);

- Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode;

- Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Microsoft Internet Explorer/Microsoft Edge – web-сервер IIS, TLS-сервер, TLS-клиент (IE);

- Служба доменной аутентификации Winlogon в составе Microsoft Windows (с помощью специализированного модуля в составе средства криптографической защиты информации (средства электронной подписи) – лицензируется отдельно);

- Microsoft ISA сервер;

- Сервер Microsoft TMG;

- Сервер Microsoft UAG;

- Стандартная служба шифрования данных на жёстком диске компьютера (рабочего месте) Microsoft Encrypt File System (Microsoft EFS) (c помощью специализированного ПО от производителя средства криптографической защиты информации (средства электронной подписи) для Microsoft Windows – лицензируется отдельно).

Согласовано:

Контрактная служба: О.В. Дергилев