**Техническое задание**

**1. Заказчик:**

ЧУЗ "РЖД-Медицина" г. Орехово-Зуево"

**2. Перечень поставляемых услуг:** Оказание услуг по предоставлению неисключительных (пользовательских) прав на использование средства криптографической защиты информации.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование | Технические требования | Кол-во | Ед.изм |
| 1 | Лицензия на право использования СКЗИ КриптоПро CSP версии 5.0 (бессрочная) | Лицензия на право использования программного обеспечения (права на программу для ЭВМ) именная, корпоративная, для рабочих станций со следующими характеристиками:**Назначение КриптоПро CSP**Формирование и проверка электронной подписи.Обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты.Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS, и IPsec.Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования.**Поддерживаемые алгоритмы**В КриптоПро CSP 5.0 наряду с российскими реализованы зарубежные криптографические алгоритмы. Теперь пользователи имеют возможность использовать привычные носители ключей для хранения секретных ключей RSA и ECDSA.**Электронная подпись**ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001, ECDSA, RSAХэш-функцииГОСТ Р 34.11-2012, ГОСТ Р 34.11-94, SHA-1, SHA-2**Шифрование**ГОСТ Р 34.12-2015 (Кузнечик и Магма), ГОСТ 28147-89, AES, DES, 3DES, RC2, RC4Таблица алгоритмов, поддерживаемых разными версиями КриптоПро CSP.**Поддерживаемые технологии хранения ключей**Облачный токенВ криптопровайдере КриптоПро CSP 5.0 впервые появилась возможность использования ключей, хранящихся на облачном сервисе КриптоПро DSS, через интерфейс CryptoAPI. Теперь ключи, хранимые в облаке, могут быть легко использованы как любыми пользовательскими приложениями, так и большинством приложений компании Microsoft.Носители с неизвлекаемыми ключами и защищенным обменом сообщениямиВ КриптоПро CSP 5.0 добавлена поддержка носителей с неизвлекаемыми ключами, реализующих протокол SESPAKE, позволяющий провести аутентификацию, не передавая в отрытом виде пароль пользователя, и установить шифрованный канал для обмена сообщений между криптопровайдером и носителем. Нарушитель, находящийся в канале между носителем и приложением пользователя, не может ни украсть пароль при аутентификации, ни подменить подписываемые данные. При использовании подобных носителей полностью решается проблема безопасной работы с неизвлекаемыми ключами.Компании Актив, ИнфоКрипт, СмартПарк, Аладдин Р.Д. и Gemalto разработали новые защищенные токены, которые поддерживают данный протокол.Носители с неизвлекаемыми ключамиМногие пользователи хотят иметь возможность работать с неизвлекаемыми ключами, но при этом не обновлять токены до уровня ФКН. Специально для них в провайдер добавлена поддержка популярных ключевых носителей Рутокен ЭЦП 2.0, JaCarta-2 ГОСТ и InfoCrypt VPN-Key-TLS.Классические пассивные USB-токены и смарт-картыБольшинство пользователей предпочитает быстрые, дешевые и удобные решения для хранения ключей. Как правило, предпочтение отдаётся токенам и смарт-картам без криптографических сопроцессоров. Как и в предыдущих версиях провайдера, в КриптоПро CSP 5.0 сохранена поддержка всех совместимых носителей производства компаний Актив, Аладдин Р.Д., Gemalto/SafeNet, Multisoft, NovaCard, Rosan, Alioth, MorphoKST и СмартПарк.Кроме того, поддерживаются способы хранения ключей в реестре Windows, на жестком диске, на флеш-накопителях на всех платформах.**Поддерживаемое программное обеспечение**КриптоПро CSP позволяет быстро и безопасно использовать российские криптографические алгоритмы в следующих стандартных приложениях:офисный пакет Microsoft Office;почтовый сервер Microsoft Exchange и клиент Microsoft Outlook;продукты Adobe Systems Inc.;браузеры Яндекс.Браузер, Спутник, Internet Explorer, Edge;средство формирования и проверки подписи приложений Microsoft Authenticode;веб-серверы Microsoft IIS, nginx, Apache;средства удаленных рабочих столов Microsoft Remote Desktop Services;Microsoft Active Directory.**Интеграция с платформой КриптоПро**С первого же релиза обеспечивается поддержка и совместимость со всеми нашими продуктами:КриптоПро УЦ;Службы УЦ;КриптоПро ЭЦП;КриптоПро IPsec;КриптоПро EFS;КриптоПро .NET;КриптоПро Java CSP.КриптоПро NGate**Операционные системы и аппаратные платформы**Microsoft Windows;Mac OS;Linux;FreeBSD;Solaris;AIX;iOS;Android;Sailfish OS.аппаратных платформ:Intel / AMD;PowerPC;ARM;MIPS (Байкал);VLIW (Эльбрус);Sparc.и виртуальных сред:Microsoft Hyper-VVMWareOracle Virtual BoxRHEV.**Интерфейсы для встраивания**Для встраивания в приложения на всех платформах КриптоПро CSP доступен через стандартные интерфейсы для криптографических средств:Microsoft CryptoAPI;PKCS#11;OpenSSL engine;Java CSP (Java Cryptography Architecture)Qt SSL.**Пользовательский интерфейс – русский.** | 6 | шт. |
| 2 | Лицензия на право использования ПО «Крипто АРМ Стандарт Плюс» версии 5 на одном рабочем месте (бессрочная)  | Лицензия на право использования программного обеспечения (права на программу для ЭВМ) именная, корпоративная, для рабочих станций со следующими характеристиками:КриптоАРМ - программа для защиты электронных документов. Используется для создания и проверки электронной подписи (в т.ч. усиленной квалифицированной электронной подписи), шифрования и расшифрования файлов, генерации ключей электронной подписи, создания самоподписанных сертификатов.КриптоАРМ Стандарт Плюс - расширенная версия программы КриптоАРМ. В отличие базовой версии, в "плюсе" поддерживается взаимодействие с ключевыми носителями (токенами, смарт-картами) с аппаратной реализацией криптографии. Работа с такими устройствами осуществляется через интерфейс PKCS#11. Примеры поддерживаемых устройств: JaCarta ГОСТ и Рутокен ЭЦП в разных форм-факторах, в виде USB-токенов или смарт-карт.**Операционные системы:**Windows 2003, XP, Vista, 7, 8, 8.1, 10 (32 и 64 бит)**Криптопровайдеры:**КриптоПро CSP 3.6 и выше, VipNet CSP, Signal-COM CSP**Ключевые носители:**Рутокен ЭЦП, JaCarta ГОСТ, JaCarta PKI/ГОСТ, eToken ГОСТ**Срок действия лицензии: Бессрочная****Пользовательский интерфейс – русский.** | 2 | шт. |

**3. Срок поставки товара:** 10 (десять) рабочих дней с даты заключения Договора.

**4. Место поставки товара:** Московская область, г. Орехово-Зуево, ул. Ленина, д. 22