МИНИСТЕРСТВО
ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
**ГОСУДАРСТВЕННОЕ
УНИТАРНОЕ ПРЕДПРИЯТИЕ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
«ЛУГАНСКИЙ
НАУЧНО- ПРОИЗВОДСТВЕННЫЙ
ЦЕНТР МЕТРОЛОГИИ,
СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ»
(ГУП ЛНР «ЛУГАНСКСТАНДАРТМЕТРОЛОГИЯ»)**

Тимирязева ул., д.50, г. Луганск, г.о.город Луганск,
Луганская Народная Республика, 291021,
тел. +7(8572) 34 68 92, E-mail: mail@csmlg.org
ОГРН 1229400057886, ИНН 9402008327,
КПП 940201001

25.09.2024 № 1774/03
На №_____ от_____

Руководителям предприятий,
юридическим лицам,
индивидуальным
предпринимателям и частным
лицам

ЗАПРОС НА ПРЕДОСТАВЛЕНИЕ ЦЕНОВОЙ ИНФОРМАЦИИ (КОММЕРЧЕСКОГО ПРЕДЛОЖЕНИЯ)

Заказчик ГУП ЛНР «ЛУГАНСКСТАНДАРТМЕТРОЛОГИЯ» для определения начальной (максимальной) цены договора просит предоставить ценовую информацию (коммерческое предложение) на приобретение ПО «ViPNet Client 4.x – номер защищаемой сети «2936ФСА»; сертифицированный криптопровайдер КриптоПРО CSP 5.0 (бессрочная).

Проведение закупки, заключение договора запланировано на октябрь 2024 года.

Требования к закупаемым товарам (работам, услугам) представлены в Приложении №1 к настоящему запросу.

В коммерческом предложении просим указать:
-характеристики товара в соответствии с данным запросом;
-цену за единицу товара;
-общую стоимость товара (цену договора);
-срок действия предложения о цене;
-страну происхождения ПО.

Просим предоставить заверенные копии:
-устава или положения (при наличии);
-свидетельства о постановке на учет российской организации в налоговом органе по месту нахождения;
-выписка из Единого государственного реестра юридических лиц;
-специального разрешения/лицензии (при наличии).

В коммерческом предложении необходимо указать, является Исполнитель ли плательщиком НДС или нет (на каком основании согласно статье Налогового Кодекса).

Информацию просим представить в виде официального письма за подписью уполномоченного лица в срок не позднее 04 октября 2024 г. на электронную почту mail@csmlg.org. или по адресу: ЛНР, г.о. город Луганск, г. Луганск, ул. Тимирязева, д. 50.

Запрос на предоставление ценовой информации направляется в соответствии с п.3.10 Методических рекомендаций по применению методов определения начальной (максимальной) цены контракта, цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем), утвержденных приказом Минэкономразвития России от 02.10.2013 № 567, и не является закупкой и не влечет за собой возникновение каких-либо обязательств заказчика.

Приложения: Техническое задание в 1 экз.

Заместитель директора по
инженерно-эксплуатационной части А.С.Алексашин

Исп. Шмитько С.А., +7(959) 109 97 13
Шапоренко Н.О.

Приложение 1

Техническое задание на ноутбук с программным обеспечением
Тех. Требования на ViPNet Client 4.x

В качестве средства защиты информации для клиентских компонент VPN-сети (далее – VPN-клиент) должен использоваться программный комплекс (ПК), отвечающий следующим требованиям:

1. VPN-клиент должен быть полностью совместим с ПК управления VPN- номер защищаемой сети «2936 ФСА», в части:
   - обновления программного обеспечения (ПО);
   - автоматического обновления справочной и ключевой информации VPN-сети;
   - управления политиками безопасности
2. VPN-клиент должен быть полностью совместим с VPN-шлюзами, представленными выше, в части шифрования/расшифрования отправляемого/принимаемого IP-трафика.
3. Поддерживать прозрачную работу через различные NAT-устройства.
4. Обеспечивать безопасную передачу (прием) данных VPN-шлюзам и VPN-клиентам (точка-точка) с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего пользования.
5. Содержать драйвер сетевой защиты, непосредственно взаимодействующий с драйвером сетевого интерфейса и осуществляющий контроль, и фильтрацию сетевого трафика.
6. Содержать сервис управления драйвером сетевой защиты, обеспечивающий функционирование узла в защищенной сети, а именно загрузку в драйвер защиты правил фильтрации, справочной информации о структуре защищенной сети и ключей шифрования, сведений о сетевых параметрах доступа для узлов защищенной сети, передачу в ПО VPN-клиента результатов обработки IP-пакетов.
7. Содержать драйвер шифрования IP-пакетов, осуществляющий шифрование и имитозащиту сетевого трафика на ключах, созданных в ПК управления VPN-сетью.
8. Обеспечивать конфиденциальность, целостность и аутентификацию каждого IP-пакета.
9. Обеспечивать настройки сетевых фильтров, параметров доступа к VPN-узлам и аудита событий.
10. Содержать приложение, осуществляющее настройку фильтров, подготовку необходимых фильтров и ключевой информации для загрузки в драйвер, аудит основных событий, ограничение интерфейса пользователя и администратора в ПО VPN-клиента, а также установку соответствующих фильтров IP-трафика в дополнение к собственным настроенным правилам фильтрации трафика.
11. Содержать систему обновления, обеспечивающую обновление ключевой и справочной информации, а также ПО VPN-клиента.
12. Содержать сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя.
13. Содержать модуль, реализующий обмен управляющей, адресной и ключевой информацией с программным обеспечением централизованного управления защищенной сетью, отправку, прием и маршрутизацию электронных документов (почтовых конвертов), отправку, прием и маршрутизацию электронных документов (почтовых конвертов).
14. Содержать службу контроля приложений, осуществляющая контроль сетевой активности приложений и позволяющая реализовывать политики доступа приложений в сеть.
15. Содержать ПО для обмена зашифрованными и подписанными сообщениями.

16. Содержать программу, осуществляющую первичную установку справочно-ключевой информации, сформированной в центре управления защищенной сетью.
17. Осуществлять функции персонального межсетевого экрана, обеспечивающие:
    - контроль сетевого трафика, проходящего через сетевые интерфейсы;
    - фильтрацию IP-пакетов по заданным правилам для зашифрованного и открытого сетевых трафиков по совокупности критериев (IP-адреса, протоколы, порты);
    - реализацию режима инициативных соединений.
18. Иметь в своем составе ПО для осуществления защищенных почтовых услуг с возможностями аутентификации отправителя и получателя, квитирования (доставлено, прочитано), электронной подписи (далее – ЭП).
19. Иметь в своем составе ПО для реализации дополнительных сервисов: защищенный чат, защищенная конференция, защищенный обмен файлами.
20. Обеспечивать замкнутость среды функционирования ПК.
21. Автоматически обрабатывать обновления, полученные из ПК управления VPN-сетью.
22. Должен функционировать под управлением следующих ОС:
    - Windows Vista (32/64-разрядная).
    - Windows Server 2008 (32/64-разрядная).
    - Windows Server 2008 R2 (64-разрядная).
    - Windows Small Business Server 2008 (64 разрядная).
    - Windows Small Business Server 2008 SP2 (64-разрядная).
    - Windows 7 (32/64-разрядная).
    - Windows 8 (32/64-разрядная).
    - Windows 8.1 (32/64-разрядная).
    - Windows Small Business Server 2011 (64 разрядная).
    - Windows Server 2012 (64-разрядная).
    - Windows Server 2012 R2 (64-разрядная).
    - Windows 10 (32/64 разрядная).
23. Должен поддерживать работу в следующих виртуальных средах:
    - Microsoft Hyper-V;
    - VMWare Workstation;
    - VMWare vSphere ESXi.
24. Обеспечивать шифрование IP-трафика, файлов и почтовых сообщений в режиме гаммирования с обратной связью, а также имитозащита информации выполняются в соответствии с ГОСТ 28147-89.
25. Обеспечивать создание ЭП, проверку ЭП, создание ключей ЭП и ключей проверки ЭП осуществляются в соответствии с алгоритмом ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
26. ПК VPN-клиент должен реализовывать функции средства ЭП (создание ЭП, проверка ЭП, создание ключа ЭП, создание ключа проверки ЭП) согласно Федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
27. Должен соответствовать требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищённости.

28. Должен соответствовать требованиям ФСБ России к шифровальным (криптографическим) средствам по классу не ниже КС2.
29. Должно иметь право обновления на новые версии продуктов в течении 1 года.
30. В комплект поставки входит оригинальный дистрибутив программного обеспечения, формуляр ФСТЭК с голографической наклейкой, копий необходимых сертификатов.

Требования к поставщику:

В соответствии с постановлением Правительства Российской Федерации № 313 от 16 апреля 2012 г., исполнитель должен иметь действующую лицензию ФСБ России:

– на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

В соответствии с приложением к Положению, утвержденному постановлением Правительства Российской Федерации № 313 от 16 апреля 2012 г., лицензия должна быть выдана на следующие виды работ: п.п. 12, 21.

В соответствии с постановлением Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) "О лицензировании деятельности по технической защите конфиденциальной информации" исполнитель должен иметь действующую лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации с указанием вида деятельности в соответствии с п.п. «е» п. 4 Положения - услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Конкретные показатели ноутбука

№	Наименование объекта закупки	Показатель объекта закупки	Единица измерения показателя (при наличии)	Значение показателей		Значение показателя, которое не может изменяться	Ед. изм. в соотвс ОКЕИ	Кол-во
				Значение показателя, которое может изменяться				
				Min	Max			
1	Ноутбук	Дисплей:					шт.	1
1.1		Диагональ экрана	Дюйм, (")	15.6				

1.2		Разрешение экрана по горизонтали		1920				
1.3		Разрешение экрана по вертикали		1080				
1.4		Светодиодная подсветка экрана				Наличие		
1.5		Покрытие поверхности экрана				Матовое		
1.6		Тип матрицы экрана				TN		
2		Процессор:						
2.1		Количество ядер процессора	шт.	2				
2.2		Количество потоков процессора	шт.	4				
2.3		Базовая тактовая частота процессора	ГГц	2.6				
2.4		Максимальная тактовая частота процессора	ГГц	3.5				
2.5		Объем кэш-памяти L1	КБ	192				
2.6		Объем кэш-памяти L2	МБ	1				
2.7		Объем кэш-памяти L3	МБ	4				
2.8		Расчетная тепловая мощность процессора (TDP), номинальный	Вт		15			
2.9		Максимальная температура, допустимая на кристалле процессора	°C		105			
2.10		Интегрированная в процессор схема обработки графических данных				Наличие		
2.11		Максимальная частота схемы обработки графических данных процессора	МГц	1200				
3		Оперативная память:						
3.1		Размер оперативной памяти	Гб	4				
3.2		Тип оперативной памяти (стандарт)				DDR4		
4		Устройства хранения данных:						
4.1		Накопитель на жёстких магнитных дисках (HDD)	шт.	1		Наличие		
4.2		Ёмкость накопителя	Гб	1000				
4.3		Скорость вращения шпинделя накопителя	об/мин	5400				
4.4		Встроенный карт-ридер				Наличие		
4.5		Поддержка карт-ридером SD/SDHC/SDXC/MMC				Наличие		
5		Встроенная web-камера	Мпикс	0.3		Наличие		
6		Встроенный микрофон				Наличие		
7		Акустическая система				Наличие		
8		Встроенный адаптер беспроводной связи Wi-Fi				Наличие		
8.1		Поддержка IEEE 802.11a				Наличие		
8.2		Поддержка IEEE 802.11b				Наличие		
8.3		Поддержка IEEE 802.11g				Наличие		
8.4		Поддержка IEEE 802.11n				Наличие		
8.4		Поддержка IEEE 802.11ac				Наличие		
9		Встроенный модуль Bluetooth				Наличие		
9.1		Поддержка Bluetooth v4.1				Наличие		
10		Разъемы и интерфейсы:						
10.1		Порт USB 2.0	шт.	1				

10.2		Порт USB 3.0 или USB 3.1	шт.	2				
10.3		Порт HDMI	шт.	1				
10.4		Комбинированный порт для микрофона и наушников	шт.	1				
11		Предустановленное программное обеспечение						
11.1		Операционная система				Windows 10		
12		Вес ноутбука	кг		1.85			
13		Габариты ноутбука:						
13.1		Высота	мм		19.9			
13.2		Ширина	мм		362.2			
13.3		Глубина	мм		251.5			
14		Комплектация ноутбука						
14.1		Инструкция пользователя				Наличие		
14.2		Блок питания				Наличие		

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на оказание услуг по предоставлению неисключительных прав (лицензий) на право использования средства криптографической защиты информации «КриптоПро CSP» версии 5.0.

1. Общая информация о закупке

1.1. Полное наименование оказываемых услуг

Оказание услуг по предоставлению неисключительных прав (лицензий) на право использования средства криптографической защиты информации «КриптоПро CSP» версии 5.0.

1.2. Общие сведения о заказчике

Адрес: 291021, Луганская Народная Республика, г.о. город Луганск, г. Луганск, р-н Артемовский, ул.Тимирязева, дом 50 Место оказания услуг

По месту нахождения Исполнителя.

По месту нахождения Заказчика.

1.3. Место сдачи результатов оказания услуг

По месту нахождения Заказчика.

1.4. Цели и задачи

Назначением услуг является обеспечение защиты открытой информации в информационных системах общего пользования (вычисление и проверка ЭП) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах (шифрование и расшифрование информации, вычисление и проверка имитовставки, вычисление значения хэш-функции, вычисление и проверка ЭП).

1.5. Требования к результатам закупки

Состав услуг, их наименование, а также требования к отчетным материалам указаны в таблице 1.

Таблица 1 - Состав, результаты оказания услуг и отчетные материалы.

Перечень услуг	Результаты оказания услуг, отчетные материалы
Лицензии на право использования средства криптографической защиты информации «КриптоПро CSP» версии 4.0.	Предоставление лицензии на право использования средства криптографической защиты информации «КриптоПро CSP» версии 5.0. 8 шт. Лицензия бессрочная

2. Информация об объекте закупки

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

2.1. Требования к реализации криптографических стандартов.

Применяемое средство криптографической защиты информации (средство электронной подписи) должно обеспечивать применение 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 электронного документа в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;
- подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001и ГОСТ Р 34.10-2012;
- подсчет значения хеш-функции в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;
- шифрование и расшифрование данных в соответствии с ГОСТ 28147-89;
- формирование закрытых и открытых ключей электронной подписи и шифрования;
- идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений;
- реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов.

2.2. Требования к сертификации

Средство электронной подписи (средство криптографической защиты информации) должно быть сертифицировано ФСБ России по классам КС1 и КС2, в качестве:

- Средства квалифицированной электронной подписи в соответствии с Требованиями ФСБ России к средствам электронной подписи;
- Средства криптографической защиты информации в соответствии с требованиями ФСБ России к шифровальным (криптографическим) средствам защиты конфиденциальной информации.

2.3. 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 CryptoAPI и CAPICOM;
- Поддержки стандарта XML DSign при формировании электронной подписи в XML документах;
- Непосредственного 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; MS Office Word, Excel, Outlook, InfoPath и т.д.) без использования дополнительных программных средств интеграции.

2.4. Требования к алгоритмам

- Алгоритм шифрования/расшифрования данных и вычисления имитовставки должен быть реализован в соответствии с требованиями ГОСТ Р 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

• Алгоритмы формирования и проверки ЭП должны быть реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

• Алгоритм выработки значения хэш-функции должен быть реализован в соответствии с требованиями ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

2.5. Требования к составу

В состав средства криптографической защиты информации (средства электронной подписи) должно входить средство сетевой аутентификации, обеспечивающее реализацию сетевого протокола SSL/TLS с использованием российских криптографических стандартов ЭП, подсчета хеш-функции и шифрования.

В состав средства криптографической защиты информации (средства электронной подписи) должно входить библиотеки IKE, ESP, AH, обеспечивающие реализацию набора протоколов IPsec с использованием отечественных криптографических алгоритмов

2.6. Функциональные требования

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

• авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи (ЭП) в соответствии с отечественными стандартами ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012);

• обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;

• обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;

• контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;

• управления ключевыми элементами системы в соответствии с регламентом средств защиты.

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

• установка личных сертификатов открытых ключей на рабочем месте/сервере с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;

• копирование и удаление закрытых ключей;

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

2.7. Требования к поддерживаемым ключевым носителям

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

• Дискета 3,5";

• Смарт-карты Оскар, Магистра;

• Электронные идентификаторы Touch-Memory DS1995, DS1996;

• Электронные идентификаторы Rutoken;

• Электронные идентификаторы eToken, Jacarta;

• Электронные идентификаторы ESMART Token;

• Смарткарты Athena IDProtect, INPASPOT, Cha cardOS, Cha JCOP, MPCOS-Gemalto;

• Сменный Flash-носитель;

• Жесткий диск ПЭВМ.

Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать возможность разработки программных библиотек поддержки произвольных типов перезаписываемых носителей.

2.8. Требования к общесистемному программному обеспечению

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

Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
Windows Server 2008 R2/2012/2012 R2/2016 (x64).

Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x:

CentOS 4/5/6/7 (x86, x64, POWER, ARM);

ТД ОС АИС ФССП России (GosLinux) (x86, x64);

Red OS (x86, x64);

Fedora 19/20 (x86, x64, ARM);

Mandriva Enterprise Server 5, Business Server 1 (x86, x64, ARM);

Oracle Linux 4/5/6/7 (x86, x64);

OpenSUSE 13.2, Leap 42 (x86, x64, ARM);

SUSE Linux Enterprise Server 11SP4/12, Desktop 12 (x86, x64, POWER, ARM);

Red Hat Enterprise Linux 4/5/6/7 (x86, x64, POWER, ARM);

Синтез-ОС.РС (x86, x64, POWER, ARM);

Ubuntu 10.04/12.04/12.10/13.04/14.04/14.10 (x86, x64, POWER, ARM);

Linux Mint 13/14/15/16/17 (x86, x64);

Debian 7/8 (x86, x64, POWER, ARM);

Astra Linux Special Edition (x86-64).

Unix

ALT Linux 7 (x86, x64, ARM);

ROSA 2011, Enterprise Desktop X.1 (Marathon), Enterprise Linux Server (x86, x64);

РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);

FreeBSD 9, pfSense 2.x (x86, x64);

AIX 5/6/7 (POWER);

Mac OS X 10.7/10.8/10.9/10.10/10.11 (x64).

Solaris

Solaris 10 (sparc, x86, x64);

Solaris 11 (sparc, x64).

Apple iOS (только КС1):

6.0/6.0.1/6.0.2/6.1/6.1.2/6.1.3/6.1.4/6.1.5/6.1.6/7.0/7.0.1/7.0.2/7.0.3/7.0.4/7.0.5/7.0.6/7.1/7.1.1/7.1.2/8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1 (ARM, arm64, arm7s).

2.9. 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:

- Microsoft Certification Authority из состава Windows 2008/2008R2/2012/2012R2;
- Электронная почта - MS Outlook из состава Microsoft Office.
- Microsoft Word, Excel из состава Microsoft Office.
- Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.
- Службы терминалов для 2008/2008R2/2012/2012R2 (включая шлюз служб терминалов) с обеспечением доступа к Службе по протоколу TLS.
- Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – web-сервер IIS, TLS-сервер, TLS-клиент (IE).
- SQL-сервер.
- ISA/TMG сервер.
- Сервер терминалов и клиент (RDP).

Данное средство должно обеспечивать возможность реализации сетевой аутентификации в домене MS Windows (на основе Winlogon) с использованием реализованных данным средством российских криптоалгоритмов

Данное средство должно обеспечивать возможность шифрования данных на жестком диске компьютера (сервера) с использованием реализованных данным средством российских криптоалгоритмов, работающего под операционными системами семейства Windows, посредством расширения стандартного функционала Microsoft Encrypt File System (Microsoft EFS).

3. Требования к объему предоставления гарантий качества товара

Поставщик гарантирует, что надлежащим образом наделен всеми необходимыми полномочиями на предоставление простых (неисключительных, пользовательских) прав на программное обеспечение (средство криптографической защиты информации КриптоПро CSP).

Поставщик гарантирует, что на момент заключения контракта не связан каким-либо договором или соглашением с третьими лицами, способным тем или иным образом помешать полному или частичному осуществлению сторонами своих обязательств.

Поставщик гарантирует урегулирование всех возможных претензий третьих лиц к Заказчику, связанных с использованием последним простых (неисключительных, пользовательских) прав, предоставленных ему Поставщиком, в соответствии с контрактом, своими силами и за свой счет.

В случае нарушения Поставщиком гарантий, предусмотренных контрактом, он обязуется возместить Заказчику все убытки, которые последний понесет в результате такого нарушения.

Поставщик гарантирует, что предоставляет права на программное обеспечение в том виде, который необходим для его надлежащего, бесперебойного функционирования.

Поставщик гарантирует Заказчику, что Поставщик имеет письменное разрешение от правообладателя на заключение договора на передачу простых (неисключительных, пользовательских) прав третьим лицам.

В случае обнаружения Заказчиком в течение срока действия Контракта дефектов программного обеспечения Поставщик устраняет эти дефекты в течение 10 (Десяти) дней со дня обращения Заказчика о необходимости их устранения своими средствами и за свой счет

4. Сроки оказания услуг и поставки товаров

Поставщик обязуется предоставить Заказчику неисключительное право на использование СКЗИ КриптоПро CSP в течение 10 (Десяти) рабочих дней с момента заключения контракта.

Неисключительное право на использование СКЗИ КриптоПро CSP считается предоставленным Заказчику в момент подписания Сторонами Акта приема-передачи.

5. Порядок передачи прав

Передача прав на ПО должна быть произведена путем заключения лицензионного (сублицензионного) договора, в случае заключения сублицензионного договора – по форме согласно настоящему техническому заданию. Права на использование ПО считаются переданными Заказчику в день подписания вышеуказанного лицензионного (сублицензионного) договора. Размер вознаграждения по лицензионному (сублицензионному) договору входит в цену Контракта и выплачивается Лицензиару в соответствии с условиями Контракта после подписания акта приема-передачи неисключительного права на использование СКЗИ КриптоПро CSP. Права на использование ПО должны быть переданы Заказчику бессрочно.