Приложение №1

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На приобретение аппаратно-программного комплекса STYX ER Client с USB ключом и программного обеспечение.

Требования к поставщику:

- Аукцион проводится в электронной системе путем пошагового снижения цены. Размер шага закупок определяется оператором по согласованию с уполномоченным органом, но не может превышать размер задатка, взимаемого с участника;
- В аукционе могут принять участие отечественные и иностранные фирмы и организации, являющиеся производителями и/или их авторизованными поставщиками, имеющие опыт поставки соответствующих объемов закупаемой на конкурсной основе продукции;
- Поставлять продукцию точно в срок по согласованному графику в соответствии с заказом (договором);
- Выдерживать согласованные цены;
- Гарантийный срок обслуживания должен составлять не менее 1 года;
- Указать стоимость и условия доставки оборудования в город Ташкент.

Техническое задание

Наименования и характеристики товара	Единица измерения	Количество
STYX ER Client с USB ключом (АКТУ.467459.001)	Штука	3500
STYX Client-DR Win11	Штука	1

Описание товара:

(АКТУ.467459.001.) - электронный идентификатор с поддержкой национальных криптографических стандартов UzDST 1106, UzDST 1092. широко применяется в информационных системах с самыми высокими требованиями к информационной безопасности, такими как: дистанционное банковское обслуживание, электронный документооборот. Средство электронной подписи обеспечивающее высокую скорость выполнения криптографических операций.

Электронный ключ предназначен для безопасной двухфакторной аутентификации пользователей, генерации и защищенного хранения ключей шифрования, ключей электронной подписи, цифровых сертификатов и других данных, а так же для выполнения шифрования и электронной подписи «на борту» устройства.

Аппаратная реализация национальных стандартов электронной подписи, шифрования и хеширования позволяет использовать в качестве интеллектуального ключевого носителя и средства электронной подписи в системах PKI, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной подписи.

позволяет выполнять криптографические операции таким образом, что закрытая ключевая информация никогда не покидает пределы токена. Таким образом, исключается возможность компрометации ключа и увеличивается общая безопасность информационной системы.

обеспечивает двухфакторную аутентификацию в компьютерных системах. Для успешной аутентификации требуется выполнение двух условий: знание пользователем PIN-кода и физическое наличие самого идентификатора. Это обеспечивает гораздо более высокий уровень безопасности по сравнению с традиционным доступом по паролю.

Основу составляет современный защищенный микроконтроллер и встроенная защищенная память, в которой безопасно хранятся данные пользователя: пароли, ключи шифрования и подписи, сертификаты и другие данные.

Электронный идентификатор поддерживает основные международные стандарты в области информационной безопасности. Это позволяет легко, без дополнительных усилий, встраивать его поддержку в существующие информационные системы.

Аутентификация

- Замена парольной аутентификации при доступе к БД, Web-серверам, VPN-сетям и security-ориентированным приложениям на двухфакторную программно-аппаратную аутентификацию.
- Аутентификация при доступе к почтовым серверам, серверам баз данных, Web-серверам, файл-серверам.
- Надежная аутентификация при удаленном администрировании и т. п.

Электронная подпись

- Аппаратная реализация электронной подписи.

Безопасное хранение ключевой информации

- Использование ключевой информации для выполнения криптографических операций на самом устройстве без возможности выдачи наружу закрытой ключевой информации.
- Сгенерированные на токене ключи не могут быть скопированы.
- При утере или краже токена безопасность не нарушается: для доступа к информации требуется PIN-код.

Защита персональных данных

- Защита электронной переписки: шифрование почты, электронная подпись почтовых отправлений.
- Защита доступа к компьютеру и в домен локальной сети.
- Возможность шифрования данных на дисках.

Корпоративное использование

- Использование в качестве интеллектуального ключевого носителя в разнообразных информационных системах, использующих технологии электронной подписи.
- Использование в качестве полноценного устройства шифрования и электронной подписи в криптографических сервис-провайдерах, системах защищенного документооборота, в ПО для шифрования логических дисков и т. д.
- Использование в корпоративных системах для надежного хранения служебной информации, персональной информации пользователей, паролей, ключей шифрования, цифровых сертификатов и любой другой конфиденциальной информации.
- Использование в качестве единого идентификационного устройства для доступа пользователя к разным элементам корпоративной системы.

Криптографические возможности

- Поддержка алгоритмов UzDST: генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи.
- Поддержка алгоритмов UzDST 1106: вычисление значения хэш-функции данных, в том числе с возможностью последующего формирования ЭЦП.
- Генерация последовательности случайных чисел требуемой длины.

Возможности аутентификации владельца

- Двухфакторная аутентификация: по предъявлению самого идентификатора и по предъявлению уникального PIN-кода.
- Поддержка 2 категорий владельцев: Администратор, Пользователь.
- Поддержка 2-х Глобальных PIN-кодов: Администратора и Пользователя.
- Поддержка Локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства.
- Настраиваемый минимальный размер PIN-кода (для любого PIN-кода настраивается независимо).
- Поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по Глобальным PIN-кодам в сочетании с аутентификацией по Локальным PIN-кодам.

- Ограничение числа попыток ввода PIN-кода.

Встроенный контроль и индикация

- Контроль целостности микропрограммы (прошивки).
- Проверка целостности RSF-файлов перед любым их использованием.
- Счетчики изменений в файловой структуре и изменений любых PIN-кодов для контроля несанкционированных изменений.
- Проверка правильности функционирования криптографических алгоритмов.
- Светодиодный индикатор с режимами работы: готовность к работе, выполнение операции.

Общие характеристики

- Современный защищенный микроконтроллер.
- Идентификация с помощью 96-битного уникального серийного номера.
- Поддержка операционных систем:
  - Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003
  - GNU/Linux
- Интерфейс USB 1.1 и выше.

Дополнительные возможности

- Собственный CSP со стандартным набором интерфейсов и функций API.
- Библиотека STYX lib для интеграции с Microsoft CNG.

Порядок оформления, предъявление результатов работ и гарантийное обслуживание:

- По завершению отдельных этапов и работы в целом Поставщик представляет акт сдачи-приемки товар и акт выполненных работ.

- Результаты работ оцениваются приемочной комиссией. Приемочную комиссию в установленном порядке образует Заказчик.
- Приемочной комиссии Поставщик предъявляет документацию, по взаимному согласованию Заказчика и Исполнителя.
- Датой сдачи – приемки работ считают дату подписания акта приемочной комиссией.

- Гарантия от производителя на поставляемый товар должна составлять не менее 1 года.

Требование к системе АПК Styx client.

Информационные сервисы единого реестра являются специализированными модулями и предназначены для обеспечения передачи информации. Информационная система должна применять сертификаты открытых ключей ЭЦП. Сертификаты открытых ключей ЭЦП должны выдаваться Центром регистрации ключей ЭЦП АКБ «Микрокредитбанк». При проверке ЭЦП должны проверяться:

- отсутствие искажения в подписанном документе и подтверждение принадлежности ЭЦП АКБ «Микрокредитбанк», на токенах которого, была сформирована ЭЦП;
- подлинность ЭЦП и действительность сертификата открытого ключа ЭЦП в момент подписания документа.
- невозможность работы участника от имени чужого;
- обеспечение регистрацию вновь вводимых участников;
- разграничение уровня доступа участника по обмену информации, установление заданные связи между участниками;
- присвоение уникальные идентификационные номера участникам;
- разрешение вход в ГВС только в том случае, если предъявлены "ключи", разрешающие работу участника и успешно выполнена процедура аутентификации;
- любая попытка работы участника в сети, как санкционированная, так и несанкционированная должна регистрироваться в специальных электронных журналах системы защиты, ведущихся по обоими сторонам устанавливаемого соединения;
- контроль целостности информации как при хранении, так и при передаче между объектами Глобальной сети;
- отправитель всегда точно должен знать, кто конкретно и когда, с учетом времени получил его информацию. Получатель всегда точно должен знать, кто конкретно и когда, с учетом времени, отправил ему информацию. Идентификационная информация должна формироваться на основе "ключа", разрешающего работу участника.

Данные должны передаваться в режиме реального времени. Передаваемые данные, должны соответствовать требованиям, изложенным в настоящем документе.

Требование к формату ключа электронной цифровой подписи и к поддерживаемым криптографическим провайдерам в системах защиты информации банка.

- Для подписания (шифрования) и проверки ЭЦП электронных документов с использованием сертификатов различных стандартов (O'zDSt 1092 алгоритм II, O'zDSt 1106 алгоритм II, и т.п.) в программном комплексе защиты информации должна быть учтена работа с внешними криптографическими провайдерами с интерфейсом Microsoft CryproAPI CNG (Microsoft® Cryptography Next Generation).

№	Наименование требования	Значение
1	Блок подстановок функции хеширования O’zDSt 1106:2009	Алгоритм II. Значения соответствуютRFC-4357 пункт 11.2 (id-GostR3411-94-CryptoProParamSet)
2	OID функции хеширования O’zDSt 1106:2009	Алгоритм II. 1.2.860.1.7.9
3	Параметры алгоритма цифровой подписи (domainparameter)для функции ЭЦП O’zDST 1092:2009	Алгоритм II. Значения параметров соответствуют RFC-4357
4	OID’ы для параметров алгоритма цифровой подписи (domainparameter)	Sign ParamsetOID:1.2.860.1.7.36.0, 1.2.860.1.7.36.1 Digest Sbox OID: 1.2.860.1.7.30.1
5	Генерация пара ключей	Внутри токена
6	Хранения закрытого ключа	Не выходит за пределы токена
7	Формат цифровой подписи в ИОК (PKI)	RFC 4491 пункт 2.2.2
8	OIDцифровой подписи в ИОК (PKI)	1.2.860.1.7.5
9	Форматы хранения закрытого ключа и если имеются, национальные OID‘ы	Для ОС Windows: закрытый формат CNG криптопровайдера
10	Форматы хранения связки закрытого ключа с сертификатом и если имеются, национальные OID‘ы	PKCS#12
11	Форматы хранения закрытого ключа на токенах	PKCS#8,
12	Форматы хранения связки закрытого ключа с сертификатом на токенах	PKCS#12, внутренний формат производителя

- Программы систем защиты информации должны работать с поддержкой криптографических алгоритмов O’zDSt 1092 (алгоритм II), O’zDSt 1106 (алгоритм II).

Требование к Операционным системам

- Windows: x64 Vista или выше (7,8,8.1,10, Server 2008, 2008R2, 2012, 2012R2).

Интеграция

- Программные комплексы по защите информации должны быть совместимы с удостоверяющим центрам АКБ «Микрокредитбанк» и Центрального банка РУз.

Обязательные дополнительные требования к поставщику:

Бесплатные неограниченные консультации по восстановлению работоспособности АПК в течении всего срока гарантии в службе технической поддержки производителя или авторизованного производителем сервисного центра;

Визиты специалиста производителя или авторизованного производителем сервисного центра в случае необходимости;

Выполнение необходимых работ по восстановлению работоспособности АПК;

Бесплатную замену и/или ремонт вышедших из строя АПК в течении гарантийного срока;

Сервисная поддержка должна оказываться в рабочие часы рабочих дней. Для обслуживания запросов сервисной поддержки, Покупатель может обращаться в Службу Технической Поддержки производителя (авторизованного производителем сервисного центра), и разработчика ПО всеми доступным средствами связи;

Сервисная поддержка должна производиться квалифицированными специалистами производителя или авторизованного производителем сервисного центра.