Обґрунтування технічних та якісних характеристик, розміру бюджетного призначення, очікувальної вартості предмета закупівлі

Для здійснення роботи з документами в системі електронної взаємодії органів виконавчої влади (СЕВ ОВВ) університету у 2024 році необхідно провести закупівлю: засіб криптографічного захисту інформації «Ключ електронний «Алмаз-1К» або еквівалент

Предмет закупівлі: Засіб криптографічного захисту інформації «Ключ електронний «Алмаз-1К» або еквівалент, код ДК 021:2015 – 32580000-2 — Інформаційне обладнання
Процедура закупівлі: відкриті торги з особливостями.

Технічні, якісні характеристики та інші умови:

№ з/п	Найменування продукції	Кількість
1.	Засіб криптографічного захисту інформації «Ключ електронний «Алмаз-1К» або еквівалент	300

1. Електронний ключ виконаний у вигляді малогабаритного знімного USB-пристрою, який має програмний CCID-інтерфейс.
2. Призначення: Формування (генерація), зберігання та використання особистих ключів користувачів.
3. Засіб кваліфікованого електронного підпису (засіб криптографічного захисту інформації) повинен забезпечувати та виконувати наступні функції:
- автентифікацію користувача при доступі до ключа;
- генерацію особистих та відкритих ключів для алгоритму електронного підпису;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;
-генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам’яті та захист їх від несанкціонованого доступу (далі – НСД);
- формування і перевірку кваліфікованого електронного підпису чи печатки;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу розподілу;
- зберігання довільних даних у внутрішній пам’яті та захист їх від НСД;
- контроль цілісності і працездатності вбудованого програмного забезпечення та інше.
4. Об’єм внутрішньої пам’яті (EEPROM) – не менше 40 кВ.
5. Технологічні особливості: виготовлений на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар, та встановлена в металевий корпус. На друкованій платі встановлюються електроні компоненти та USB-з’єднувач типу A-plug (виделка). Інтерфейс USB 2.0 або 3.0.
6. Електронний ключ реалізує наступні криптографічні алгоритми та протоколи:
- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);
- електронний підпис за ДСТУ 4145-2002 (всі довжини передбачені стандартом);
- гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних за ДСТУ ISO/IEC 11770-3:2015 (пп. 11.1) (довжина ключа до 431 біт).
7. Функції, що виконуються: обчислення електронного підпису даних; шифрування та розшифрування даних; генерації ключових даних (формування криптографічних ключів – особистих ключів та відповідних їм відкритих).

8. Швидкість формування електронного підпису – за стандартом ДСТУ 4145-2002, з довжиною ключа 257 біт – не більше 500 мс.
9. Швидкість формування спільного секрету Діффі-Гелмана в гр. т. еліптичної кривої, поле 431 – не більше 1500 мс.
10. Протокол розподілу ключових даних згідно ДСТУ ISO/IEC 11770-3:2015 (пп. 11.1) та технічних специфікацій до технічних рекомендацій IETF RFC 5652, затверджених наказом Адміністрації Держспецзв'язку № 687 від 27.10.2020 р., довжина ключа до 431 біт.
11. Експертний висновок Державної служби спеціального зв'язку та захисту інформації України – так.
12. Операційні системи, які підтримуються – Microsoft Windows (32/64-біт) 7, 8, 10, 11, Server 2003, 2012, 2016 та Linux (Ubuntu/Debian/CentOS/RHEL).
13. Пристрій повинен мати можливість ведення та перегляду журналу реєстрації подій (фіксуються події, які пов'язані із генерацією ключів, зміною паролю, спробами ввести невірний пароль доступу тощо).
14. Ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі.
15. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому постійному запам'ятовуючому пристрої електронного ключа.
16. На корпусі кожного пристрою нанесений індивідуальний серійний чи заводський номер.
17. Кількість гарантованих робочих циклів під'єднань-від'єднань пристрою (до виходу з ладу) – не менше 5000.
18. Термін зберігання даних у пам'яті - не менше 6 років.
19. Можливість використання в якості носія ключової інформації для програмного комплексу клієнта захисту «ІІТ Захист з'єднань-2. Клієнт».
20. Гарантійний строк експлуатації – не менше 36 місяців.

ЗАГАЛЬНІ ВІДОМОСТІ ПРО ПРЕДМЕТ ЗАКУПІВЛІ

1. Товар, що є предметом закупівлі повинен бути новим (2023-2024 рік виготовлення) і таким, що не був у використанні.

2. Якість Товару повинна відповідати державним стандартам, технічним регламентам та законодавству щодо показників якості такого роду/виду товарів.

**** Примітка: у разі, коли в описі предмета закупівлі містяться посилання на конкретні торговельну марку чи фірму, патент, конструкцію або тип предмета закупівлі, джерело його походження або виробника, слід читати як «або еквівалент».***

**** Примітка: Якщо учасник пропонує інший товар (еквівалент) ніж передбачений цією тендерною документацією, даний товар за своїми властивостями повинен повністю відповідати товару, що є предметом закупівлі за всіма показниками.***

Учасник, який погоджується з умовами та вимогами, зазначеними в Додатку №2 у складі своєї пропозиції повинен надати даний Додаток, завірений підписом та печаткою (у разі наявності).

Місце поставки товару: за місцезнаходженням Замовника (79007, м. Львів, вул. Городоцька, 26).

Обґрунтування розміру бюджетного призначення: з врахуванням кошторисних призначень – 331 980,00 грн. з ПДВ.

Обґрунтування очікуваної вартості: у ході моніторингу цін на засіб криптографічного захисту інформації «Ключ електронний «Алмаз-1К» взято до уваги ціни в онлайн-магазинах: АТ «ІІТ» https://ekalmaz1c.iit.com.ua/#1 - 1020,00 грн.; ДП ДІЯ – 1020,00 грн.; Token.prom.ua – 1280,00 грн.

1020,00 грн. + 1020,00 грн + 1280,00 грн. = 3320,00 грн. / 3 = 1 106,6 грн. (за 1 штуку).