**Додаток 2**

|  |  |  |
| --- | --- | --- |
| **Обґрунтування технічних та якісних характеристик**  **предмета закупівлі, розміру бюджетного призначення, очікуваної**  **вартості предмета закупівлі** | | |
| **1** | **Назва предмета закупівлі** | 1. **Захищені носії особистих ключів (Токени)**  2. ДК 021:2015: 30230000-0 - Комп’ютерне обладнання   |  |  |  |  | | --- | --- | --- | --- | | 3. закупівля Закупівля через центральну закупівельну організацію (ЦЗО)  4. Ідентифікатор закупівлі: [UA-2024-09-05-005955-a](https://www.dzo.com.ua/tenders/24144182)   |  |  | | --- | --- | |  |  | |  | |
| **2** | **Кількість** | **5 шт** |

**Технічні вимоги.**

| **Технічні характеристики та вимоги до Товару: Захищені носії особистих ключів (Токени)** | |
| --- | --- |
| 1 | 2 |
| Захищеність носія особистих ключів | Пристрій має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання (підтверджено чинним експертним висновком в галузі криптографічного захисту інформації). |
| Відповідність вимогам нормативних документів системи криптографічного захисту інформації України | Наявність сертифікату відповідності, або позитивного експертного висновку Державної служби спеціального зв'язку та захисту інформації України за результатами державної експертизи в сфері криптографічного захисту інформації, щодо можливості використання пристрою для захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом. |
| Електронні довірчі послуги | Пристрій придатний для використання в якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг (підтверджено чинним експертним висновком в галузі криптографічного захисту інформації). |
| Розмір EEPROM пам’яті | 64 КБ, або зберігання не менше 12 пар особистих ключів та відповідних сертифікатів алгоритму ДСТУ 4145-2002 431 біт та 12 пар особистих ключів та відповідних сертифікатів алгоритму RSA 2048 біт. |
| Інтерфейс підключення | FullSpeed USB 2.0 |
| Інтерфейси прикладного програмування та стандарти | PKCS#11, Microsoft Crypto API (CAPI),  JavaCryptographyArchitecture (JCA),  Збереження сертифікатів X.509 |
| Апаратно реалізовані алгоритми  (повинно бути підтверджено чинним експертним висновком в галузі криптографічного захисту інформації) | ДСТУ 4145-2002 (257 - 509 біт).  ГОСТ 34.311-95.  ДСТУ 7564:2014 (режими Купина-384, Купина-512).  ДСТУ ГОСТ 28147:2009.  ДСТУ 7624:2014 (Калина-128/128, Калина-128/256).  Обчислення спільного секрету для криптографічного протоколу Діфі-Гелмана, що базується на криптографічних перетвореннях у групі точок еліптичної кривої (ECDH).  RSA (електронний підпис та шифрування 2048 - 4096 біт).  ECDSA (256 – 521 біт).  SHA-1, SHA-256.  AES (в тому числі виготовлення імітовставки МАС, CMAC). |
| Профілі захисту | У пристрої реалізовані механізми, які забезпечують виконання функціональних вимог безпеки, що визначені (повинно бути підтверджено чинним експертним висновком в галузі криптографічного захисту інформації):   * ДСТУ EN 419211-1:2016; * ДСТУ EN 419211-2:2016; * ДСТУ EN 419211-3:2016; * ДСТУ EN 419211-4:2016; * ДСТУ EN 419211-5:2016; * ДСТУ EN 419211-6:2016. |
| Функції, що виконуються | * обчислення електронного підпису даних; * шифрування та розшифрування даних; * генерації ключових даних (формування криптографічних ключів – особистих ключів та відповідних їм відкритих);   двохфакторна автентифікація користувачів у Microsoft ActiveDirectory. |
| Швидкість формування електронного підпису | За стандартом ДСТУ 4145-2002, з довжиною ключа 257 біт – не більше 100 мс.  За стандартом RSA, з довжиною ключа 2048 біт – не більше 200 мс.  За стандартом ECDSA, з довжиною ключа 256 біт – не більше 50 мс. |
| ОС, які підтримуються | MS Windows 10/11, MS Windows Server 2016/2019/2022, Linux, Mac OS, в тому числі 64-розрядні версії зазначених ОС. |
| Термін зберігання даних у пам’яті | Не менше 10 років. |
| Кількість перезаписів в одну комірку пам’яті | Не менше 500,000. |
| Кількість гарантованих робочих циклів під’єднань-від’єднань пристрою (до виходу з ладу) | Не менше 5 000. |
| Додаткові вимоги | * 7 (сім) спроб вводу неправильного паролю (ПІН) доступу до пристрою, після чого пристрій повинен автоматично блокуватись; * під час розблокування пристрою адміністратором, усі дані користувача на пристрої (особисті ключі) повинні знищуватись (тобто розблокування прирівнюється до переініціалізації пристрою); * наявність програмного забезпечення для: перегляду ключових контейнерів на пристрої; імпорту особистих ключів та відповідних сертифікатів відкритих ключів з файлу на пристрій; експорту сертифікатів ключів з пристрою у файл; видалення ключових контейнерів; генерації особистих ключів та запитів на сертифікат відповідних відкритих ключів; * невиключна ліцензія на право використання програмного забезпечення, що реалізовує інтерфейси прикладного програмування та стандарти, утиліт тощо у кількості примірників, яка відповідає кількості одиниць придбаних пристроїв і терміном дії, який є не меншим строку служби цих пристроїв; * **металевий корпус,** і на кожного пристрою повинні бути нанесені персоналізаційні дані, що містять серійний номер;   пристрої мають бути новими (що не були в експлуатації), кожен пристрій повинен постачатись в оригінальній заводській упаковці. |
| Гарантія | *Пристрій повинен забезпечуватись гарантією від виробника та сервісною підтримкою строком не менш ніж 12 (дванадцять) календарних місяців. Сервісна підтримка включає надання консультацій за телефоном, по електронній пошті та на сайті виробника з питань експлуатації у робочі дні з 9.00 до 18.00* |

Товар має бути новим, таким, що не перебував в експлуатації (використанні). Доставка товару здійснюється однією партією за рахунок учасника.

Якість товару має відповідати стандартам, технічним вимогам, які діють на території України, та підтверджуватися сертифікатом/паспортом якості виробника на зазначений товар (у випадках, передбачених законодавством України). Пакування та маркування товару, що поставляється за даним договором, повинне відповідати діючим стандартам, технічним умовам та забезпечувати зберігання споживчих властивостей товару під час транспортування та зберігання.

Місце поставки товару: м. Чернівці, Героїв Майдану 200А. Доставка товару здійснюється однією партією.

**Для підтвердження відповідності запропонованого товару вищезазначеним вимогам замовника учасник у складі тендерної пропозиції надає:**

1. Документ, який підтверджує якість запропонованого товару, а саме: сертифікат, паспорт якості на товар (у випадках, передбачених законодавством України) тощо.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  | | | **Обґрунтування очікуваної вартості предмета закупівлі, розміру бюджетного призначення** | Очікувана вартість предмета закупівлі визначена відповідно до «Примірної методики визначення очікуваної вартості предмета закупівлі», затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства від 18.02.2020 № 275 шляхом моніторингу цін, отриманих комерційних пропозицій та складає:  **7500,00 грн. (сім тисяч п'ятсот гривень 00 копійок).** |