

Обґрунтування технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі:
(відповідно до пункту 4¹ постанови КМУ від 11.10.2016 № 710 "Про ефективне використання державних коштів")

I. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб:

Державна служба статистики України;
вул. Шота Руставелі, 3, м. Київ, 01601;
код за ЄДРПОУ – 37507880

II. Назва предмета закупівлі:

"ДК 021:2015 "Єдиний закупівельний словник": 32580000-2 Інформаційне обладнання (Захищені носії ключової інформації)"

III. Обґрунтування технічних та якісних характеристик предмета закупівлі:

ТЕХНІЧНІ ВИМОГИ

**на закупівлю: "ДК 021:2015 "Єдиний закупівельний словник":
32580000-2 Інформаційне обладнання (Захищені носії ключової інформації)"**

1. Загальні вимоги до захищених носіїв особистих ключів

1.1. Захищені носії особистих ключів повинні представляти апаратні засоби, які реалізують українські та міжнародні стандарти в галузі криптографічного захисту інформації, включаючи засіб кваліфікованого електронного підпису та/або печатки.

1.2. Захищені носії особистих ключів повинні бути сумісними для використання в інформаційних системах державних органів, зокрема таких як система дистанційного обслуговування "Клієнт Казначейства – Казначейство" та АС "Є-Звітність", інші системи подання електронної звітності до державних органів, системи електронного документообігу, авторизації користувачів і захищеного зберігання ключової інформації.

1.3. Захищені носії особистих ключів повинні бути програмно та технічно сумісними з наступними засобами, комплексами та системами, які використовуються в Державній службі статистики України:

- комплекс програмний центру сертифікації ключів "ІТ ЦСК-1" (версія 1.3);
- комплекс програмний користувача центру сертифікації ключів "ІТ Користувач ЦСК-1";
- програмний комплекс клієнта захисту мережних з'єднань "ІТ Захист з'єднань 2. Клієнт захисту з'єднань";
- програмний комплекс шлюзу захисту "ІТ Захист з'єднань 2. Шлюз захисту";
- програмний комплекс віддаленого управління IP-шифраторами "ІТ Захист IP-потоків-2. Віддалене управління IP-шифраторами";
- IP-шифратори "Канал-201" (мікро-пристрій), IP-шифратори "Канал-201", IP-шифратори "Канал-301";
- мережний криптомодуль "Гряда-301" (міні-пристрій).

1.4. Захищені носії особистих ключів повинні застосовуватися для захищеного зберігання і використання ключів кваліфікованого електронного підпису (КЕП), отриманих у Кваліфікованих надавачів електронних довірчих послуг, виконувати функції формування і перевірки електронного підпису, шифрування, автентифікації, зберігання секретної (ключової) інформації.

2. Технічні вимоги

2.1. Засіб КЕП має бути представлений у вигляді електронного USB-пристрою та мати стійкий від механічних пошкоджень корпус з металевим роз'ємом USB для безпечного зберігання та використання записаних на нього даних.

2.2. Захищеність носія особистих ключів – пристрій повинен забезпечувати захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання (повинно бути підтверджено чинним експертним висновком в галузі криптографічного захисту інформації).

2.3. Відповідність вимогам нормативних документів системи криптографічного захисту інформації України – пристрій повинен мати сертифікат відповідності або позитивний експертний висновок Державної служби спеціального зв'язку та захисту інформації України за результатами державної експертизи в сфері криптографічного захисту інформації.

2.4. Інтерфейс підключення – USB 2.0, протокол обміну – CCID.

2.5. Мають бути апаратно реалізовані криптографічні алгоритми – ДСТУ 4145-2002, ГОСТ 34.311-95, ДСТУ ГОСТ 28147:2009 (повинно бути підтверджено чинним експертним висновком в галузі криптографічного захисту інформації).

2.6. Функції, що виконуються: обчислення електронного підпису даних; шифрування та розшифрування даних; генерації ключових даних (формування криптографічних ключів – особистих ключів та відповідних їм відкритих).

2.7. Швидкість формування електронного підпису – за стандартом ДСТУ 4145-2002, з довжиною ключа 257 біт – не більше 100 мс.

2.8. Операційні системи, які підтримуються – Microsoft Windows (32/64-біт) 7, 8, 10, 11, Server 2003, 2012, 2016, 2019 та Linux (Ubuntu/Debian/CentOS/RHEL).

2.9. Термін зберігання даних у пам'яті - не менше 10 років.

2.10. Кількість гарантованих робочих циклів під'єднань-від'єднань пристрою (до виходу з ладу) – не менше 5 000.

3. Інші вимоги:

– на корпусі кожного пристрою має бути нанесений індивідуальний серійний чи заводський номер;

– пристрій має використовуватися в якості засобу КЕП чи печатки для надання кваліфікованих електронних довірчих послуг та відповідати вимогам (реалізувати вимоги профілів захисту для пристроїв створення безпечного підпису) згідно з ДСТУ EN 419211-1:2016 і ДСТУ EN 419211-2:2016 (повинно бути підтверджено чинним експертним висновком в галузі криптографічного захисту інформації);

– невиключна ліцензія на право використання програмного забезпечення, що реалізує інтерфейси засобів криптографічного захисту інформації у кількості примірників, яка відповідає кількості одиниць придбаних пристроїв і терміном дії, який є не меншим строку служби цих пристроїв.

4. Підтвердження відповідності:

Для підтвердження відповідності захищених носіїв особистих ключів вимогам (технічним та якісним характеристикам) предмета закупівлі у складі своєї пропозиції Учасник повинен надати:

1. Сертифікат (або сертифікати) відповідності та/або (діючий) позитивний експертний висновок (або експертні висновки) за результатами державної експертизи у сфері криптографічного захисту інформації, які підтверджують відповідність технічним та якісним вимогам визначених пунктом 2 цього додатку.

2. Документ (та/або гарантійний лист) від виробника або представника виробника на території України про безперебійну та сумісну роботу запропонованих Учасником захищених носіїв особистих ключів з засобами та комплексами, які використовуються в Державній службі статистики України та наведені у пункті 1.2 цього додатку.

IV. Обґрунтування розміру бюджетного призначення, очікуваної вартості предмета закупівлі:

Очікувана вартість предмета закупівлі визначена у межах видатків, передбачених Кошторисом на 2024 рік для апарату Державної служби статистики за бюджетною програмою КПКВК 0414010 "Керівництво та управління у сфері статистики" (з урахуванням змін) по КЕКВ 2210 "Предмети, матеріали, обладнання та інвентар". Очікувана вартість предмета закупівлі розрахована відповідно до Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275, за таким підходом:

За інформацією з відкритих джерел (вебсайти розробників або офіційних партнерів) середня ринкова вартість захищеного носія особистого ключа може становити 955 грн або 935 грн, враховуючи можливі знижки. Зокрема аналізувалися вебсайти:

- АТ "Інститут Інформаційних Технологій" (<https://ekalmaz1c.iit.com.ua/>);

- ТОВ "Авест-Україна" (<https://www.avest.com.ua/rishennia/zahyshhenyj-nosijeczp-token-avestkey/>);

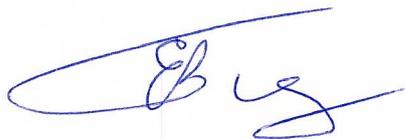
- Компанія MASTERKEY (<https://ca.masterkey.ua/aparatni-zasoby/>).

Середня вартість захищеного носія особистого ключа складає:

$(945+900 (840 \text{ зі знижкою})+1020)/3=955$ (935 зі знижкою) \approx 945 грн.

Очікувана вартість закупівлі 200 штук захищених носіїв становить 189 000,00 грн.

Директор департаменту
інформаційних технологій



Олена ПУЗАНОВА