ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ

(оприлюднюється на виконання постанови КМУ № 710 від 11.10.2016 «Про ефективне використання державних коштів» (зі змінами))

**Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб — підприємців та громадських формувань, його категорія: Держмитслужба м. Київ , вул. Дегтярівська, 11г, ЄДРПОУ 43115923.**

**Вид та ідентифікатор процедури закупівлі:** UA-2024-07-10-008513-a.

1. Предмет закупівлі: (зазначається назва предмета закупівлі та код ДК 021:2015 із застосуванням Єдиного закупівельного словника (див. пункт 2.3 розділу ІІ Порядку організації планування та проведення публічних закупівель в Державній митній службі України)).

**«**Програмне забезпечення для ідентифікації та аутентифікації користувачів, для внутрішніх систем без доступу до мережі Інтернет та послуги з його впровадження»за кодом ДК 021:2015-72260000-5 Послуги, пов’язані з програмним забезпеченням

1. Обґрунтування доцільності закупівлі (чим зумовлена необхідність закупівлі, мета закупівлі, посилання на вимоги чинного законодавства).

Метою закупівлі послуг є забезпечення доступу до інформаційних систем Державної митної служби через єдину точку входу та з механізмом двухфакторної аутентифікації.

Впровадження програмного забезпечення для ідентифікації та аутентифікації користувачів, для внутрішніх систем без доступу до мережі Інтернет забезпечить управління обліковими записами користувачів, автоматичне керування (оркестрація) привілеїв доступу на основі матриці доступу до інформаційних ресурсів та вирішить питання щодо невідповідності вимог стосовно складності паролів і періодичності їх зміни в різних інформаційних системах Державної митної служби України.

Ідентифікацію й аутентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація й аутентифікація – це перша лінія оборони, "прохідна" інформаційного простору організації.

Ідентифікація дозволяє суб'єктові (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка дійсності".

Надійна ідентифікація й аутентифікація ускладнена не тільки через мережеві загрози, але й з цілого ряду причин. По-перше, майже всі аутентификаційні сутності можна довідатися, украсти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача й системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже на його місце могла сісти інша людина), а це не тільки клопітно, але й підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніший засіб захисту, тим він дорожчий.

Сучасні засоби ідентифікації/аутентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід у мережу - це, у першу чергу, вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежний обіг, то багаторазова ідентифікація/аутентифікація стає занадто обтяжною. На жаль, поки не можна сказати, що єдиний вхід у мережу став нормою, що домінантні рішення поки не сформувалися.

Технологія єдиного входу - технологія, що дозволяє користувачеві пройти аутентифікацію (вхід зі своїми обліковими даними) один раз і отримати доступ до різних інформаційних ресурсів (переходити з одного ресурсу до іншого, без повторної [аутентифікації](https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F)).

Наприклад, у великих приватних мережах часто існує декілька незалежних підсистем. З допомогою SSO реалізується доступ до всіх підсистем без повторного введення логіну/паролю. Для цього користувачеві буде достатньо ввести логін/пароль лише раз для однієї з підсистем і він матиме доступ до всіх інших.

Отже, впровадження програмного забезпечення для ідентифікації та аутентифікації користувачів для внутрішніх систем без доступу до мережі Інтернет забезпечить управління обліковими записами користувачів, автоматичне керування (оркестрація) привілеїв доступу на основі матриці доступу до інформаційних ресурсів та вирішить питання щодо невідповідності вимог стосовно складності паролів і періодичності їх зміни в різних інформаційних системах Державної митної служби України.

1. Обґрунтування обсягів закупівлі (відповідно до чого визначено обсяги закупівлі або підставі чого обраховано).

Обсяги закупівель визначені відповідно до потреб замовника на 2024 рік.

1. Обґрунтування технічних та якісних характеристик закупівлі (якісні характеристики).

Визначено відповідно до потреб замовника та з урахуванням загальноприйнятих норм і стандартів для зазначеного предмета закупівлі.

1. Обґрунтування бюджетного призначення та/або очікуваної вартості предмета закупівлі:

**Очікувана вартість та обґрунтування очікуваної вартості предмета закупівлі:** **3 600 000,00** гривень. Визначення очікуваної вартості предмета закупівлі обумовлено статистичним аналізом загальнодоступної інформації про ціну предмета закупівлі на підставі затвердженої центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері публічних закупівель, примірної методики визначення очікуваної вартості предмета закупівлі, а саме: згідно з пунктом 1 розділу ІІІ наказу Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 із змінами та методом порівняння ринкових цін та визначення середньоринкової ціни. Так, інформацію стосовно вартості послуг отримано від виробника обладнання на основі Global Price List.

**ТЕХНІЧНІ ВИМОГИ**

**ІНФОРМАЦІЯ ПРО ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

**Послуги, пов’язані з програмним забезпеченням –**

**за кодом ДК 021:2015-72260000-5**

**Програмне забезпечення** **для ідентифікації та аутентифікації користувачів, для внутрішніх систем без доступу до мережі Інтернет та послуги з його впровадження**

**Загальні відомості**

1. **Призначення програмного забезпечення**

Програмне забезпечення для ідентифікації та аутентифікації користувачів, для внутрішніх систем без доступу до мережі Інтернет повинно забезпечувати функціонал механізму багатофакторної аутентифікації та одноразового входу (MFA/SSO) (далі – Програмне забезпечення) призначене для забезпечення високого рівня безпеки в системах інформаційної безпеки та ідентифікації користувачів. Основна мета цього Програмного забезпечення - забезпечити захист від несанкціонованого доступу до облікових записів та конфіденційної інформації.

У зв'язку з ростом загрози кібератак на державні інформаційні ресурси, обумовленого загостренням політичної ситуації та військовою агресією з боку російської федерації, виникає серйозна загроза безпеці облікових записів користувачів, особливо тих, які мають підвищені привілеї та права доступу до систем. Враховуючи це, важливо впровадити заходи забезпечення безпеки, такі як механізми багатофакторної аутентифікації та одноразового входу (MFA/SSO). Ці заходи дозволять підвищити надійність аутентифікації користувачів та зменшити ризик несанкціонованого доступу до інформаційних систем.

Завдяки багатофакторній аутентифікації (MFA), програмне забезпечення дозволяє користувачам використовувати додаткові методи підтвердження своєї особи під час входу до системи. Такий підхід забезпечує додатковий рівень захисту, оскільки навіть якщо зловмиснику вдасться отримати доступ до основного пароля користувача, він все одно не зможе увійти до системи без додаткових аутентифікаційних факторів. Одноразовий вхід (SSO) дозволяє користувачам увійти до різних систем та сервісів, використовуючи лише один обліковий запис. Це спрощує процес аутентифікації та дозволяє ефективно керувати доступом до різних ресурсів без необхідності повторного введення облікових даних кожного разу.

Закупівля послуг з постачання та впровадження Програмного забезпечення є ключовим кроком для запобігання можливим проблемам, пов'язаним з безпекою облікових записів. Це дозволить підприємству ефективно керувати доступом до цих облікових записів, мінімізувати ризик несанкціонованого доступу та забезпечити надійність інформаційних ресурсів.

1. **Мета і завдання впровадження Програмного забезпечення**

Метою впровадження Програмного забезпечення є підвищення рівня безпеки ідентифікації користувачів та захисту конфіденційної інформації в інформаційних системах.

Впровадження Програмного забезпечення забезпечить:

* Зниження ризику несанкціонованого доступу до інформаційних систем та ресурсів**.**
* Підвищення рівня захисту даних**.**
* Покращення користувацького досвіду завдяки одноразовому входу, що дозволяє уникнути необхідності повторного введення облікових даних для кожного сервісу або системи.
* Централізоване керування доступом до різних ресурсів та облікових записів.
1. **Вимоги чинного законодавства**
2. Конституція України;
3. Закон України «Про електронну ідентифікацію та електронні довірчі послуги»;
4. Закон України «Про інформацію»;
5. Закон України «Про електронні документи та електронний документообіг»;
6. Закон України «Про доступ до публічної інформації»;
7. Закон України «Про захист персональних даних»;
8. Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
9. Митний кодекс України;
10. Постанова Кабінету Міністрів України від 12 березня 2022 року № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»;
11. Постанова Кабінету Міністрів України від 08 вересня 2016 року № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів»;
12. Постанова Кабінету Міністрів України від 02 лютого 2024 року № 119 «Деякі питання Національної програми інформатизації»;
13. Постанова Кабінету Міністрів України від 4 лютого 1998 року № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»
14. Розпорядження КМУ «Деякі питання реалізації концептуальних напрямів реформування системи органів, що реалізують державну митну політику»
від 13 травня 2020 р. № 569-р;
15. Довгостроковий національний стратегічний план цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України та її територіальних підрозділів на основі Багаторічного стратегічного плану електронної митниці ЄС (Multi-annual strategic plan for electronic customs, MASP-C), затвердженого наказом Міністерства фінансів України від 09.02.2024 № 63 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами».
16. **Вимоги до постачання Програмного забезпечення**

Виконавець протягом 60 (шістдесяти) календарних днів з дати укладання Договору передає Замовнику Програмне забезпечення та здійснює його базову інсталяцію, пусконалагоджувальні роботи (у тому числі інтеграцію з існуючим обладнанням та системами Замовника) та тестування. Після налаштування програмного забезпечення Виконавець повинен провести навчання не менше 3-х співробітників Замовника по експлуатації та роботі з програмним забезпеченням.

1. **Загальні вимоги до технічної підтримки**
2. Термін технічної підтримки програмного забезпечення, що поставляється за Договором складає не менше ніж 36 місяців від дати підписання Акту приймання-передачі послуг відповідно до умов договору.
3. Надання консультацій електронною поштою з питань налаштування та експлуатації обладнання в робочі дні з 9.00 до 18.00 години. Послуги даного типу (консультації) являють собою рекомендації та/або відповіді на запитання Замовника стосовно особливостей налагодження, адміністрування Програмного забезпечення.
4. Реагування на запити на обслуговування протягом 1-єї години з моменту отримання запиту на обслуговування.
5. Постійний доступ до Центру технічної підтримки виробника програмного забезпечення, що працює в режимі: 24х7х365 (цілодобово (00:00-24:00) з понеділка по неділю включно, 365 днів на рік з можливістю звернення через веб-сайт або електронну пошту (e-mail).
6. Учасник повинен надати Замовнику перелік телефонів, веб-сайт або електронну пошту (e-mail) Центру технічної підтримки виробника Програмного забезпечення протягом 3-х календарних днів з моменту підписання Договору.
7. Доступ до закритої частини сайту виробника і онлайн бази знань виробника з технічною інформацією та корисними інструментами.
8. Надання Замовнику основних та перехідних версій програмного забезпечення Виробника за допомогою веб-сайту виробника.
9. Надання рекомендацій по налаштуванню політик, що застосовуються в роботі програмного забезпечення. Надання допомоги у пошуку рішень відомих проблем в базі знань виробника програмного забезпечення та в інших джерелах.

**СПЕЦИФІКАЦІЯ ПОСЛУГ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Найменування** | **Короткий опис** | **Кількість** | **Примітки** |
| 1. | Програмне забезпечення для ідентифікації та аутентифікації користувачів, для внутрішніх систем без доступу до мережі Інтернет та послуги з його впровадження, комплект у складі: | Програмне забезпечення (ліцензія(ї)) в електронному вигляді з функціоналом механізмів багатофакторної аутентифікації та одноразового входу (MFA/SSO) та пристрої генерації одноразових паролів  | 1 |  |
| 1.1. | Ліцензія на користувача | Програмне забезпечення (ліцензія(ї)) в електронному вигляді, яка буде забезпечувати роботу функціоналу  | 150 | Детальний опис вимог до функціоналу наведено у таблиці 1 |
| 1.2. | Пристрій генерації одноразових паролів | Токен-генератор  | 150 | Детальні вимоги описані в пунктах п.п. 55-58 Таблиці 1 |
| 1.3. | Послуги з впровадження  | Розгортання Програмного забезпечення та його налаштування для ідентифікації та аутентифікації користувачів складається з таких етапів:* Наземне розгортання Програмного забезпечення
* Налаштування апаратних токенів
* Налаштування програмних токенів
* Налаштування агентів на робочих станціях співробітників
* Інтеграційне налаштування
* Розробка технічної документації
 | 1 | Детальний вимоги п.п. 10-97 Таблиці 1 |