

Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі

ТЕХНІЧНІ ВИМОГИ ТА СПЕЦИФІКАЦІЯ ТОВАРУ

Лот 1 - робочі станції для оформлення та видачі паспортів громадян України для виїзду за кордон та паспортів громадян у формі картки.

Місце поставки – 02094, м. Київ, вул. Бажова, 11/8

Термін поставки: березень – квітень 2017 року

Об'єкт закупівлі

Робоча станція для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, з комплектом обладнання для зняття біометричних даних (параметрів) особи, реєстрації/зняття з реєстрації місць проживання/перебування громадян України, іноземців та осіб без громадянства (*далі – РС1*).

Загальні відомості

Даний документ містить основні вимоги до обладнання та спеціалізованого програмного забезпечення РС1 для оформлення та видачі паспортних документів, взяття біометричних даних і реєстрації місць проживання (*таблиця 1*); до захисту інформації в робочих станціях усіх типів (*таблиця 2*).

Термін гарантії на обладнання та на технічну підтримку програмного забезпечення – **не менше 12 місяців** з дня введення робочих станцій в експлуатацію.

Таблиця 1 - Технічні вимоги та специфікація РС1 для оформлення та видачі паспортних документів, взяття біометричних даних і реєстрації місць проживання

1.1. Призначення РС1	РС1 призначена для автоматизації діяльності посадових осіб для виконання державних функцій щодо надання послуг з оформлення документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус (<i>далі – документи</i>), взяття їх біометричних даних (параметрів), а також реєстрації/зняття з реєстрації місць проживання/перебування громадян України, іноземців та осіб без громадянства. РС1 забезпечує роботу посадових осіб в інтерфейсі web-сервісу під час виконання встановлених процедур та операцій з оформлення та видачі документів, у тому числі паспорта громадянина України для виїзду за кордон з безконтактним електронним носієм або паспорта громадянина України у формі картки.
1.2. Склад РС1	РС1 представляє програмно-технічний комплекс на базі персонального комп'ютера з встановленим загальним та спеціалізованим програмним забезпеченням, комплектом обладнання (з

	відповідними технічними характеристиками) для взяття біометричних даних (параметрів) особи під час оформлення та видачі їй документів. До складу PC1 входять апаратні та програмні компоненти.
1.3. Склад апаратних компонентів PC1	До складу PC1 входять наступні апаратні компоненти: - персональний комп'ютер: материнська плата, процесор, оперативна пам'ять, жорсткий магнітний диск, відеоадаптер; - 2 LED монітори (для оператора та клієнта); - клавіатура та маніпулятор типу "миша"; - блок безперебійного живлення; - концентратор USB; - цифрова фотокамера з об'єктивом та фото аксесуарами; - зчитувач відбитків пальців; - планшет для підпису; - повносторінковий зчитувач документів (OCR, RFID, MRZ) з модулем для ID-карт; - багатофункціональний пристрій A4 або окремі принтер та сканер; - цифрова клавіатура для введення ПІН-кодів; - мережевий фільтр для підключення, 6 розеток; - мережевий фільтр для підключення, 3 або більше розеток, довжина кабелю не менше ніж 3 м.
1.3.1. Вимоги до персонального комп'ютеру PC1	<u>Чипсет материнської плати:</u> не гірше ніж гірше Intel H81 або аналог. <u>Частота процесору:</u> не нижче ніж 3,2 ГГц, кількість ядер не менше 2. <u>Оперативна пам'ять:</u> не гірше DDR3-1600, 4Гб. <u>Жорсткий диск:</u> об'єм не менше 500 Гб; кешпам'ять не менше 32 Мб; швидкість обертів диска не менше 7200 об/хв. <u>Графічний відеоадаптер:</u> з можливістю підключення 2 моніторів або аналог. <u>Корпус та блок живлення:</u> ATX потужністю не менше ніж 400 Вт або аналог. <u>Пристрої вводу-виводу:</u> повнорозмірна клавіатура та миша з інтерфейсом PS/2 або USB.
1.3.2. Вимоги до монітора PC1	<u>Діагональ:</u> не менше ніж 21,5" (Wide 16:9). <u>Тип матриці:</u> не гірше ніж TN+film. <u>Час відгуку:</u> не більше ніж 5 мс. <u>Кут огляду (гориз./вертик.):</u> 90°/65°. <u>Макс. роздільна здатність:</u> не нижче ніж 1920 dpi x 1080 dpi. <u>Інтерфейс:</u> D-Sub; DVI. <u>Яскравість:</u> не нижче ніж 200 кд/м².

	<u>Контрастність реальна / динамічна:</u> не нижче 1 000:1 / 5000 000:1. <u>Споживана потужність:</u> не вище ніж 20 Вт.
1.3.3. Вимоги до джерела безперебійного живлення PC1	<u>Топологія:</u> Line-interactive. <u>Тип синусоїди при роботі від батареї:</u> апроксимована синусоїда. <u>Потужність повна:</u> не менше ніж 1000 ВА. <u>Потужність активна:</u> 500 Вт. <u>Час переключення на батарейне живлення:</u> 5 мсек.
1.3.4. Вимоги до концентратора USB PC1	<u>Інтерфейс:</u> USB 2.0. <u>Кількість портів:</u> не менше 7. <u>Живлення:</u> мережеве, 220 В.
1.3.5. Вимоги до цифрової фотокамери з об'єктивом та фотоаксесуарів PC1	<u>Технічні вимоги до фотокамери:</u> - роздільна здатність знімків: 12 млн. пікселів або більше; - сумісність з об'єктивами: EF, EF-S та 18-55 IS II Kit; - підтримка: JPEG, RAW; - серійна зйомка: JPEG - 3 кадри/с, RAW - 2 кадри/с; - карти пам'яті: SD/SDHC; - мережевий блок живлення: 220 В. <u>Перелік необхідних фотоаксесуарів:</u> - штатив для фотокамери; - штатив для спалаху; - спалах для фотокамери з тримачем - 2 шт.; - комплект синхронізаторів з радіомодулем для спалаху (ресивер, 2 трансмітери) або синхрокабель; - парасоля для спалаху, діаметр 84 см зі стійкою; - фон тканевий (білий); - кріплення для спалаху та парасолі; - подовжувач USB 2.0, довжина не менше ніж 1 м.
1.3.6. Вимоги до зчитувача відбитків пальців PC1	<u>Можливості:</u> - підключення до базового комп'ютера (у тому числі до ноутбука); - зняття відбитків для кожного пальця окремо; - наявність технології ідентифікації живої тканини та штучних відбитків; - оптична схема повинна дозволяти отримувати відбитки високої якості навіть з вологих пальців. <u>Технічні вимоги:</u> - роздільна здатність зображень: 500 пікселів на дюйм; - відповідність за якістю специфікації "FBI Image Quality Specification" додаток F, "WHQL"; - динамічний діапазон більше 8 біт, глибина градацій сірого більше 256; - якість зображень відповідно до стандартів: GS, CE, EMV, BSI-TR PDU, FBI EFTS/F;

	- розмір екрана для зняття відбитків: 24 мм x 16 мм; - розмір сканера: 60 мм x 83 мм x 49 мм; - інтерфейс: USB 2.0.
1.3.7. Вимоги до планшета для підпису PC1	<u>Тип дисплею:</u> RGB, монохромний. <u>Роздільна здатність зображень:</u> 500 пікселів на дюйм. <u>Активна область введення:</u> 96 мм x 60 мм. <u>Розмір сканера:</u> 161 мм x 174 мм x 11 мм.
1.3.8. Вимоги до повносторінкового зчитувача документів (OCR, RFID, MRZ) з модулем для ID-карт PC1	<u>Можливості:</u> - підключення до базового комп'ютера (у тому числі до ноутбука); - сканування оптичної інформації; - зчитування інформації з MRZ зони; - зчитування інформації безконтактного чіпа. <u>Технічні вимоги:</u> - роздільна здатність зображень: 500 пікселів на дюйм; - OCR MRZ зчитувач: ICAO9303; - безконтактний зчитувач: ISO 14443; - стандарти: ICAO, IAS, ISO 14443, pc/sc, fips; - швидкість обміну даними: до 848 кбіт/с; - розмір пристрою: 180 мм x 175 мм x 145 мм; - інтерфейс: USB 2.0 (швидкість 12 Мб/с).
1.3.9. Вимоги до багатофункціонального пристрою PC1(або окремих принтеру та сканеру)	<u>Принтер:</u> - формат друку: A4; - якість друку: 600 x 600 точок на дюйм; - швидкість: до 18 стр/хв. <u>Сканер:</u> - формат: A4; - тип датчика: контактний (CIS); - оптичний дозвіл: до 9600 x 9600 точок на дюйм; - глибина кольору: 24 біт; - швидкість сканування: 16 сек. <u>Копір:</u> - формат: A4; - оптичний дозвіл: 600 x 600 точок на дюйм; - швидкість: до 18 стр/хв.; - масштабування: 25-200%. - інтерфейс: USB 2.0 Hi-Speed. Підтримувані операційні системи: Windows 10/8.1/8/7/Vista SP1 і SP2 / XP SP3 32; Mac OS X v10.6.8 або новіша, або аналог. Кабель USB для багатофункціонального пристрою (або принтеру), довжина 3,0 м.
1.3.10. Вимоги до цифрової клавіатури для	Цифрова клавіатура для введення ПІН-кодів Genius Numpad i120 USB Slim або аналог. <u>Вигляд:</u> плоска цифрова клавіатура.

введення ПІН-кодів PC1	<u>Тип:</u> мембранна. <u>Кількість клавіш:</u> 18 стандартних клавіш, клавіша Backspace. <u>Порт інтерфейсу:</u> USB (NumPad). <u>Підключення:</u> Plug&Play. <u>Підтримка:</u> Windows 8/7 / Vista / XP. <u>Розміри:</u> 132 мм x 16 мм x 92 мм.
Термін гарантійного обслуговування апаратних компонентів має становити не менше 12 місяців з дати підписання Сторонами видаткової накладної.	
1.4. Вимоги до програмних компонентів PC1	Програмне забезпечення (ПЗ) PC1 складається з загального та спеціалізованого. <u>Загальне ПЗ:</u> – операційна система: Microsoft Windows 10 Pro / Microsoft Windows 10 Pro (downgrade to 8.1) SNGL OLP або аналог; – антивірусне ПЗ: ESET Smart Security або аналог. <u>Спеціалізоване ПЗ:</u> – для проведення первинного логічного контролю якості та коректності отримання персональних даних відповідно до вимог ISO; – верифікації/ідентифікації по відбитках пальців (AFIS); – отримання персональних даних та реалізації механізмів контролю доступу до БЕН; – модуль перевірки якості фотографій згідно з рекомендаціями ICAO; – програмний додаток "Біометричні дані".
1.4.1. Вимоги до спеціалізованого ПЗ для проведення первинного логічного контролю якості та коректності отримання персональних даних відповідно до вимог ISO	Спеціалізоване ПЗ призначене для збору біометричних даних (параметрів) особи, яка подала заявку на оформлення та виготовлення їй документів. Спеціалізоване ПЗ повинно взаємодіяти з наступними апаратними компонентами PC1: – цифровою фотокамерою; – зчитувачем відбитків пальців; – планшетом для підпису; – зчитувачем документів. Спеціалізоване ПЗ повинно виконувати наступні функції: – збирати біометричні дані (параметри) особи; – забезпечувати візуальний контроль сканування біометричних даних (параметрів) особи; – формувати пакет біометричних даних (параметрів) у форматі XML; – зчитувати інформацію з виготовленого документа. Функція збору біометричних даних полягає в тому, що за допомогою апаратних засобів (зчитувача відбитків пальців, планшета для підпису, фотокамери), підключених до персонального комп'ютера, збираються

	біометричні дані особи (відбитки пальців, особистий підпис, фотографія). Функція візуального контролю сканування полягає в тому, що всі зображення відсканованих відбитків пальців, зображення особистого підпису та фотозображення особи відображаються на моніторі в режимі реального часу. Функція формування пакету біометричних даних (параметрів) у форматі XML полягає в тому, що всі зібрані біометричні дані (параметри) особи (відбитки пальців, особистий підпис, фотографія) формуються в пакет даних у форматі XML. Функція зчитування інформації з виготовленого документа полягає в перевірці можливості зчитування біометричних даних, що містяться на ньому. Функція виконується за допомогою зчитувача документів.
1.4.2. Вимоги до спеціалізованого ПЗ верифікації/ідентифікації по відбитках пальців (AFIS)	Спеціалізоване ПЗ повинно забезпечувати централізоване зберігання відбитків пальців, отриманих за результатом збору біометричних даних (параметрів) особи для виготовлення документів. При цьому повинен забезпечуватися контроль якості зображень відсканованих відбитків, здійснюватися їх перетворення в цифровий графічний формат, сегментація, перетворення у цифровий шаблон, співставлення отриманих шаблонів із шаблонами, що зберігаються в базі даних (пошук та ідентифікація). Автоматизовані процеси, що пов'язані з введенням та первинним обробленням інформації, повинні реалізовуватись за технологією "клієнт-сервер" на програмно-технічних комплексах робочих місць. Спеціалізоване ПЗ повинно забезпечувати централізований порядок збору біометричних даних (параметрів), їх обробку та передачу з використанням відповідного протоколу обміну даними.
1.4.3. Вимоги до спеціалізованого ПЗ отримання персональних даних та реалізації механізмів контролю доступу до БЕН	Спеціалізоване ПЗ повинно забезпечувати оптичне сканування, розпізнавання машинозчитувальної зони (<i>далі – MRZ зона</i>), її декодування, здійснення перевірки достовірності даних MRZ зони. Спеціалізоване ПЗ повинно забезпечувати доступ до даних, записаних на безконтактний електронний носій (БЕН) документів: а) встановлювати сесію обміну даними з БЕН (види автентифікації): – BAC – BAC + AT – PACE_MRZ – PACE_MRZ + AT – PACE_CAN – PACE_CAN + AT – PACE_PIN1 – PACE_PIN1 + AT – PACE_PUK1

	- PACE_PIN2 - PACE_PUK2 б) зчитувати дані, записані в БЕН, відповідно до рівня доступу, що використовується; с) перевіряти достовірність зчитаних даних відповідно до вимог ICAO та ДСТУ 4145. Спеціалізоване ПЗ повинно візуалізувати дані, отримані за результатом сканування, та дані, зчитані з БЕН. Спеціалізоване ПЗ повинно підписувати дані з використанням персонального електронного цифрового підпису (ЕЦП) користувача (особи) та введенням ПІН-коду (PIN-коду). Здійснювати запис змінної інформації у дозаписувані групи даних (DG32 - DG39). Здійснювати зміну PIN-коду 1, PUK-коду 1, PIN-коду 2 та PUK-коду 2.
1.4.4. Вимоги до спеціалізованого ПЗ модуля перевірки якості фотографій згідно з рекомендаціями ICAO	Спеціалізоване ПЗ повинно забезпечувати автоматизований аналіз зображень на предмет відповідності вимогам, що висуваються Міжнародною організацією цивільної авіації (<i>далі – ICAO</i>) та виконувати наступні функції: - зчитування даних обраного графічного файлу формату *.jpeg або *.gif; - обрахування характеристичних параметрів, що містять інформацію про загальні властивості зображення (освітленість, контрастність тощо) для обраного графічного файлу; - здійснення пошуку об'єктів - розпізнавання обличчя та його елементів на обраному графічному файлі; - обрахування параметрів знайдених графічних елементів для обраного графічного файлу; - встановлення відповідності (або невідповідності) зображення вимогам ICAO на основі отриманих параметрів та розробленої метрики; - повернення відповіді з інформацією про результат обробки. У випадку, якщо фото не відповідає вимогам, у відповіді зазначається ймовірна причина невідповідності. Спеціалізоване ПЗ повинно бути мультиплатформним з можливістю виконуватися під операційними системами Windows 8 і вище.
1.4.5. Вимоги до спеціалізованого ПЗ програмний додаток "Біометричні дані"	Спеціалізоване ПЗ повинно забезпечувати роботу через єдине меню окремих прикладних програм, призначених для взяття біометричних даних (параметрів) особи, реєстрації/зняття з реєстрації місць проживання/перебування громадян України, іноземців та осіб без громадянства під час надання послуг з оформлення документів.

	Спеціалізоване ПЗ повинно через єдине меню за допомогою окремих прикладних програм забезпечувати централізоване взяття біометричних даних (параметрів) особи: – відцифрованого образу обличчя; – відцифрованих відбитків пальців рук; – відцифрованого зразка підпису; – верифікації відбитків пальців. Спеціалізоване ПЗ повинно здійснювати авторизацію робочої станції для забезпечення її доступу до інформаційних ресурсів Державної міграційної служби України (Єдиного державного демографічного реєстру (ЄДДР)). Спеціалізоване ПЗ повинно в інтерфейсі web-сервісу виконання встановлених процедур та операцій з оформлення та видачі документів забезпечувати автоматизований віддалений обмін (з використанням відповідного протоколу) даними щодо особи між робочою станцією та ЄДДР. Спеціалізоване ПЗ повинно мати індикатор його роботи у вигляді відповідного значку у панелі повідомлень на екрані монітору робочої станції.
1.5. Вимоги до захисту інформації в РС1	Захист інформації в РС1 повинен забезпечуватись з урахуванням вимог до: – захищеного носія інформації; – ПЗ захищеного зберігання персональних даних; – ПЗ накладання цифрового підпису. Відповідні вимоги наведені в таблиці 2.
1.6. Вимоги до документації на РС1	До складу документації на РС1 повинна входити документація, що входить до відповідних компонентів постачання: апаратних та програмних. Документація передається Замовнику в електронному та/або паперовому вигляді.
1.7. Вимоги до надання послуг РС1	РС1 постачається Виконавцем з наданням наступних послуг: – з доставки обладнання апаратної компоненти; – з підключення та налаштування обладнання апаратної компоненти на об'єкті Замовника; – послуги з налаштування програмних компонентів (спеціалізованого ПЗ); – технічна підтримка спеціалізованого ПЗ не менше 12 місяців з дати встановлення та налаштування зазначеного ПЗ.

Таблиця 2 - Технічні вимоги до захисту інформації в робочих станціях усіх типів

3.1. Вимоги до захисту інформації в РС	Захист інформації в робочих станціях (РС1) повинен відповідати вимогам до: – захищеного носія інформації; – програмного забезпечення (ПЗ) захищеного зберігання персональних даних; – ПЗ накладання цифрового підпису.																															
3.1.1. Вимоги до захищеного носія інформації	Захищений носій інформації повинен відповідати наступним вимогам: – бути придатним до роботи в середовищі операційних систем сімейств Windows та Linux (версій операційних систем, що постачаються в рамках проекту); – здійснювати обчислення ключів та генерацію випадкової двійкової послідовності відповідно до вимог стандарту ДСТУ 4145-2002 (з використанням поліноміального базису) та RSA Cryptography Standard; – забезпечувати одночасне зберігання ключів та сертифікатів відкритих ключів відповідно до вимог стандартів ДСТУ 4145-2002, RSA Cryptography Standard; – забезпечувати формування електронного цифрового підпису (ЕЦП) відповідності до стандарту ДСТУ 4145-2002 за наступними показниками: <table><tr><th>Ключ</th><th>Швидкість</th></tr><tr><td>163 біт</td><td>до 100 мс</td></tr><tr><td>191 біт</td><td>до 100 мс</td></tr><tr><td>257 біт</td><td>до 100 мс</td></tr><tr><td>431 біт</td><td>до 550 мс</td></tr><tr><td>509 біт</td><td>–</td></tr></table> – забезпечувати формування ЕЦП у відповідності до RSA Cryptography Standard за наступними показниками: <table><tr><th>Ключ</th><th>Швидкість</th></tr><tr><td>512 біт</td><td>–</td></tr><tr><td>1024 біт</td><td>до 150 мс</td></tr><tr><td>1536 біт</td><td>до 400 мс</td></tr><tr><td>2048 біт</td><td>до 900 мс</td></tr></table> – здійснювати обчислення ключів з наступними довжинами: <table><tr><th>Алгоритм</th><th>Мін.</th><th>Макс.</th></tr><tr><td>ДСТУ 4145</td><td>163 біт</td><td>431 біт</td></tr><tr><td>RSA</td><td>1024 біт</td><td>2048 біт</td></tr></table> – виконувати криптографічні операції в захищеній пам'яті захищеного носія;	Ключ	Швидкість	163 біт	до 100 мс	191 біт	до 100 мс	257 біт	до 100 мс	431 біт	до 550 мс	509 біт	–	Ключ	Швидкість	512 біт	–	1024 біт	до 150 мс	1536 біт	до 400 мс	2048 біт	до 900 мс	Алгоритм	Мін.	Макс.	ДСТУ 4145	163 біт	431 біт	RSA	1024 біт	2048 біт
Ключ	Швидкість																															
163 біт	до 100 мс																															
191 біт	до 100 мс																															
257 біт	до 100 мс																															
431 біт	до 550 мс																															
509 біт	–																															
Ключ	Швидкість																															
512 біт	–																															
1024 біт	до 150 мс																															
1536 біт	до 400 мс																															
2048 біт	до 900 мс																															
Алгоритм	Мін.	Макс.																														
ДСТУ 4145	163 біт	431 біт																														
RSA	1024 біт	2048 біт																														

	- забезпечувати неможливість здійснення експорту особистих ключів, що формувалися на захищеному носії, зберігаються на захищеному носії та мають відповідний атрибут; - об'єм захищеної пам'яті захищеного носія має становити не менш 210 Кб; - забезпечувати взаємодію з Microsoft Base Smart Card Crypto Provider через комплект драйверів Smart Card Mini-Driver захищеного носія; - забезпечувати можливість збереження довільних даних користувача; - постачатися разом з комплектом засобів розробки (SDK) за необхідності; - інтерфейс носія повинен відповідати вимогам стандарту PKCS#1 v2.30: "Cryptographic Token Interface Standard". Захищений носій інформації повинен мати позитивний експертний висновок Державної служби спеціального зв'язку та захисту інформації України (далі - <i>Держспецзв'язку України</i>) за результатами державної експертизи в сфері криптографічного захисту інформації (<i>КЗІ</i>) щодо відповідності вимогам нормативних документів системи КЗІ України. Захищений носій інформації повинен бути представлений у формі фактора USB-токен, який при взаємодії з комп'ютером повинен забезпечувати підтримку протоколів Windows PC\SC, CCID, ISO 7816.
3.1.2. Вимоги до ПЗ захищеного зберігання персональних даних	В якості ПЗ захищеного зберігання персональних даних повинен використовуватись програмний засіб криптографічного захисту інформації на інформаційних носіях. При цьому ПЗ захищеного зберігання персональних даних повинно відповідати наступним вимогам: - мати позитивний експертний висновок Держспецзв'язку України з результатами державної експертизи в сфері КЗІ щодо відповідності вимогам нормативних документів системи КЗІ України або листу гарантуючий проведення відповідної державної експертизи отриманням позитивного експертного висновку на момент постачання ПЗ; - бути призначеним для забезпечення конфіденційності та цілісності інформації шляхом здійсненні її криптографічного перетворення (виконання функцій шифрування та дешифрування) та здійснювати розмежування доступу до такої інформації, що зберігається на носії інформації (жорсткий диск комп'ютера, переносний жорсткий диск, флеш-накопичувач) відповідно до ключових даних та сертифікатів відкритих ключів; - бути призначеним для використання в складі середовища операційної системи сімейства Windows, а саме: Microsoft Windows XP (x86/x64), Microsoft Windows Server 2003 (x86/x64), Microsoft Vista (x86/x64), Microsoft Windows 7 (x86/x64), Microsoft Windows Server 2008 R2, Microsoft Windows 8 (x86/x64), Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2; - мати можливість: • використання у складі автоматизованих систем (АС) класів 1, 2, 3; • застосування для обробки інформації з обмеженим доступом (конфіденційної, службової), у тому числі такої, вимога щодо захисту якої встановлена законом; • реалізації у вигляді набору програмних модулів, готових до використання (написаних на мові програмування C, C++);

- використання у складі будь-якої інформаційної системи (або АС) якості її окремої та незалежної частини (складової) з визначени переліком функцій;
- реалізувати наступні механізми:
 - контролю цілісності ПЗ;
 - захисту від порушення конфіденційності інформації внаслідок помилкових дій користувача або в разі відхилень у роботі складових елементів ПЗ;
 - захисту ключових даних на їх носіях від несанкціонованого зчитування;
 - захисту від здійснення порушником навмисного зовнішнього впливу;
 - захисту від порушення конфіденційності та цілісності ключових даних на ключових документах;
- складатися з наступних компонентів:
 - створення шифрованих контейнерів;
 - адміністрування шифрованих контейнерів;
 - драйвер роботи з шифрованими контейнерами;
- реалізувати наступні криптографічні алгоритми:
 - шифрування даних відповідно до ДСТУ ГОСТ 28147 у режимі гамування із зворотнім зв'язком;
 - шифрування даних з контролем цілісності відповідно до ДСТУ ГОСТ 28147 у режимі імітовставки для розподілу ключових даних;
 - гешування інформації відповідно до ГОСТ 34.311-95;
 - перевірки ЕЦП в поліноміальному базисі відповідно до ДСТУ 414:2002;
- реалізація криптографічних алгоритмів повинна здійснюватися бібліотекою функцій криптографічних перетворень, що має позитивний експертний висновок Держспецзв'язку України з результатами державної експертизи в сфері КЗІ або лист, гарантуючий проведення відповідної державної експертизи з отримання позитивного експертного висновку на момент постачання ПЗ;
- реалізувати наступні формати, структури, протоколи, алгоритми:
 - списку відкликаних сертифікатів відповідно до вимог RFC 528 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" та вимог до формату списку відкликаних сертифікатів, затверджених наказом Мін'юсту України та Адміністрації Держспецзв'язку України від 20 серпня 2012 р. №1236/5/453, зареєстрованим в Мін'юсті України 20 серпня 2012 р. за №1400/21712;
 - об'єктні ідентифікатори для криптоалгоритмів, що є державними стандартами відповідно до вимог до структури об'єктних ідентифікаторів для криптоалгоритмів, затверджених наказом Мін'юсту України та Адміністрації Держспецзв'язку України від 20 серпня 2012 р. №1236/5/453, зареєстрованим в Мін'юсті України 20 серпня 2012 р. за №1399/21711;
 - криптографічних повідомлень, що створюються та обробляються об'єктом експертизи, відповідають вимогам RFC 565 "Cryptographic Message Syntax (CMS)", вимогам до формату криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України від 18 грудня 2012 р. №73, зареєстрованим в Мін'юсті України 14 січня 2013 р. за №108/2264

	• посиленого сертифіката відкритого ключа відповідає вимогам д формату посиленого сертифіката відкритого ключа, затверджені наказом Мін'юсту України та Адміністрації Держспецзв'язк України від 20 серпня 2012 р №1236/5/453, зареєстрованим Мін'юсті України 20 серпня 2012 р. за №1398/21710. - забезпечити: • можливість використання ПЗ одночасно декількома користувачам із забезпеченням розмежування доступу до інформації на підста ключових даних та сертифікатів відкритих ключів; • можливість керування повноваженнями користувачів щод одержання доступу до ПЗ; • можливість використання ключових даних користувача ПЗ, ш зберігаються ключовому документі; • безпечний механізм відновлення даних користувача ПЗ у випадк компрометації його ключових даних без погіршення властивосте безпеки такої інформації; • ідентифікацію особи користувача ПЗ на підставі сертифікат відкритого ключа; • створення та використання шифрованих файлових контейнер (шифрованих віртуальних дисків); • створення шифрованих контейнерів без файлової системи або файловою системою NTFS чи FAT; • можливість створення динамічних шифрованих файлови контейнерів; • створення переносного диску з шифрованими файловим контейнерами та компонентами ПЗ на борту переносного жорстког диску, флеш-накопичувачі; • створення шифрованого носія на основі переносного жорстког диску, флеш-накопичувача; • роботу ПЗ у якості "процесу-служби" для використання пі управлінням серверних операційних систем сімейства Windows; • використання одночасно понад десяти шифрованих контейнерів; • можливість роботи з використанням "майстер-ключ"; • можливість роботи з використанням списків відкликани сертифікатів або без таких; • можливість здійснення адміністративних налаштувань лише особ що має відповідні повноваження; • підтримку роботи шифрованих контейнерів шляхом використанн драйверу у фоновому режимі; • використання довгострокового ключового елемента, отриманого ві Держспецзв'язку України, або довгострокового ключовог елемента, що зазначений у відповідному переліку; • можливість шифрування логічних дисків (томів) жорсткого диск комп'ютера, переносного жорсткого диску, флеш-накопичувача.
3.1.3. Вимоги до ПЗ накладання цифрового підпису	ПЗ накладання цифрового підпису повинно відповідати наступни вимогам: - повинно забезпечувати виконання функцій накладання та перевірк ЕЦП блоків даних (обчислення ЕЦП), шифрування та дешифруванн блоків даних, генерації ключових даних (формуванн криптографічних ключів – особистих ключів та відповідних ї відкритих ключів) у складі АС будь-якого класу; - за своїм призначенням відноситись до категорій "Ш", "К" та "П";

- за видом виконання – "Б", підвид – "Б2" (програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під управлінням);
- за класом – "Б2" (відповідає вимогам забезпечення стійкості криптографічних перетворень в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня
- бути реалізовано у вигляді набору програмних модулів (компонентів) готових до використання, написаних на мові програмування Java;
- мати можливість бути використаним у складі будь-якої інформаційної системи (або АС), яка реалізована у якості портального рішення. Функціонувати у якості її окремої та незалежної частини з визначеним переліком функцій.

ПЗ накладання цифрового підпису повинно реалізовувати наступні механізми:

- контроль цілісності ПЗ;
- тестування на правильність функціонування та блокування роботи разі виявлення порушень;
- захист від порушення конфіденційності інформації внаслідок помилкових дій користувача або в разі відхилень у роботі складових елементів ПЗ;
- розмежування доступу до функцій ПЗ, криптографічної схеми та ключових даних;
- захист ключових даних на їх носіях від несанкціонованого зчитування;
- захист ПЗ від здійснення порушником навмисного зовнішнього впливу;
- захист від порушення конфіденційності та цілісності ключових даних на ключових документах.

Вимоги до клієнтської компоненти ПЗ накладання цифрового підпису:

- клієнтська компонента повинна забезпечувати:
 - графічний інтерфейс користувача;
 - інтерфейс взаємодії з сторонніми прикладними системами;
 - інтерфейс для взаємодії з компонентою веб-додатка;
- клієнтська компонента повинна:
 - мати можливість одержання для оброблення блоку даних безпосередньо від прикладної системи (API або компоненти веб-додатка), або з визначеного користувачем місця (графічний інтерфейс користувача);
 - повинна забезпечувати повернення обробленого блоку даних безпосередньо до прикладної системи, або виконати збереження обробленого блоку даних у визначене користувачем місце;
 - повинна забезпечити реалізацію функцій накладання ЕЦП:
 - одержаний від прикладної системи блок даних та здійснення перевірки ЕЦП, одержаного від прикладної системи блоку даних, та значення ЕЦП такого блоку даних;
 - забезпечити реалізацію функцій шифрування одержаного від прикладної системи блоку даних та здійснення дешифрування одержаного від прикладної системи шифрованого блоку даних;
 - забезпечити обчислення ЕЦП, одержаного блоку даних у вигляді файлу, що зберігається на носії інформації, та блоку даних (для роботи через API або компоненту веб-додатка);

- клієнтська компонента повинна забезпечити передачу до прикладної системи (за відповідним запитом), за результатом виконання операції з перевірки ЕЦП:
 - відомостей щодо коректності отриманих від прикладної системи даних;
 - відомостей про результат перевірки ЕЦП;
 - відомостей, що містяться в полі "Підписувач" ("subject") посиленого сертифіката відкритого ключа відповідно з використанням якого було здійснено накладання ЕЦП;
 - час накладання ЕЦП;
- клієнтська компонента повинна забезпечити реалізацію наступних варіантів використання функцій накладання та перевірки ЕЦП:
 - блок даних та підпис знаходяться разом;
 - підпис знаходиться окремо від даних;
- клієнтська компонента повинна забезпечувати інтерфейс взаємодії різними акредитованими центрами сертифікації ключів з протоколами Online Certificate Status Protocol (**OCS**P) та Time-Stamp Protocol (**TSP**) для:
 - перевірки статусу посиленого сертифіката відкритого ключа в режимі реального часу;
 - отримання позначки часу;
- клієнтська компонента повинна забезпечувати можливість перевірки поточного статусу сертифіката із використанням механізму списку відкликаних сертифікатів (Certificate Revocation List);
- клієнтська компонента повинна забезпечити реалізацію функцій:
 - генерування ключових даних на ключовий документ (особистий та відповідний йому відкритий ключ);
 - генерування запиту на формування сертифіката відкритого ключа (за стандартом PKCS#10 Certification Request Syntax Specification);
- з метою реалізації "безпечного" режиму функціонування клієнтської компоненти повинна забезпечити:
 - контроль цілісності власних файлів та бібліотек;
 - реєстрацію подій, що класифікуються як "системні помилки" або помилки функціонування допоміжного програмного забезпечення
 - реєстрацію подій, пов'язаних з навмисними або ненавмисними помилковими діями користувачів;
- клієнтська компонента повинна забезпечити реєстрацію наступних вдалих подій обробки даних:
 - вдалі операції з накладання та перевірки ЕЦП;
 - вдалі операції з шифрування та дешифрування даних;
 - факти оновлення списку відкликаних сертифікатів;
 - факт отримання за OSCP відповіді щодо статусу сертифіката відкритого ключа;
 - факт отримання позначки часу;
- клієнтська компонента повинна взаємодіяти з носіями ключової інформації по інтерфейсу, що реалізований відповідно до PKCS#1 Cryptographic Token Interface (Cryptoki).

Специфікація

Робоча станція для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, з комплектом обладнання для зняття біометричних даних (параметрів) особи, реєстрації/зняття з реєстрації місць проживання/перебування громадян України, іноземців та осіб без громадянства

№	Найменування	Од.	Кіль-ть
	Робоча станція для оформлення та видачі паспорта громадянина України для виїзду за кордон з електронним носієм або паспорта громадянина України у формі картки		
1	Робоча станція з комплектом обладнання, встановленим спеціалізованим програмним забезпеченням та комплексом засобів захисту інформації у складі:	шт.	2
	<i>Персональний комп'ютер з встановленим загальним програмним забезпеченням:</i>		
	Системний блок Intel DC 3,3 GHz / 4 Gb / 500 Gb / Video з 2-ма виходами для підключення 2-х моніторів / Клавіатура / Миша / Win 10 Pro / Антивірусне ПЗ	шт.	2
	Монітор TN 21.5", VGA	шт.	2
	Монітор TN 21.5", VGA/DVI	шт.	2
	Кабель DVI для монітора 1,8 м	шт.	2
	Багатофункціональний пристрій A4 ч/б	шт.	2
	Кабель USB для багатофункціонального пристрою 3,0 м	шт.	2
	Цифровий блок для введення ПІН-кодів	шт.	2
	Концентратор 7 портів USB 2.0 з блоком живлення	шт.	2
	Джерело безперебійного живлення 1000 ВА	шт.	2
	Мережевий фільтр для підключення, 6 розеток - 2 шт.	к-т	2
	<i>Комплект обладнання для взяття біометричних даних (параметрів) особи:</i>		
	Дзеркальна фотокамера з мережевим блоком живлення; комплект фотоаксесуарів (штатив для фотокамери; штатив для спалаху; спалах для фотокамери D-120 з тримачем - 2 шт.; кріплення для спалаху та парасолі; комплект синхронізаторів (ресивер; 2 трансмітери); парасолька для спалаху з діаметром 84 см; фон тканевий білий 1,35 м x 1,0 м)	шт.	2

	Зчитувач відбитків пальців Dermalog ZF1	шт.	2
	Планшет для підпису Wacom	шт.	2
	Зчитувач документів Dermalog XF9e	шт.	2
	Спеціалізоване програмне забезпечення (СПЗ):		
	Програмне забезпечення для проведення первинного логічного контролю якості та коректності отримання персональних даних відповідно до вимог ISO. В-2.0	ліц.	2
	Програмне забезпечення верифікації/ідентифікації по відбиткам пальців (один до одного, один до багатьох - AFIS). В-2.0	ліц.	2
	Спеціалізоване програмне забезпечення отримання персональних даних та реалізації механізмів контролю доступу до БЕН. В-2.0	ліц.	2
	Модуль перевірки якості фотографій згідно з рекомендаціями ICAO	ліц.	2
	Невиключна ліцензія на використання програмного додатку "Біометричні дані"	ліц.	2
	Комплекс засобів захисту інформації (КЗЗІ) у складі:		
	Засіб криптографічного захисту інформації - носій ключової інформації "ЕфітKey"	ліц.	4
	Засіб програмний криптографічного захисту інформації на інформаційних носіях "КриптософтStorage"	ліц.	2
	Засіб програмний криптографічного захисту інформації "Крипто Автограф". Програмний модуль - "Клієнт"	ліц.	2
2	Послуги з доставки, підключення, налаштування обладнання, СПЗ та КЗЗІ		2
3	Технічна підтримка СПЗ на рік		2

У разі, якщо дані технічні вимоги та специфікація товару містять посилання на конкретну марку, фірму, патент, конструкцію або тип товару, то вважається, що технічні вимоги та специфікація товару містять вираз "або еквівалент".