Рекомендації щодо отримання послуг електронного цифрового підпису органами державної влади та місцевого самоврядування, підприємствами, установами державної форми власності для роботи з Єдиними та Державними реєстрами Міністерства юстиції України та іншими інформаційними системами

Відповідно до Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженого Постановою Кабінету Міністрів України від 28 жовтня 2004 р. №1452, наказом керівника органу державної влади, органу місцевого самоврядування, підприємства, установи державної форми власності, що є юридичною особою (далі - установа), визначається підрозділ інформаційних технологій, а у разі відсутності такого - підрозділ, що виконує відповідні функції (далі - відповідальний підрозділ), або **відповідального працівника**, що буде здійснювати забезпечення застосування електронного цифрового підпису в установі.

Для отримання послуг електронного цифрового підпису в Акредитованому центрі сертифікації ключів органів юстиції України необхідно:

1. Кожній особі, яка буде користуватись електронним цифровим підписом (підписувач), ознайомитись з Регламентом роботи Акредитованого центру сертифікації ключів органів юстиції України.
2. Завантажити та встановити на робочому місці програмне забезпечення надійного засобу електронного цифрового підпису "ІІТ Користувач ЦСК-1".
3. Ознайомитись з Настановою користувача програмного забезпечення "ІІТ Користувач ЦСК-1".
4. Особі, яка буде користуватись електронним цифровим підписом, **самостійно** здійснити генерацію та збереження **особистого ключа** та **запитів на формування сертифікатів** відкритих ключів відповідно до Настанови користувача.

УВАГА! Забороняється довіряти генерацію ключів іншим особам! Особистий ключ та запити на формування сертифікатів відкритих ключів повинні зберігатись на різних носіях інформації! Носій інформації із особистим ключем зберігається у таємниці та не передається іншим особам. Передача носія інформації із особистим ключем стороннім особам, вважається його компрометацію.

Під час генерації запити на формування сертифікатів відкритих ключів слід зберігати у форматі:

«EU-XXXXXXXX-Прізвище.p10» та

«EU-KEP-XXXXXXXX-Прізвище.p10», де

Прізвище – прізвище підписувача без ініціалів;

EU-XXXXXXXX.p10 та EU-KEP-XXXXXXXX.p10 – унікальні імена файлів запитів, що формуються програмним забезпеченням "ІІТ Користувач ЦСК-1" автоматично під час генерації особистого ключа. Для збереження файлів необхідно до унікальних імен додати прізвище підписувача, наприклад:

EU-69PH0S9W-Іванчик.p10 та

EU-KEP-69PH0S9W-Іванчик.p10.

У разі коли згідно із законодавством необхідне засвідчення печаткою справжності підпису на документах та відповідності копій документів оригіналам, установа застосовує спеціально призначений для таких цілей електронний цифровий підпис (далі - **електронна печатка**).

Установа застосовує електронну печатку лише за наявності у неї відповідної печатки, що застосовується для документів на папері.

У сертифікаті відкритого ключа, що використовується установою для електронної печатки, додатково зазначається спеціальне призначення електронного цифрового підпису та сфера його застосування, а також відтворюється текстова інформація, розміщена на відповідній печатці.

Право проставлення електронної печатки на електронних документах надається лише тому працівнику установи, який проставляє відповідну печатку на документах на папері.

Особі, яка буде використовувати електронну печатку, необхідно **самостійно** здійснити генерацію та збереження **особистого ключа** та **запитів на формування сертифікатів** відкритих ключів електронної печатки відповідно до Настанови користувача.

Для збереження файлів запитів на формування сертифікатів відкритих ключів електронної печатки установи необхідно до унікальних імен додати слова «електронна печатка», наприклад:

EU-70PH0S9W-електронна печатка.p10 та

EU-KEP-70PH0S9W-електронна печатка.p10.

5. Заповнити, підписати у уповноваженого керівника установи та засвідчити печаткою **Заяву про реєстрацію**.

6. Підготувати документи, необхідні для ідентифікації та автентифікації заявників та підписувачів в Акредитованому центрі сертифікації ключів:

надаються одноразово або у разі виникнення змін:

- оригінал установчого документу установи (статут, положення, рішення про створення тощо) або його нотаріально засвідчена копія (надається виключно для ознайомлення). У разі державної реєстрації установи після 01.01.2016 подається копія опису із відміткою про код доступу до порталу електронних сервісів юридичних осіб, фізичних осіб - підприємців та громадських формувань. Якщо не має можливості відтворити установчий документ, установою подається відповідний лист (зразок тут);
- копія документа, що підтверджує повноваження керівника установи, засвідчена підписом уповноваженого працівника та печаткою кадрової служби, або підписом керівника та печаткою установи: копія наказу про призначення на посаду, витяг з наказу про призначення на посаду тощо;
- копія наказу керівника установи про визначення відповідального працівника/підрозділу, на якого/який покладено обов'язки забезпечення застосування електронного цифрового підпису в установі (зразок тут), завірена підписом керівника або уповноваженої особи установи та печаткою установи (у разі звернення безпосередньо керівника установи цей документ не надається);
- оригінал (для ознайомлення, подається кожного разу при зверненні) та копія паспорта відповідальної особи, на яку покладено обов'язки забезпечення застосування електронного цифрового підпису в установі або керівника установи, у разі звернення безпосередньо керівника установи (копії 1-2 сторінок (3-6 за наявності відміток)), засвідчена підписом власника (надається одноразово або у разі виникнення змін). При наявності паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в Єдиному державному демографічному реєстрі, надається оригінал та копія даного документа.

надаються щодо кожного підписувача кожного разу при зверненні:

- копія паспорта підписувача (копії 1-2 сторінок (3-6 за наявності відміток)), засвідчена підписом власника. Якщо підписувач має паспорт громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в Єдиному державному демографічному реєстрі, надається копія даного документа;
- копія облікової картки платника податків підписувача, засвідчена підписом власника. Якщо через релігійні переконання фізична особа відмовилась від реєстраційного номеру облікової картки платника податків, додатково подається копія сторінки паспорту з відміткою про таку відмову, завірена підписом власника.

УВАГА! Під час підготовки документів звернути увагу на недопущення підчисток, дописок від руки у машинописний текст, закреслених слів, написів олівцем, а також пошкоджень, внаслідок яких неможливо прочитати текст.

7. Державним підприємствам необхідно сплатити 100% вартості послуг за **квитанцією.**

УВАГА! Формування посиленого сертифіката відкритого ключа для державних підприємств здійснюється після отримання оплати послуг ЕЦП від заявника у розмірі, згідно тарифного плану.

8. Відповідальному працівнику, який буде здійснювати забезпечення застосування електронного цифрового підпису в установі, звернутись до найближчого офісу Акредитованого центру сертифікації ключів із згаданим вище пакетом документів **та запитами на формування сертифікатів відкритих ключів** за отриманням послуги формування сертифікатів відкритих ключів.

9. Послуги з формування сертифікатів відкритих ключів підписувачів та обслуговування сертифікатів (розповсюдження, скасування, зберігання, блокування та поновлення) здійснюються відповідно до Регламенту роботи Акредитованого центру сертифікації ключів органів юстиції України.