ПОГОДЖЕНО

Перший заступник Міністра цифрової трансформації України

_____ О. ВИСКУБ
(Підписано кваліфікованим електронним підписом)

ЗАТВЕРДЖУЮ

Міністр внутрішніх справ України

_____ І. КЛИМЕНКО
(Підписано кваліфікованим електронним підписом)

.

РЕГЛАМЕНТ РОБОТИ

КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ – АКРЕДИТОВАНОГО ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

На 154 аркушах

Київ 2025

ЗМІСТ

ВСТУП

Перелік скорочень

БЕН	безконтактний електронний носій
ВПР	відокремлений пункт реєстрації
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄІС МВС	єдина інформаційна система Міністерства внутрішніх справ України
Засіб КЕП	засіб кваліфікованого електронного підпису чи печатки
ІКС	інформаційно-комунікаційна система
КЕД послуга	кваліфікована електронна довірча послуга
КЕП	кваліфікований електронний підпис чи печатка
КЗІ	криптографічний захист інформації
КНЕДП	надавач кваліфікованих електронних довірчих послуг
КНЕДП АЦСК МВС	– кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів Міністерства внутрішніх справ України
МВС	Міністерство внутрішніх справ України
ОС	операційна система
ПЗ	програмне забезпечення
ПТК	програмно-технічний комплекс
РНОКПП	реєстраційний номер облікової картки платника податків
УНЗР	унікальний номер запису в ЄДДР
ЦОД	Центр обробки даних
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol TSP Time Stamp Protocol

Терміни та визначення

У Регламенті роботи кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України (далі – Регламент) терміни та визначення вживаються у значенні, наведеному в законах України «Про електронну ідентифікацію та електронні довірчі послуги», «Про електронні документи та електронний документообіг», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», постанові Кабінету Міністрів України від 28.06.2024 2024 р. № 764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг», інших нормативно-правових актах, у сферах електронної ідентифікації та електронних довірчих послуг, та з питань криптографічного та технічного захисту інформації.

Статус Регламенту

Цей Регламент є документом КНЕДП – АЦСК МВС, що визначає організаційно-методологічні, технічні та технологічні умови діяльності КНЕДП – АЦСК МВС під час надання КЕД послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Регламент розроблений відповідно до:

– Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (із змінами) (далі - Закон);

– Закону України «Про електронні документи та електронний документообіг» (із змінами);

– Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань» (із змінами);

– Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»;

– постанови Кабінету Міністрів України від 28.06.2024 2024 № 764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»;

– постанови Кабінету Міністрів України від 01.08.2023 № 798 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»;

– постанови Кабінету Міністрів України від 30.11.2016 № 869 «Про затвердження Порядку внесення засобів кваліфікованого електронного підпису до безконтактного електронного носія, що міститься в паспорті громадянина України, та надання кваліфікованих електронних довірчих послуг з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм» (зі змінами);

– постанови Кабінету Міністрів України від 23.07.2024 р. № 842 «Про затвердження переліку документів та електронних даних, отриманих у зв’язку з наданням електронних довірчих послуг, що підлягають постійному зберіганню, та Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг»;

– постанови Кабінету Міністрів України від 10.12.2024 №1408 «Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг»;

– наказу Міністерства внутрішніх справ України від 27.03.2018 № 238 «Про затвердження Порядку взаємодії кваліфікованого надавача електронних довірчих послуг — акредитованого центру сертифікації ключів Міністерства внутрішніх справ України та Державної міграційної служби України під час надання кваліфікованих електронних довірчих послуг з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм», зареєстрованого в Міністерстві юстиції України 19 квітня 2018 р. за № 475/31927;

– наказу Міністерства цифрової трансформації України від 05.12.2022 року № 130 «Про затвердження Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування», зареєстрованого в Міністерстві юстиції України 20 січня 2023 року за № 129/39185;

– наказ Міністерства цифрової трансформації України від 18 лютого 2024 № 12 «Про затвердження Особливостей надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката шифрування», зареєстрований в Міністерстві юстиції України 05 лютого 2024 р. за № 176/41521;

– інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Положення Регламенту поширюються на:

– працівників центрального офісу КНЕДП – АЦСК МВС;
– працівників ВПР КНЕДП – АЦСК МВС;
– користувачів (заявників, підписувачів, створювачів електронних печаток, які на підставі договору отримують КЕД послуги в КНЕДП – АЦСК МВС).

Положення Регламенту є обов'язковими для виконання працівниками центрального офісу КНЕДП – АЦСК МВС та ВПР КНЕДП – АЦСК МВС, а також для користувачів в частині, що їх стосується.

Визнання положень цього Регламенту користувачами КЕД послуг є обов'язковою умовою та підставою для укладання з ними Договору про надання кваліфікованих електронних довірчих послуг (договір приєднання) (далі - Договір).

Положення цього Регламенту засновані на принципах дотримання прав та виконання обов'язків суб'єктами надання та отримання КЕД послуг, наведені в Законі.

Будь яка зацікавлена особа може ознайомитися з положеннями Регламенту на офіційному веб-сайті КНЕДП – АЦСК МВС, в центральному офісі КНЕДП – АЦСК МВС та офісах ВПР КНЕДП – АЦСК МВС.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила ніж ті, що передбачені цим Регламентом, застосовуються правила міжнародного договору.

Внесення змін та доповнень до Регламенту

Погодження, внесення змін та доповнень до цього Регламенту здійснюється КНЕДП – АЦСК МВС відповідно до Закону.

Про внесення змін та доповнень до цього Регламенту КНЕДП – АЦСК МВС повідомляє своїх користувачів, інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному веб-сайті КНЕДП – АЦСК МВС.

Всі зміни та доповнення, внесені КНЕДП – АЦСК МВС до Регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом в силу відповідних нормативно-правових актів, але не раніше моменту опублікування змін на офіційному веб-сайті КНЕДП – АЦСК МВС.

Всі зміни та доповнення, внесені КНЕДП – АЦСК МВС до цього Регламенту, що не пов'язані зі зміною законодавства, набувають чинності через 10 (десять) календарних днів з дня розміщення зазначених змін і доповнень на офіційному веб-сайті КНЕДП – АЦСК МВС.

Всі зміни та доповнення, внесені КНЕДП – АЦСК МВС до цього Регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом в силу відповідних нормативно - правових актів, але не раніше моменту опублікування змін до цього Регламенту на офіційному веб-сайті КНЕДП – АЦСК МВС.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КНЕДП – АЦСК МВС

Повні найменування юридичної особи: Міністерство внутрішніх справ України, the Ministry of Internal Affairs of Ukraine.

Скорочені найменування юридичної особи: МВС України, the MIAU.

Повні найменування КНЕДП – АЦСК МВС: кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів Міністерства внутрішніх справ України, Qualified Trust Services Provider – Certification Authority of the Ministry of Internal Affairs of Ukraine.

Скорочені найменування КНЕДП – АЦСК МВС: КНЕДП – АЦСК МВС України, QTSP of the MIAU.

Юридична адреса КНЕДП – АЦСК МВС: Україна, 00024, м. Київ, вул. Богомольця Академіка, 10.

Поштова адреса центрального офісу КНЕДП – АЦСК МВС: Україна, 00024, м. Київ, вул. Богомольця Академіка, 10.

Адреса розміщення центрального офісу КНЕДП – АЦСК МВС: Україна, 00024, м. Київ, вул. Богомольця Академіка, 10.

Адреси місцезнаходжень ВПР КНЕДП – АЦСК МВС розміщуються на офіційному веб-сайті КНЕДП – АЦСК МВС.

Телефон: +38 (044) 254-77-55.

Код ЄДРПОУ: 00032684.

Електронна адреса офіційного веб-сайту КНЕДП – АЦСК МВС: https://ca.mvs.gov.ua.

Адреса електронної пошти центрального офісу КНЕДП – АЦСК МВС: ca@mvs.gov.ua.

Центральний офіс КНЕДП – АЦСК МВС представлений окремим структурним підрозділом Міністерства внутрішніх справ України, що забезпечує організацію надання КЕД послуг представництвами КНЕДП – АЦСК МВС та забезпечує виконання вимог законодавства до кваліфікованих надавачів електронних довірчих послуг.

Представництвами КНЕДП – АЦСК МВС є ВПР КНЕДП – АЦСК МВС, що представлені окремими підрозділами або територіальними органами Міністерства внутрішніх справ України, або юридичними чи фізичними особами, які на підставі наказу або договору, укладеним з Міністерством внутрішніх справ України, здійснюють реєстрацію користувачів КЕД послуг з дотриманням вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг та захисту інформації.

Договір укладається від імені Міністерства внутрішніх справ України.

2. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

До КЕД послуг, які надає КНЕДП – АЦСК МВС, відносяться:

КЕД послуга створення, перевірки та підтвердження КЕП;

КЕД послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, шифрування (далі – кваліфікований сертифікат);

КЕД послуга формування, перевірки та підтвердження чинності кваліфікованої електронної позначки часу.

.

3. ПЕРЕЛІК ПОСАД ТА ФУНКЦІОНАЛЬНІ ОБОВ'ЯЗКИ ПРАЦІВНИКІВ КНЕДП – АЦСК МВС

До складу центрального офісу КНЕДП – АЦСК МВС, посадові обов'язки якого безпосередньо пов'язані з наданням КЕД послуг, входять працівники Департаменту інформатизації Міністерства внутрішніх справ України, на яких покладено функціональні обов'язки:

- керівника КНЕДП – АЦСК МВС;
- адміністратора реєстрації;
- адміністратора сертифікації;
- адміністратора безпеки;
- аудитора системи;
- системного адміністратора.

Детальний опис обов'язків персоналу КНЕДП – АЦСК МВС визначено в пункті 5.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України (додаток 1 до Регламенту) (далі – Політика сертифіката).

До складу працівників ВПР КНЕДП – АЦСК МВС входять працівники Департаменту інформатизації Міністерства внутрішніх справ України, територіальних органів МВС, підрозділів центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, закладів, установ чи підприємств, що належать до сфер їх управління, а також юридичних осіб, які на підставі наказу або договору з МВС здійснюють надання КЕД послуг.

На працівників ВПР КНЕДП – АЦСК МВС покладено функціональні обов'язки:

- керівника відокремленого пункту реєстрації;
- адміністратора реєстрації відокремленого пункту реєстрації (далі – віддалений адміністратор реєстрації);
- відповідального за захист інформації на відокремленому пункті реєстрації.

Детальний опис обов'язків посадових осіб ВПР КНЕДП – АЦСК МВС визначено в пунктах 5.3.1 - 5.3.5 Політики сертифіката.

4. ПОЛІТИКА СЕРТИФІКАТА ТА ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ

ПРАКТИК

4.1. Політика сертифіката

4.1.1. Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів, сформованих КНЕДП – АЦСК МВС

Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів визначено в пункті 1.4.1 Політики сертифіката.

4.1.2. Обмеження щодо використання кваліфікованих сертифікатів, сформованих КНЕДП – АЦСК МВС

Обмеження щодо використання кваліфікованих сертифікатів визначено в пункті 1.4.2 Політики сертифіката.

4.1.3. Перелік інформації, що розміщується КНЕДП – АЦСК МВС на офіційному веб-сайті

В пункті 2.2 Політики сертифіката наведено перелік інформації, доступ до якої забезпечує КНЕДП – АЦСК МВС через офіційний веб-сайт.

4.1.4. Час та порядок публікації кваліфікованих сертифікатів та списків відкликаних сертифікатів

Час та порядок публікації кваліфікованих сертифікатів та списків відкликаних сертифікатів визначено в пункті 2.3 Політики сертифіката.

4.1.5. Механізм підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката

Механізм підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката, визначено в пункті 3.2.1 Політики сертифіката.

4.1.6. Умови встановлення користувачів, ВПР

Умови встановлення користувачів (автентифікації особи) визначено в пункті 3.2.2 Політики сертифіката, пунктах 3.2.2, 3.2.3 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до Регламенту) (далі - Положення сертифікаційних практик).

Підтвердження повноважень уповноваженого представника юридичної особи визначено в пункті 3.2.4 Політики сертифіката та пункті 3.2.5 Положення сертифікаційних практик.

4.1.7. Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС

Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС визначено в пункті 3.3 Політики сертифіката та пункті 3.3 Положення сертифікаційних практик.

4.1.8. Механізми автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката

Механізм автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката визначено в пункті 3.4 Політики сертифіката та пункті 3.4 Положення сертифікаційних практик.

4.1.9. Опис фізичного середовища

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

4.1.10. Процедурний контроль

Положення щодо процедурного контролю визначені в пункті 5.2 Політики сертифіката.

4.1.11. Порядок ведення журналів аудиту подій

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

4.1.12. Порядок ведення архівів КНЕДП – АЦСК МВС

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

4.1.13. Процес, порядок та умови генерації пар ключів КНЕДП – АЦСК МВС та користувачів

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

4.1.14. Процедури отримання користувачем особистого ключа в результаті надання КЕД послуги КНЕДП – АЦСК МВС

Процедури отримання користувачем особистого ключа в результаті надання КЕД послуги визначена в пункті 6.1.2 Політики сертифіката.

4.1.15. Механізм надання відкритого ключа користувача КНЕДП – АЦСК МВС для формування кваліфікованого сертифіката

Механізм надання відкритого ключа користувача КНЕДП – АЦСК МВС для формування кваліфікованого сертифіката визначено у пункті 6.1.3 Політики сертифіката.

4.1.16. Порядок захисту та доступу до особистого ключа КНЕДП – АЦСК МВС

Цей розділ регламенту не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

4.1.18. Процес подання запиту на формування кваліфікованого сертифіката

Порядок подання запиту на формування кваліфікованого сертифіката визначено в пункті 4.1 Положення сертифікаційних практик.

4.1.19. Порядок надання сформованого кваліфікованого сертифіката користувачу

Порядок надання сформованого кваліфікованого сертифіката користувачу визначено в пункті 4.3 Положеннях сертифікаційних практик.

Послідовність дій користувача щодо перевірки даних, що містяться в сформованому кваліфікованому сертифікаті визначено в пункті 4.4 Положення сертифікаційних практик.

4.1.20. Порядок публікації сформованого кваліфікованого сертифіката користувача на офіційному веб-сайті КНЕДП – АЦСК МВС

Порядок публікації сформованого кваліфікованого сертифіката користувача на офіційному веб-сайті КНЕДП – АЦСК МВС визначено в пункті 2.2.1 Положення сертифікаційних практик.

4.1.21. Умови використання кваліфікованого сертифіката користувача та його особистого ключа

Умови використання КЕД послуг користувачами визначено в пункті 1.3.3.2 Політики сертифіката.

Кваліфіковані сертифікати користувачів використовуються у сферах та із обмеженнями, зазначеними у пунктах 1.4.1 та 1.4.2 Політики сертифіката.

Наслідками неправильного використання кваліфікованого сертифіката та особистого ключа можуть стати недостовірна автентифікація користувача в інформаційних системах, заволодіння зловмисниками правами доступу користувача до інформації, підробка електронних документів, матеріальні та репутаційні втрати користувача.

Умови використання кваліфікованого сертифіката користувача та його особистого ключа, а також відомості про наслідки їх неправильного використання зазначаються у договорі про надання КЕД послуг.

4.1.22. Процедура подачі запиту на формування кваліфікованого сертифіката для користувачів, які мають чинний кваліфікований сертифікат, сформованого КНЕДП – АЦСК МВС

Порядок подачі запиту на формування кваліфікованого сертифіката для користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС, визначено в пункті 4.7 Положення сертифікаційних практик.

4.1.23. Обставини скасування (блокування, поновлення) кваліфікованого сертифіката

Перелік обставин для зміни статусу кваліфікованого сертифіката визначено в пункті 3.4 Положення сертифікаційних практик.

Порядок блокування та скасування кваліфікованого сертифіката визначено в пункті 4.9 Положення сертифікаційних практик.

Порядок формування списків відкликаних сертифікатів, публікація та розповсюдження списків відкликаних сертифікатів визначено в пункті 2.3 Положення сертифікаційних практик.

4.1.24. Строк закінчення дії кваліфікованого сертифіката користувача

Строк дії кваліфікованих сертифікатів користувачів визначено в пункті 1.4.1.2 Політики сертифіката.

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років.

Дата та час початку та закінчення строку дії кваліфікованого сертифіката користувача, зазначається у кваліфікованому сертифікаті.

Дата та час початку та закінчення строку дії кваліфікованого сертифіката користувача зазначається у такому сертифікаті із точністю до однієї секунди.

Після перевершення дати та часу закінчення строку дії кваліфікованого сертифіката користувача кваліфікований сертифікат вважається нечинним, а КЕП користувача кваліфікований сертифікат якого нечинний, – недійсним.

4.1.25. Організаційні вимоги

Цим Регламентом, Практикою сертифіката, Положенням сертифікаційних практик, а також іншими нормативними документами КНЕДП – АЦСК МВС визначаються вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення користувачів, функціонування ВПР, опису фізичного середовища.

5. ПРОЦЕДУРИ ТА ПРОЦЕСИ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ КЕД ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ

5.1. Надання засобів КЕП

Для надання КЕД послуг КНЕДП – АЦСК МВС використовуються засоби КЕП, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації або документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

Засоби КЕП можуть надаватися КНЕДП – АЦСК МВС у вигляді апаратно-програмних засобів, окремих програмних додатків або програмних модулів (криптобібліотек), що призначені для функціонування у складі інших програмних додатків.

Надання КНЕДП – АЦСК МВС засобів КЕП у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що призначені для функціонування у складі інших програмних додатків, може здійснюватися шляхом передачі цих засобів безпосередньо користувачу на його носії інформації або шляхом надання доступу через офіційний веб-сайт КНЕДП – АЦСК МВС.

КНЕДП – АЦСК МВС забезпечує надання користувачам засобів КЕП для ініціювання генерації ключів, а також створення, перевірки та підтвердження КЕП шляхом розміщення відповідних інсталяційних пакетів на офіційному веб-сайті КНЕДП – АЦСК МВС.

Особливості надання засобів КЕП користувачам – володільцям паспорта громадянина України з імплантованим БЕН визначаються постановою Кабінету Міністрів України від 30.11.2016 № 869 «Про затвердження Порядку внесення засобів кваліфікованого електронного підпису до безконтактного електронного носія, що міститься в паспорті громадянина України, та надання кваліфікованих електронних довірчих послуг з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм» (зі змінами) з урахуванням вимог наказу Міністерства внутрішніх справ України від 27.03.2018 № 238 «Про затвердження Порядку взаємодії кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України та Державної міграційної служби України під час надання послуг кваліфікованого електронного підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм».

5.2. Надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу

Порядок надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу визначено в пункті 6.9 Політики сертифіката.

5.3. Перевірка та підтвердження КЕП

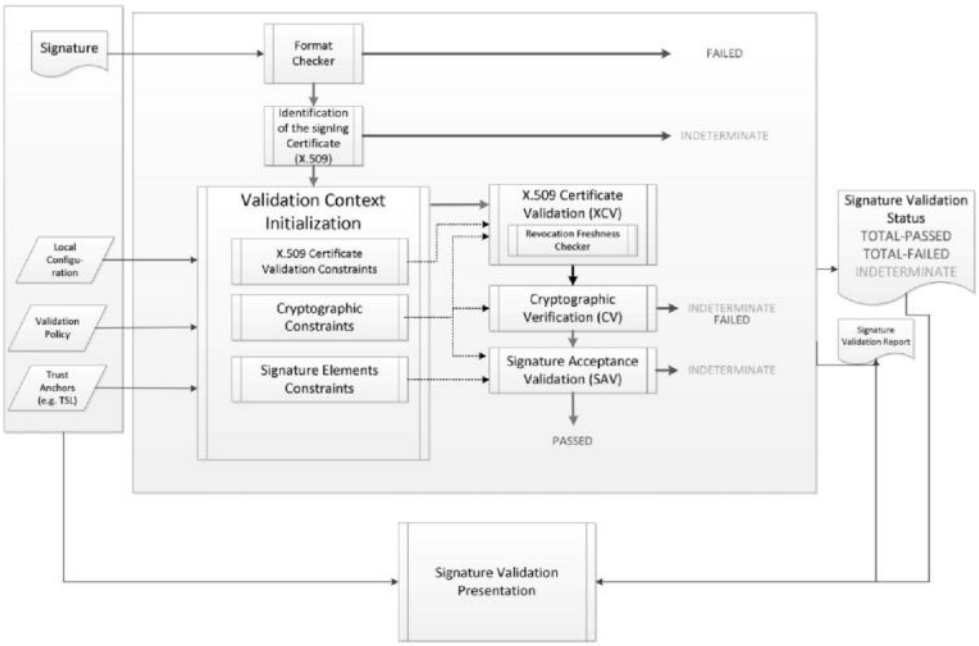
Перевірка та підтвердження КЕП, накладеного на електронний документ, здійснюються КНЕДП – АЦСК МВС в межах надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки. Користувачі можуть здійснити перевірку підпису за допомогою Сервісу перевірки підпису, розміщеного за посиланнями:

на веб-сайті КНЕДП – АЦСК МВС - АЦСК МВС - АЦСК МВС за посиланням: https://ca.mvs.gov.ua/verify;

на веб-сайті центрального засвідчувального органу за посиланням: https://czo.gov.ua/verify;

на веб-сайті інтегрованої системи електронної ідентифікації за посиланням: https://id.gov.ua/verify.

Процес перевірки підпису за допомогою Сервісу перевірки підпису, що відповідає ДСТУ ETSI EN 319 102-1:2022 (ETSI EN 319 102-1 V1.3.1 (2021-11), IDT) "Електронні підписи та інфраструктури (ESI). Процедури створення та перевірки цифрових підписів AdES. Частина 1. Формування та перевірка" (далі - ETSI EN 319 102-1), наведений на схемі.



Перевірку підпису також можна здійснити за допомогою ПК «Користувач АЦСК МВС», інсталяційний пакет якого розміщено на офіційному веб-сайті КНЕДП – АЦСК МВС (https://ca.mvs.gov.ua/user-downloads).

5.3.1. Вимоги до процесу перевірки підпису

Процес перевірки підпису, що здійснюється за допомогою Сервісу перевірки підпису, відповідає ETSI EN 319 102-1.

У пунктах 5.3.2 – 5.3.4 цього Регламенту визначаються окремі компоненти процесу перевірки підпису і обмеження. Якщо в цьому Регламенті не встановлені конкретні вимоги до процесу перевірки підпису, застосовуються вимоги, визначені в ETSI EN 319 102-1. Конкретні вимоги до процесу перевірки підпису, встановлені в цьому Регламенті, мають перевагу над вимогами, визначеними в ETSI EN 319 102-1.

КНЕДП - АЦСК МВС реалізує алгоритм, визначений у ETSI EN 319 102-1, дозволяючи альтернативні реалізації, за умови, що вони створюють ту саму основну індикацію статусу, коли отримує той самий набір вхідної інформації. Сервіс перевірки підпису надає вичерпний звіт про перевірку, дозволяючи прикладному програмному забезпеченню перевіряти деталі кваліфікацій, прийнятих під час перевірки, і детально досліджувати причини відображені в кваліфікації, наданій Сервісом перевірки підпису. Сервіс перевірки підпису надає звіт у зручний для користувача спосіб – придатну для читання HTML-сторінку з можливістю завантаження звіту про перевірку у вигляді PDF-файлу. Результат процесу перевірки підпису містить атрибути та артефакти, передбачені ETSI EN 319 102-1, у тому числі, але не обмежуючись:

- список перевірених підписів;
- статус із зазначенням результатів процесу перевірки підпису;
- помилки, що описують, чому підпис недійсний (TOTAL-FAILED), або попередження, що описують, чому Сервісу перевірки підпису було неможливо визначити статус підпису (INDETERMINATE);
- вказівку на політику, згідно з якою було здійснено перевірку підпису;
- використання будь-якого псевдоніма, якщо застосовується.

Згідно з алгоритмом, визначеним у ETSI EN 319 102-1 , статус перевірки підпису може бути:

1. TOTAL-PASSED
2. TOTAL-FAILED
3. INDETERMINATE

Структура семантики звіту перевірки наведена в Таблиці 2.

Таблиця 2

Головна кваліфікація	Відповідна інформація у звіті про перевірку	Семантика
TOTAL-PASSED	Процес перевірки повинен встановити підтверджений ланцюжок сертифікатів, включаючи сертифікат, який використовується в процесі перевірки. Крім того, процес перевірки може надати результат перевірки для кожного з обмежень перевірки. Процес перевірки повинен забезпечити доступ DA до підписаних атрибутів, присутніх у підписі, ідентифікації підписувача та ланцюжка сертифікатів	Результатом процесу перевірки підпису є TOTAL-PASSED на основі таких міркувань: • криптографічні перевірки підпису пройшли успішно (включаючи перевірки хешів окремих об'єктів даних, які були підписані опосередковано); • будь-які обмеження, застосовні до сертифікації особи підписувача, були підтверджені (тобто сертифікат, як наслідок, було визнано надійним); і • підпис був позитивно перевірений на відповідність обмеженням перевірки і, отже, вважається таким, що відповідає цим обмеженням
TOTAL-FAILED	Процес перевірки повинен встановити додаткову інформацію для пояснення індикації TOTAL-FAILED для кожного з обмежень перевірки, які були враховані та для яких стався негативний результат	Процес перевірки підпису призводить до TOTAL-FAILED, оскільки не вдалося перевірити формат, криптографічні перевірки підпису (включаючи перевірки хешів окремих об'єктів даних, які були підписані опосередковано), або було доведено, що генерація підпису мала місце після відкликання сертифіката

Крім основного статусу, звіт перевірки підпису також містить додаткову інформацію із семантикою, що визначена в Таблиці 3.

Таблиця 3

Головна кваліфікація	Вторинна кваліфікація	Відповідна інформація у звіті про перевірку	Семантика
TOTAL-FAILED	**FORMAT_FAILURE**	Процес перевірки повинен надати будь-яку доступну інформацію, що пояснює, чому розбір підпису не вдався	Підпис не відповідає одному з базових стандартів настільки, що структурний блок криптографічної перевірки не може його обробити
	HASH_FAILURE	Процес повинен встановити: Ідентифікатор(и) (наприклад, URI або OID), що однозначно визначає елемент у підписаному об'єкті даних (наприклад, атрибути підпису або SD), який спричинив помилку	Результатом процесу перевірки підпису є TOTAL- FAILED, оскільки принаймні один хеш підписаного(их) об'єкта(ів) даних, який було включено до процесу підписання, не відповідає відповідному хеш-значенню в підписі
	SIG_CRYPTO_FAILURE	Процес повинен встановити сертифікат, який використовується в процесі перевірки	Процес перевірки підпису призводить до TOTAL-FAILED, оскільки значення підпису в підписі не вдалося перевірити за допомогою відкритого ключа підписувача в сертифікаті
	REVOKED	Процес повинен встановити: • Ланцюжок сертифікатів, який використовується в процесі перевірки. • Час і якщо наявна, причина анулювання сертифіката	Результатом процесу перевірки підпису є TOTAL- FAILED, оскільки: • скасовано сертифікат; і • є докази створення підпису після відкликання сертифікату
	EXPIRED	Процес повинен встановити перевірений ланцюжок сертифікатів	Результатом процесу перевірки підпису є TOTAL - FAILED, оскільки є доказ того, що підпис було створено після закінчення строку

			дії (notAfter) сертифіката
	NOT_YET_VALID		Результатом процесу перевірки підпису є TOTAL - FAILED, оскільки є доказ того, що підпис було створено до дати видачі (notBefore) сертифіката
INDETERMINATE	**SIG_CONSTRAINTS_FAILURE**	Процес повинен встановити набір обмежень, яким не відповідає підпис	Результатом процесу перевірки підпису є INDETERMINATE, оскільки один або кілька атрибутів підпису не відповідають обмеженням перевірки
	CHAIN_CONSTRAINTS_FAILURE	Процес повинен встановити: • Ланцюжок сертифікатів, який використовується в процесі перевірки. • Набір обмежень, які не були виконані ланцюжком	Результатом процесу перевірки підпису є INDETERMINATE, оскільки ланцюжок сертифікатів, який використовується в процесі перевірки, не відповідає обмеженням перевірки, пов'язаним із сертифікатом
	CERTIFICATE CHAIN_GENERAL_FAILURE	• Процес повинен • встановити додаткову інформацію щодо причини	• Результатом процесу перевірки підпису є INDETERMINATE, оскільки набір сертифікатів, • доступних для ланцюжкової перевірки, викликав помилку з невизначеної причини
	CRYPTO_CONSTRAINTS_FAILURE	Процес повинен встановити ідентифікацію сутності (підпис, сертифікат), створеної за допомогою алгоритму або розміру ключа, нижчого за необхідний рівень криптографічної	Результатом процесу перевірки підпису є INDETERMINATE, оскільки принаймні один із алгоритмів, які використовувалися в сутності (наприклад, значення підпису, сертифікат тощо), що бере участь у перевірці підпису, або розмір ключа, який

		безпеки. • Якщо відомо, час, до якого алгоритм або розмір ключа вважалися безпечними	використовується з таким алгоритмом, нижчий від необхідного криптографічного рівня захисту, і: цей матеріал було створено після часу, до якого цей алгоритм/ключ вважався безпечним (якщо такий час відомий); і матеріал не захищений достатньо сильною позначкою часу, застосованою до часу, до якого алгоритм/ключ вважався безпечним (якщо такий час відомий)
	POLICY_PROCESSING_ ERROR	Процес повинен надати додаткову інформацію про проблему	Результатом процесу перевірки підпису є INDETERMINATE, оскільки певний формальний файл політики не вдалося обробити з будь-якої причини (наприклад, недоступний, неможливий аналіз, невідповідність дайджесту тощо)
	SIGNATURE_POLICY_N OT_AVAILABLE	-	Процес перевірки підпису призводить до INDETERMINATE, оскільки електронний документ, що містить деталі політики, недоступний
	TIMESTAMP_ORDER_ FAILURE	Процес повинен встановити список позначок часу, які не відповідають обмеженням упорядкування	Результатом процесу перевірки підпису є INDETERMINATE, оскільки деякі обмеження щодо порядку позначок часу підпису та/або підписаних позначок часу об'єкта(ів) даних не дотримуються

NO_SIGNING_CERTIFICATE_FOUND	-	Процес перевірки підпису призводить до INDETERMINATE, оскільки сертифікат неможливо ідентифікувати
NO_CERTIFICATE_CHAIN_FOUND		Результатом процесу перевірки підпису є INDETERMINATE, оскільки для ідентифікованого сертифіката не знайдено жодного ланцюжка сертифікатів
NO_CERTIFICATE_CHAIN_FOUND_NO_POE		Результатом процесу перевірки підпису є INDETERMINATE, оскільки для ідентифікованого сертифіката підпису не знайдено жодного ланцюжка сертифікатів через те, що прив'язка довіри не є надійною на дату/час перевірки відповідно до політики перевірки, що використовується. Однак алгоритм перевірки підпису не може переконатися, що час підписання лежить до або після часу, коли прив'язка довіри була довіреною політикою перевірки, що використовується
REVOKED_NO_POE	Процес повинен встановити: • Ланцюжок сертифікатів, який використовується в процесі перевірки. • Час і причина відкликання сертифіката	Процес перевірки підпису призводить до INDETERMINATE, оскільки сертифікат було відкликано в дату/час перевірки. Однак алгоритм перевірки підпису не може переконатися, що час підписання лежить до або після часу відкликання

REVOKED_CA_NO_POE	Процес повинен встановити: • Ланцюжок сертифікатів, який включає відкликаний сертифікат центру сертифікації. • Час і причина відкликання сертифіката	Результатом процесу перевірки підпису є INDETERMINATE, оскільки знайдено принаймні один ланцюжок сертифікатів, але проміжний сертифікат центру сертифікації відкликано
OUT_OF_BOUNDS_NOT_REVOKED	-	Процес перевірки підпису призводить до INDETERMINATE, оскільки строк дії сертифіката підпису минув або він ще не дійсний на дату/час перевірки, а алгоритм перевірки підпису не може переконатися, що час підписання лежить у межах інтервалу дії сертифіката підпису. Сертифікат, як відомо, не анульований
OUT_OF_BOUNDS_NO_POE	-	Процес перевірки підпису призводить до INDETERMINATE, оскільки термін дії сертифіката минув або він ще не дійсний на дату/час перевірки, а алгоритм перевірки підпису не може переконатися, що час підписання лежить у межах інтервалу дії сертифіката
REVOCATION_OUT_OF_BOUNDS_NO_POE	Процес підтвердження повинен забезпечувати наступне: • Ланцюжок сертифікатів, який використовується в процесі перевірки. • Дані відкликання,	Процес перевірки підпису призводить до INDETERMINATE, оскільки строк дії сертифіката підпису даних відкликання, що містить інформацію про статус відкликання сертифіката підпису, закінчився або

	які стосуються помилки	ще не дійсний на дату/час перевірки, а алгоритм перевірки підпису не може переконатися, що дані відкликання підтверджені існувати в той час, який знаходиться в межах строку дії сертифіката підпису цих даних відкликання
CRYPTO_CONSTRAINTS_FAILURE_NO_POE	Процес повинен встановити: • Ідентифікацію матеріалу (підпис, сертифікат), створеного за допомогою алгоритму або розміру ключа, нижчого за необхідний рівень криптографічної безпеки. • Час, до якого алгоритм або розмір ключа вважалися безпечними, якщо відомо	Процес перевірки підпису призводить до INDETERMINATE, оскільки принаймні один із алгоритмів, які використовувалися в об'єктах (наприклад, значення підпису, сертифікат тощо), задіяних у перевірці підпису, або розмір ключа, який використовується з таким алгоритмом, нижче необхідного рівня криптографічної безпеки, і немає доказів того, що цей матеріал було створено до часу, до якого цей алгоритм/ключ вважався безпечним
NO_POE	Процес повинен встановити принаймні підписані об'єкти, для яких відсутні POE. Процес перевірки має надати додаткову інформацію про проблему	Процес перевірки підпису призводить до INDETERMINATE, оскільки відсутній доказ існування, щоб підтвердити, що підписаний об'єкт був створений до певної компрометуючої події (наприклад, несправний алгоритм)
TRY_LATER	Процес повинен встановити момент часу, коли очікується, що стане доступною необхідна	Процес перевірки підпису призводить до INDETERMINATE, оскільки не всі обмеження можуть бути виконані за допомогою доступної інформації. Однак це можливо зробити за

		інформація про відкликання	допомогою додаткової інформації про відкликання, яка буде доступна пізніше
	SIGNED_DATA_NOT_ FOUND	Процес повинен встановити ідентифікатор(и) (наприклад, URI) підписаних даних, які спричинили помилку	Процес перевірки підпису призводить до INDETERMINATE, оскільки підписані дані не можуть бути отримані
	CUSTOM	Процес повинен виводити інформацію, яка дозволяє ідентифікувати причину результату спеціальної діагностики	Процес перевірки підпису призводить до INDETERMINATE для спеціальної діагностики, не зазначеної в цьому документі
	GENERIC	Процес повинен встановити додаткову інформацію, чому статус перевірки було оголошено INDETERMINATE	Процес перевірки підпису призводить до INDETERMINATE через будь-яку іншу причину

Сервіс перевірки підпису застосовує відповідну політику перевірки підпису, згідно з якою:

- Сервіс перевірки підпису не приймає кілька джерел політики перевірки підпису;
- Політику перевірки підпису не можна ігнорувати та замінювати ролями перевірки підпису згідно з протоколом, визначеним у ETSI EN 319 102-1;
- Процес перевірки гарантує, що політика перевірки підпису, яка використовується, відповідає стратегії, визначеній у політиці Сервісу перевірки підпису або умовам використання служби перевірки підпису;
- Стратегія, визначена в політиці Сервісу перевірки підпису або в умовах використання Сервісу перевірки підпису, дотримується таких принципів:
- Для того самого введення, включаючи політику перевірки підпису, Сервіс перевірки підпису поверне той самий результат;
- Сервіс перевірки підпису може приймати різні елементи як докази існування для підпису.

5.3.2. Процес перевірки підпису

Залежно від формату електронного підпису/печатки, який використовується, Сервіс перевірки підпису підтримує процеси перевірки для базових форматів підпису/печатки та розширених форматів (з доданою електронною позначкою часу або даними перевірки часу) наступним чином:

- Процес перевірки базового підпису/печатки – Базовий рівень;
- Процес перевірки підписів/печаток із базовим часом - Базовий рівень + T;

- Процес перевірки підписів/печаток із довгостроковими даними перевірки - Базовий рівень + LT

Процес складається з наступних кроків:

Крок 1. Користувач створює та надсилає запит на перевірку підпису.

Обмеження перевірки підпису визначено в ETSI EN 319 102-1, і відповідно до цієї політики КНЕДП - АЦСК МВС обмежує перевірку підпису лише описаними в ній параметрами.

КНЕДП - АЦСК МВС не підтримує політики перевірки підпису, надані користувачем.

Крок 2. Сервіс перевірки підпису реалізує процес перевірки підпису відповідно до ETSI EN 319 102-1.

Перевірка виконується Сервісом перевірки підпису відповідно до обмежень, встановлених самим сервісом.

Крок 3. Сервіс перевірки підпису готує та надсилає відповідь для перевірки підпису. КНЕДП - АЦСК МВС може використовувати протоколи, описані в ДСТУ ETSI TS 119 442:2021 (ETSI TS 119 442 V1.1.1 (2019-02), IDT) "Електронні підписи та інфраструктури (ESI). Профілі протоколів для постачальників довірчих послуг, що надають послуги перевірки цифрових підписів AdES".

Крок 4. Презентація звіту про перевірку підпису.

5.3.3. Обмеження перевірки для документів з електронним підписом

Сервіс перевірки підпису контролюється набором обмежень перевірки. Ці обмеження під час роботи визначаються під час керування Сервісом перевірки підпису. Крім того, можуть існувати обмеження щодо використаних сертифікатів для електронного підпису/печатки. Сервіс підтримує певні обмеження, пов’язані з елементами розміщеного підпису/печатки, дозволеними криптографічними комбінаціями та використовуваними алгоритмами, а також інші обмеження. Існують обмеження щодо розміру файлу з електронним підписом, який приймається для підписання.

5.3.4. Обмеження перевірки для сертифікатів електронного підпису чи печатки

Сервіс перевірки підпису підтримує обмеження перевірки для сертифікатів електронного підпису/печатки відповідно до ДСТУ ETSI TS 119 172-1:2016 (ETSI TS 119 172-1:2015, IDT) "Електронні підписи та інфраструктури (ESI). Політики підпису. Частина 1. Складники та зміст документів щодо політик підпису, придатних для читання людиною" (далі - ETSI TS 119 172-1).

5.3.5. Обмеження криптографічних наборів

Сервіс перевірки підпису підтримує криптографічні обмеження, пов’язані з необхідними алгоритмами та параметрами відповідно до ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) "Електронні підписи та інфраструктури (ESI). Криптографічні пакети", і відповідає вимогам ETSI TS 119 172-1.

5.3.6. Обмеження елементів підпису чи печатки

Сервіс перевірки підпису підтримує обмеження на елементи кваліфікованої перевірки електронних підписів і печаток згідно з вимогами ETSI TS 119 172-1.

5.3.7. Вимоги до протоколу перевірки підпису

Канал зв’язку між користувачем і Сервісом перевірки підпису передає запити на перевірку підпису в одному напрямку та повертає відповідь. Він може бути як синхронним, так і асинхронним. Протокол перевірки підпису відповідає ETSI EN 319 102-1.

5.3.8. Інтерфейси

Інтерфейс Сервісу перевірки підпису визначає інтерфейс перевірки підпису для одного документа, на який накладено електронний підпис чи печатку.

5.3.9. Канал зв'язку

Канал зв'язку між користувачем і Сервісом перевірки підпису захищений за допомогою надійно захищеного каналу за протоколом HTTPS і використанням каналу безпеки TLS 1.2 або вище. КНЕДП - АЦСК МВС гарантує, що може встановити безпечний канал з користувачем і зберегти конфіденційність даних.

Сервіс перевірки підпису не вимагає від користувача автентифікації в ньому за допомогою засобів електронної ідентифікації.

5.3.10. КНЕДП - АЦСК МВС – інші надавачі електронних довірчих послуг

На статус перевірки підпису та звіт про перевірку підпису можуть впливати положення практик, політики надання електронних довірчих послуг та угоди інших надавачів електронних довірчих послуг, діяльність яких знаходиться поза контролем КНЕДП - АЦСК МВС.

Сервіс перевірки підпису (КНЕДП - АЦСК МВС) може з метою отримання необхідної інформації надсилати запити до інших надавачів електронних довірчих послуг, які забезпечують формування електронних позначок часу, перевірку підпису, формування списків відкликаних сертифікатів (CRC) та протоколів визначення статусу сертифіката (OCSP).

Питання функціонування каналу зв’язку між КНЕДП - АЦСК МВС та іншим надавачами електронних довірчих послуг виходить за межі цього Регламенту.

5.3.11. Вимоги до звіту про перевірку підпису

КНЕДП - АЦСК МВС надає два типи звітів про перевірку:

- простий звіт про перевірку підпису, що надає необхідну інформацію щодо особи підписувача та індикацію статусу кожного підтвердженого підпису, включаючи додаткову індикацію;
- деталізований звіт про перевірку підпису, що надає інформацію про кожне обмеження перевірки підпису, яке обробляється, включаючи будь-які обмеження перевірки підпису, які неявно застосовані реалізацією.