МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

Мінцифри

вул. Ділова, 24, м. Київ, 03150, тел. (044) 207-17-30

E-mail: hello@thedigital.gov.ua, сайт: www.thedigital.gov.ua, код згідно з ЄДРПОУ 43220851

від _____20___р. № _____ На №_____ від _____20___р.

Державна регуляторна служба

Щодо погодження
проекту нормативного акта

Міністерство цифрової трансформації України відповідно до статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності» після оприлюднення доопрацьованого проекту акта з метою одержання зауважень і пропозицій надсилає на погодження проект постанови Кабінету Міністрів України «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг» (далі – проект акта).

Разом з тим інформуємо, що проект акта, який надсилався до Державної регуляторної служби України листом від 28.12.2023 № 1/04-1-16123, погоджено Державною регуляторною службою України (рішення про погодження проекту регуляторного акта від 17.01.2024 № 12).

Додатки: 1. Проект акта на 57 арк. в 1 прим.
2. Пояснювальна записка на 23 арк. в 1 прим.
3. Аналіз регуляторного впливу на 19 арк. в 1 прим.

Віце-прем'єр-міністр України з
інновацій, розвитку освіти, науки
та технологій –Міністр **Михайло ФЕДОРОВ**

Інна Плотнікова 0973712086
plotnikova@thedigital.gov.ua

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ _____ 2024 р. № _____

Порядок
інформування контролюючого органу та користувачів послуг електронної ідентифікації, користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації

1. Цей Порядок визначає механізм інформування контролюючого органу та користувачів послуг електронної ідентифікації, користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації під час надання послуг електронної ідентифікації або електронних довірчих послуг.

2. Дія цього Порядку не поширюється на здійснення електронної ідентифікації та надання електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Закон).

3. У цьому Порядку терміни вживаються в такому значенні:

порушення конфіденційності та/або цілісності інформації – будь-яка ідентифікована подія в інформаційно-комунікаційній системі надавача послуг електронної ідентифікації та надавача електронних довірчих послуг, яка вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту чи раніше невідому ситуацію, що може призвести до витоку персональних даних користувачів або несанкціонованої модифікації інформації в інформаційно-комунікаційній системі;

конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем інформаційно-комунікаційної системи та/або процесом;

цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем інформаційно-комунікаційної системи та/або процесом.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила з інформаційної безпеки відносно доступу до неї.

Інформація зберігає цілісність, якщо дотримуються встановлені правила з інформаційної безпеки відносно її модифікації (видалення).

4. Інші терміни вживаються у значенні, наведеному законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про інформацію”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про захист персональних даних” та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.

5. Конфіденційною є інформація, визначена частиною другою статті 21 Закону України “Про інформацію”.

6. Інформування контролюючого органу та користувачів про порушення конфіденційності та/або цілісності інформації здійснюється з метою своєчасного забезпечення захисту персональних даних користувачів послуг електронної ідентифікації, або електронних довірчих послуг та попередження витоку персональних даних користувачів або несанкціонованої модифікації інформації в інформаційно-комунікаційній системі.

7. Надавачі послуг електронної ідентифікації та надавачі електронних довірчих послуг коли їм стало відомо про порушення конфіденційності та/або цілісності інформації, що впливають на надання послуг електронної ідентифікації, або електронних довірчих послуг, або стосуються персональних даних користувачів послуг електронної ідентифікації, або електронних довірчих послуг:

1) не пізніше ніж протягом 24 годин з моменту, коли їм стало відомо про порушення, надсилають повідомлення контролюючому органу та, в разі необхідності, органу з питань захисту персональних даних, в електронній формі з накладенням кваліфікованого електронного підпису керівника організації або уповноваженої особи надавача послуг електронної ідентифікації або надавача електронних довірчих послуг;

2) не пізніше двох годин з моменту, коли їм стало відомо про таке порушення, розміщують на своєму веб-сайті інформацію про порушення конфіденційності та/або цілісності інформації та повідомляють про це технічними засобами електронних комунікацій усім користувачам послуг електронної ідентифікації або електронних довірчих послуг.

8. Повідомлення (інформація), що надсилається до контролюючого органу повинно містити:

короткий виклад обставин, що можуть свідчити про вчинення порушення, дату й час його вчинення або дату й час його виявлення;

відомості про користувачів послуг електронної ідентифікації або електронних довірчих послуг, яким завдано або може бути завдано шкоду (збитки) (за наявності);

відомості про завдання або можливого завдання шкоди (збитків) іншим суб’єктам що здійснюють діяльність у сферах електронної ідентифікації та електронних довірчих послуг;

інші відомості, які мають значення для розгляду повідомлення (інформації).

9. До повідомлення (інформації) що надсилається до контролюючого органу, додаються (за наявності):

засвідчені в установленому порядку копії документів, які можуть свідчити про порушення конфіденційності та/або цілісності інформації;

матеріали фотозйомки, звуко-, відеозапису та інші носії інформації, у тому числі електронні, що можуть свідчити про порушення конфіденційності та/або цілісності інформації;

інші матеріали, які мають значення для розгляду повідомлення (інформації).

_____

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ _____ 2024 р. № _____

Порядок

використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг

1. Цей Порядок визначає механізм використання псевдонімів користувачами послуг електронної ідентифікації або електронних довірчих послуг (далі – користувачі) під час отримання таких послуг.

2. Дія цього Порядку не поширюється на здійснення електронної ідентифікації та надання електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Закон).

3. Термін “псевдонім” у цьому Порядку вживається в такому значенні – це вигадане ім’я, що складається із сукупності слів чи знаків, символів, обране автором (співавторами) чи виконавцем (співвиконавцями) для позначення себе відповідно як автора (співавторів) або як виконавця (співвиконавців), яке може бути використано користувачами під час отримання послуг електронної ідентифікації або електронних довірчих послуг.

Інші терміни вживаються у значенні, наведеному в законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про авторське право і суміжні права” та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.

4. При використанні псевдоніма відповідно до Закону України “Про авторське право і суміжні права” фізичні особи, які є користувачами, під час отримання послуг електронної ідентифікації або електронних довірчих послуг мають право замість прізвища (за наявності), власного імені та по батькові (за наявності) використовувати псевдонім, за умови обов’язкового зазначення про його використання у засобах електронної ідентифікації та сертифікатах відкритих ключів, а також надання документа(ів), що засвідчує(ють) використання особою відповідного псевдоніма.

5. Користувачі, що мають на меті використовувати псевдонім у засобах електронної ідентифікації або сертифікатах відкритих ключів під час електронної взаємодії з інформаційними системами, можуть звернутися для отримання таких послуг до надавачів послуг електронної ідентифікації або кваліфікованих надавачів електронних довірчих послуг.

6. Загальні відомості про надавачів послуг електронної ідентифікації розміщено розміщуються на офіційному веб-сайті Мінцифри.

Для отримання засобів електронної ідентифікації з відповідним рівнем довіри фізичні особи подають до надавача послуг електронної ідентифікації документи та/або електронні дані, необхідні для ідентифікації особи, а також ідентифікаційні дані, які міститимуться у засобі електронної ідентифікації, зокрема псевдонім.

Форма заяви, умови отримання та перелік необхідних документів для отримання послуг електронної ідентифікації розміщується на веб-сайті надавача послуг електронної ідентифікації.

7. Інформація про кваліфікованих надавачів електронних довірчих послуг разом з інформацією про кваліфіковані електронні довірчі послуги, які вони надають, міститься в Довірчому списку.

Довірчий список веде та підтримує в актуальному стані на своєму офіційному веб-сайті центральний засвідчувальний орган (https://czo.gov.ua/trustedlist).

Кваліфіковані електронні довірчі послуги надаються виключно кваліфікованими надавачами електронних довірчих послуг на підставі укладеного між надавачем і заявником договору про надання кваліфікованої електронної довірчої послуги.

Форма заяви, умови отримання та перелік необхідних документів для отримання кваліфікованих електронних довірчих послуг розміщуються на веб-сайті кваліфікованого надавача електронних довірчих послуг.

8. Надавач послуг електронної ідентифікації або надавач електронних довірчих послуг повинен ідентифікувати відповідно до вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг фізичну особу, яка має намір використовувати псевдонім.

9. У процесі підтвердження кваліфікованого електронного підпису дійсність таких підпису підтверджується, за умови зазначення у кваліфікованому сертифікаті електронного підпису про використання в ньому псевдоніма (у разі його використання особою на момент створення кваліфікованого електронного підпису).

При цьому надавачі електронних довірчих послуг повинні враховувати положення національного стандарту ДСТУ ETSI EN 319 412-2:2021 (ETSI EN 319 412-2 V2.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам”.

10. Назву псевдоніма користувачі зазначають у заяві про отримання послуг електронної ідентифікації або електронних довірчих послуг.

Використання користувачами одночасно псевдоніма, а також прізвища (за наявності), власного імені та по батькові (за наявності) не допускається.

У разі, якщо користувачі використовують псевдонім замість прізвища (за наявності), власного імені та по батькові (за наявності) в полях кваліфікованих сертифікатів, такі сертифікати є обов’язковими до публікації на веб-сайті кваліфікованого надавача.

11. Поле атрибута “Псевдонім” складає таку ж кількість знаків як і поле “commonName”.

Термін чинності кваліфікованого сертифіката відкритого ключа з використанням псевдоніму та сфера його застосування не відрізняється від аналогічного кваліфікованого сертифіката відкритого ключа з використанням прізвища (за наявності), власного імені та по батькові (за наявності).

Сфера застосування кваліфікованого сертифіката відкритого ключа з використанням псевдоніму здійснюється в контексті сфери дії Закону України «Про авторське право і суміжні права».

12. Надавач послуг електронної ідентифікації або надавач електронних довірчих послуг не надає послуги електронної ідентифікації або електронні довірчі послуги у разі:

ненадання фізичною особою документа(ів), що засвідчує(ють) використання особою відповідного псевдоніма;

використання в полі атрибута “Псевдонім” більше знаків ніж у полі “commonName”;

виявлення в документах пошкоджень, які не дають змоги однозначно тлумачити зміст, виправлень або дописок.

Особи можуть повторно звернутись в будь-який час до надавача послуг електронної ідентифікації або надавача електронних довірчих послуг для отримання послуг електронної ідентифікації або електронних довірчих послуг.

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ _____ 2024 р. № _____

ПОРЯДОК

проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг

1. Цей Порядок визначає механізм проведення перевірки ідентифікаційних даних юридичної особи чи фізичної особи – підприємця кваліфікованими надавачами електронних довірчих послуг (далі – надавачі) під час формування кваліфікованих сертифікатів відкритих ключів.

2. Дія цього Порядку не поширюється на надання кваліфікованих електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

3. У цьому Порядку терміни вживаються у значенні, наведеному в Законі України “Про електронну ідентифікацію та електронні довірчі послуги”, інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.

4. Надавач під час формування кваліфікованих сертифікатів відкритих ключів проводить перевірку цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця відповідно до цього Порядку та частини п’ятої статті 22 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

5. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає вчинення дій, передбачених частиною першою статті 20 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

6. Формування кваліфікованого сертифіката електронного підпису чи печатки здійснюється надавачем за запитом користувача відповідно до пунктів 62 – 64 Вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених цією постановою.

7. Для ідентифікації юридичної особи чи фізичної особи – підприємця надавач проводить перевірку ідентифікаційних даних, необхідних для формування

кваліфікованого сертифіката електронного підпису чи печатки юридичній особі чи фізичній особі – підприємцю та підтвердження належності юридичної особи чи фізичної особи – підприємця, яка звернулася за отриманням послуги з формування кваліфікованого сертифіката відкритого ключа, ідентифікаційних даних юридичної особи чи фізичної особи – підприємця, отриманих надавачем або його відокремленим пунктом реєстрації.

Зазначені ідентифікаційні дані надаються одним з способів, передбачених частиною другою статті 22 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

Для підтвердження ідентифікаційних даних уповноваженого представника юридичної особи чи фізичної особи – підприємця надавач використовує результати перевірки відомостей (даних) про особу, отримані з Єдиного державного демографічного реєстру, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

У разі відсутності в іноземців та осіб без громадянства документів, що підтверджують ідентифікаційні дані, виданих відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, їх ідентифікація здійснюється за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства.

Якщо від імені юридичної особи діє колегіальний орган, надавачу подається документ, у якому визначено повноваження такого органу та розподіл обов’язків між його членами.

8. Надавач встановлює належність ідентифікаційних даних юридичній особі або уповноваженому представнику юридичної особи чи фізичній особі – підприємцю одним з таких способів:

за документом, що визначає повноваження уповноваженого представника юридичної особи чи фізичної особи – підприємця;

з використанням інформації, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб – підприємців та громадських формувань;

за інформацією з торговельного, банківського, судового реєстрів, які ведуться країною резидентства іноземної юридичної особи, перелік яких публікує на своєму офіційному веб-сайті центральний засвідчувальний орган, або за документом, виданим відповідно до законодавства іноземної держави, легалізованим (консульська легалізація чи проставлення апостиля) відповідно до

законодавства у сфері легалізації офіційних документів, якщо інше не встановлено законом або міжнародними договорами України.

9. Надавач під час формування кваліфікованого сертифіката електронного підпису чи печатки повертає документи у разі:

подання не в повному обсязі документів, передбачених пунктами 7 і 8 цього Порядку;

виявлення в документах пошкоджень, які не дають змоги однозначно тлумачити зміст, виправлень або дописок;

виявлення недостовірних даних у наданих документах

Особи можуть повторно звернутись в будь-який час до надавачів ідентифікації та кваліфікованих надавачів для формування кваліфікованого сертифіката електронного підпису чи печатки.

_____

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ _____ 2024 р. № _____

Порядок

перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів з використанням відомостей інформаційних систем та публічних електронних реєстрів

1. Загальні положення

1. Цей Порядок визначає механізм проведення надавачами послуг електронної ідентифікації та кваліфікованими надавачами електронних довірчих послуг, які можуть здійснювати перевірку інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів – за зверненнями громадян), Єдиного державного демографічного реєстру та документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, Державного реєстру фізичних осіб – платників податків, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації отриманої відповідно до Закону України “Про публічні електронні реєстри” у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації.

2. Дія цього Порядку не поширюється на здійснення електронної ідентифікації та надання електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Закон).

3. У цьому Порядку терміни вживаються у значенні, наведеному в законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про публічні електронні реєстри”, постанові Кабінету Міністрів України від 8 вересня

2016 р. № 606 “Деякі питання електронної взаємодії електронних інформаційних ресурсів” (Офіційний вісник України 2016 р., № 73, ст. 2455) та інших нормативно-правових актів у сферах електронної ідентифікації та електронних довірчих послуг.

4. Об’єктом перевірки є інформація про фізичних осіб, у тому числі іноземців, фізичних осіб – підприємців, юридичних осіб, уповноважених представників юридичних осіб, іноземної юридичної особи або фізичної особи – підприємця (далі – особи), ідентифікаційні дані яких міститимуться у засобах електронної ідентифікації або у кваліфікованих сертифікатах відкритих ключів.

5. Видача засобу електронної ідентифікації здійснюється надавачем послуг електронної ідентифікації (далі – надавач ідентифікації) в день звернення користувача послуг електронної ідентифікації на основі ідентифікаційних даних особи, одержаних від користувача послуг електронної ідентифікації під час його реєстрації відповідно до вимог до засобів електронної ідентифікації в контексті схеми електронної ідентифікації та процедури, що застосовуються для визначення рівня довіри до засобів електронної ідентифікації відповідно до частини четвертої статті 15 Закону.

6. Формування кваліфікованого сертифіката електронного підпису чи печатки заявника здійснюється кваліфікованим надавачем електронних довірчих послуг (далі – кваліфікований надавач) на основі ідентифікаційних даних особи, одержаних від заявника, та згідно з вимогами до надавачів електронних довірчих послуг (у тому числі вимог з безпеки та захисту інформації та вимог до працівників надавача електронних довірчих послуг) та їхніх відокремлених пунктів реєстрації, встановленими відповідно до частини шостої статті 13 Закону.

7. Для підтвердження одержаних ідентифікаційних даних надавачі ідентифікації та кваліфіковані надавачі можуть здійснити перевірку інформації про осіб з використанням відомостей з інформаційних ресурсів (далі – перевірка інформації) єдиної інформаційної системи МВС (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів – за зверненнями громадян), Державного реєстру фізичних осіб – платників податків, Єдиним державним реєстром юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформацією з інших публічних електронних реєстрів відповідно до Закону України “Про публічні електронні реєстри”, в тому числі верифікацією відомостей про смерть, що містяться в Державному реєстрі актів цивільного стану громадян, а також інформації з інших публічних електронних реєстрів відповідно до Закону України “Про публічні електронні реєстри” (далі – інформаційні системи та реєстри), отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації.

8. Надавачі ідентифікації під час видачі засобів електронної ідентифікації, а також кваліфіковані надавачі під час формування та видачі кваліфікованих сертифікатів відкритих ключів мають право проводити перевірку ідентифікаційних даних осіб, яким видаються такі засоби або кваліфіковані сертифікати відкритих ключів (далі – користувачі) з інформаційними ресурсами інформаційних систем та реєстрів.

Зазначені ідентифікаційні дані надаються особами одним з таких способів:

за особистої присутності;

віддалено з використанням засобу електронної ідентифікації, що має високий або середній рівень довіри;

з використанням відеоверифікації з дотриманням вимог законодавства у сферах захисту інформації, електронної ідентифікації та електронних довірчих послуг;

за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, раніше сформованого та виданого відповідно до закону, за умови чинності такого сертифіката;

з використанням інших способів ідентифікації, визначених законом.

9. Надавачі ідентифікації та кваліфіковані надавачі встановлюють належність ідентифікаційних даних особі одним з таких способів:

за документом, що посвідчує особу та підтверджує громадянство України;

з використанням інформації, що міститься в інформаційних системах та реєстрах;

за інформацією з торговельного, банківського, судового реєстрів, які ведуться країною резидентства іноземної юридичної особи, перелік яких публікує на своєму офіційному веб-сайті центральний засвідчувальний орган, або за документом, виданим відповідно до законодавства іноземної держави, легалізованим (консульська легалізація чи проставлення апостиля) відповідно до законодавства у сфері легалізації офіційних документів, якщо інше не встановлено законом або міжнародними договорами України.

10. Для суб’єктів, визначених абзацом другим частини четвертої статті 15^3 Закону “Про електронну ідентифікацію та електронні довірчі послуги” приєднання до інтегрованої системи електронної ідентифікації та використання її ресурсів здійснюється безкоштовно.

11. Перевірку інформації про осіб з даними інформаційних систем та реєстрів адміністратор та технічний адміністратор інтегрованої системи електронної ідентифікації забезпечує шляхом електронної інформаційної взаємодії з

публічними електронними реєстрами відповідно до Закону України “Про публічні електронні реєстри”.

12. Адміністратор та технічний адміністратор інтегрованої системи електронної ідентифікації щодо надавачів електронної ідентифікації та кваліфікованих надавачів виконує функції оператора надання доступу до реєстрової інформації у значенні, наведеному в Законі України “Про публічні електронні реєстри”.

13. Перевірка інформації про осіб з даними інформаційних систем та реєстрів здійснюється після проходження електронної ідентифікації та автентифікації осіб в інтегрованій системі електронної ідентифікації.

14. У разі успішної перевірки інформації про осіб з даними інформаційних систем та реєстрів, надавач послуг електронної ідентифікації або кваліфікований надавач електронних довірчих послуг видає засоби електронної ідентифікації чи формує кваліфіковані сертифікати відкритого ключа.

15. У разі невідповідності ідентифікаційних даних наданих особою під час електронної ідентифікації та електронної автентифікації особи в інтегрованій системі електронної ідентифікації, з відповідними даними з інформаційних систем та реєстрів надавач ідентифікації не видає засоби електронної ідентифікації, а кваліфікований надавач не формує кваліфікованих сертифікатів відкритого ключа.

Особи можуть повторно звернутись в будь-який час до надавачів ідентифікації та кваліфікованих надавачів для отримання послуг електронної ідентифікації чи електронних довірчих послуг.

16. Захист інформації та персональних даних осіб під час перевірки інформації про осіб з даними інформаційних систем та реєстрів здійснюється відповідно до вимог законодавства у сферах захисту інформації та персональних даних.

_____

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту постанови Кабінету Міністрів України «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»

1. Мета

Проект постанови Кабінету Міністрів України «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг» (далі – проект акта) розроблено з метою приведення у відповідність до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (далі – Закон), а також визначення організаційно-методологічних, технічних та технологічних умов, яких повинні дотримуватися надавачі послуг електронної ідентифікації та надавачі електронних довірчих послуг.

2. Обґрунтування необхідності прийняття акта

Згідно з пунктом 38 частини першої статті 1 Закону некваліфікований надавач електронних довірчих послуг – надавач електронних довірчих послуг, відомості про якого не внесені до Довірчого списку та який відповідає вимогам, визначеним Кабінетом Міністрів України до некваліфікованих надавачів електронних довірчих послуг.

Статтею 4^1 Закону передбачено, що фізичні особи, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг, під час отримання таких послуг мають право замість прізвища, власного імені та по батькові (за наявності) використовувати псевдонім у випадках, визначених законом, за умови обов’язкового зазначення про його використання у засобах електронної ідентифікації та сертифікатах відкритих ключів у порядку, визначеному Кабінетом Міністрів України.

Згідно зі статтею 11^2 Закону передбачено, зокрема, що вимоги до надавачів послуг електронної ідентифікації, їхніх відокремлених пунктів реєстрації, у тому числі вимоги щодо безпеки та захисту інформації, а також порядок перевірки їх дотримання, порядок інформування контролюючого органу та користувачів послуг електронної ідентифікації встановлюються Кабінетом Міністрів України.

Також надавачі електронних довірчих послуг серед іншого мають право проводити під час формування та видачі кваліфікованих сертифікатів відкритих ключів перевірку інформації про осіб, яким видаються такі сертифікати, з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів за зверненнями громадян), Державного реєстру фізичних

осіб – платників податків, Державного реєстру актів цивільного стану громадян, єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей щодо викрадених (втрачених) документів – за зверненнями громадян), Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України «Про публічні електронні реєстри», отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації в порядку, визначеному Кабінетом Міністрів України. Кваліфіковані надавачі електронних довірчих послуг, крім прав, визначених частиною першою цієї статті, також мають право самостійно обирати в рамках кожної послуги, які саме стандарти вони будуть застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, визначеного Кабінетом Міністрів України. Надавачі електронних довірчих послуг зобов'язані забезпечувати: інформування контролюючого органу та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли їм стало відомо про таке порушення, у порядку, встановленому Кабінетом Міністрів України; інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли їм стало відомо про таке порушення, у порядку, встановленому Кабінетом Міністрів України. Вимоги до надавачів електронних довірчих послуг (у тому числі вимоги з безпеки та захисту інформації та вимоги до працівників надавача електронних довірчих послуг) та їхніх відокремлених пунктів реєстрації, порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України. Перелік змін у наданні кваліфікованих електронних довірчих послуг, про які кваліфіковані надавачі зобов'язані поінформувати контролюючий орган та центральний засвідчувальний орган або засвідчувальний центр, встановлюються Кабінетом Міністрів України (стаття 13 Закону).

Статтею 18 Закону, зокрема, передбачено, що вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Також відповідно до частин другої, третьої статті 20 Закону, зокрема, передбачено, що формування та видача кваліфікованих сертифікатів відкритого ключа іншого призначення, ніж для автентифікації веб-сайту, створення електронного підпису та електронної печатки, здійснюються відповідно до вимог цього Закону з урахуванням особливостей, встановлених Кабінетом Міністрів України. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого

сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Згідно з частиною другою статті 21 Закону вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Також під час перевірки цивільної правоздатності та дієздатності юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки або автентифікації веб-сайту) чи фізичної особи – підприємця (з метою формування кваліфікованого сертифіката електронної печатки) кваліфікований надавач електронних довірчих послуг зобов'язаний використовувати інформацію про юридичну особу чи фізичну особу – підприємця, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб – підприємців та громадських формувань або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, а також пересвідчитися, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа або автентифікації веб-сайту. Порядок проведення перевірки, передбаченої цією частиною, визначається Кабінетом Міністрів України (стаття 22 Закону).

Статтею 23 Закону, зокрема, передбачено, що порядок перевірки дотримання обов'язкових вимог до кваліфікованих сертифікатів відкритих ключів затверджується Кабінетом Міністрів України.

Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України (стаття 26 Закону).

Відповідно до частини другої статті 27 Закону вимоги до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Вимоги до надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України (стаття 28 Закону).

З огляду на зазначене прийняття проекту акта забезпечить визначення вимог до надавачів послуг електронної ідентифікації, електронних довірчих послуг та послуг, що ними надаються, актуального переліку стандартів, які використовуватимуться цими надавачами під час надання електронних послуг, вимог з безпеки та захисту інформації та порядку їх перевірки, дозволить використання псевдонімів замість прізвища, власного ім'я та по батькові (за наявності) у визначених законодавством випадках, затвердження порядку інформування про порушення конфіденційності та/або цілісності інформації, порядку перевірки інформації про осіб, яким видаються засоби електронної

ідентифікації або кваліфіковані сертифікати відкритих ключів та порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг.

Враховуючи вищезазначене, прийняття проекту акта сприятиме максимальному наближенню положень національного законодавства до європейських вимог у сферах електронної ідентифікації та електронних довірчих послуг.

3. Основні положення проекту акта

Проектом акта пропонується затвердити:

Вимоги до надавачів послуг електронної ідентифікації та електронних довірчих послуг;

Порядок інформування контролюючого органу та користувачів послуг електронної ідентифікації, користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації;

Порядок перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів з використанням відомостей інформаційних систем та публічних електронних реєстрів;

Порядок використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг;

Порядок проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг.

Також проектом акта пропонується визнати такою, що втратила чинність, постанову Кабінету Міністрів України від 7 листопада 2018 р. № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг».

4. Правові аспекти

Закон України «Про електронну ідентифікацію та електронні довірчі послуги», Положення про Міністерство цифрової трансформації України, затверджене постановою Кабінету Міністрів України від 18 вересня 2019 року № 856.

5. Фінансово-економічне обґрунтування

Реалізація проекту акта не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів. Фінансування видатків, необхідних для реалізації проекту акта буде здійснюватися в межах видатків, передбачених Державним бюджетом України на відповідний бюджетний період за бюджетною програмою «Електронне урядування» (код 2901030). Ризики, у тому числі фіскальні, відсутні. Фінансово-економічні розрахунки додаються.

6. Позиція заінтересованих сторін

Проект акта потребує проведення публічних консультацій відповідно до Порядку проведення консультацій з громадськістю з питань формування та реалізації державної політики, затвердженого постановою Кабінету Міністрів України від 03 листопада 2010 року № 996 «Про забезпечення участі громадськості у формуванні та реалізації державної політики».

Проект акта не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної, сфери наукової та науково-технічної діяльності.

7. Оцінка відповідності

Проект акта не стосується зобов'язань України у сфері європейської інтеграції, відповідає положенням Конвенції про захист прав людини і основоположних свобод.

Проект акта не містить положень, які порушують принцип забезпечення рівних прав та можливостей жінок і чоловіків. Реалізація проекту акта не матиме впливу на представників обох статей.

У проекті акта відсутні положення, що містять ознаки дискримінації чи створюють підстави для дискримінації.

У проекті акта відсутні правила і процедури, які можуть містити ризики вчинення корупційних правопорушень та правопорушень, пов'язаних із корупцією. Проект акта не потребує проведення громадської антикорупційної експертизи.

8. Прогноз результатів

Реалізація проекту акта не матиме впливу на ринкове середовище, забезпечення захисту прав та інтересів суб'єктів господарювання, громадян і держави; розвиток регіонів, підвищення чи зниження спроможності територіальних громад; ринок праці, рівень зайнятості населення; громадське здоров'я, покращення чи погіршення стану здоров'я населення або його окремих груп; екологію та навколишнє природне середовище, обсяг природних ресурсів, рівень забруднення атмосферного повітря, води, земель, зокрема забруднення утвореними відходами, інші суспільні відносини.

Вплив на інтереси заінтересованих сторін:

Заінтересована сторона	**Вплив реалізації акта на заінтересовану сторону**	**Пояснення очікуваного впливу**
Надавачі послуг електронної ідентифікації та	Позитивний	Прийняття проекту акта сприятиме встановленню, зокрема вимог до надавачів послуг електронної ідентифікації, електронних довірчих послуг (у тому числі

електронних довірчих послуг		вимог з безпеки та захисту інформації та вимог до працівників надавача електронних довірчих послуг) та їхніх відокремлених пунктів реєстрації, а також порядку перевірки їх дотримання

Віце-прем’єр-міністр України з інновацій, розвитку освіти, науки та технологій – Міністр цифрової трансформації України **Михайло ФЕДОРОВ**

____ _____ 2024 р.

Додаток
до пояснювальної записки

ФІНАНСОВО-ЕКОНОМІЧНІ РОЗРАХУНКИ ДО ПРОЕКТУ АКТА

«Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»

(назва проекту акта)

1. Період реалізації акта (рік)

Початок реалізації акта 2024

Кінцевий термін реалізації акта постійно

2. Стратегічні цілі та показники результату, яких планує досягти головний розробник проекту акта

Назва показника результату	Одиниця виміру	Поточний рік (2024)	Рік (2025)	Рік (2026)	Рік (2027)
Стратегічна ціль 1 Розвиток адміністративних послуг та їх цифровізація					
Кількість кваліфікованих сертифікатів відкритих ключів, які обслуговуються центральним засвідчувальним органом	од	112	112	112	112
Кількість кваліфікованих сертифікатів, які будуть сформовані кваліфікованим надавачам	од	34	34	34	34

3. Бюджетна програма, в межах якої планується реалізація акта

КПКВК або ТПКВКМБ	Назва
2901030	Електронне урядування

4. Загальна вартість публічної послуги з формування та реалізації акта

тис. грн

Джерела здійснення витрат	Поточний рік (2024)	Рік (2025)	Рік (2026)	Рік (2027)
За рахунок коштів бюджету, у тому числі:	19 098,4	7 428,2	7 428,2	7 428,2
державного бюджету	19 098,4	7 428,2	7 428,2	7 428,2
місцевого бюджету	-	-	-	-
За рахунок інших джерел, не заборонених законодавством	-	-	-	-
УСЬОГО	19 098,4	7 428,2	7 428,2	7 428,2

5. Перелік питань щодо потреби проведення зведених фінансово-економічних розрахунків

Питання	Поточний рік (2024)		Рік (2025)		Рік (2026)		Рік (2027)	
	так	ні	так	ні	так	ні	так	ні
1	2	3	4	5	6	7	8	9
1. Державна підтримка та допомога								

Чи надаватиметься нова та/або відбудуться зміни у наданні державної підтримки та/або допомоги фізичним/юридичним особам?	-	-	-	-	-	-	-	-
Чи будуть надаватися нові та/або вноситися зміни у наданні допомоги, виплати, пенсії, тощо певним заінтересованим сторонам?	-	-	-	-	-	-	-	-
2. Оплата праці								
Чи будуть змінюватись умови оплати праці працівників установ та організацій, що утримуються з відповідних бюджетів?	-	-	-	-	-	-	-	-
Чи буде збільшено/зменшено чисельність працівників бюджетної установи?	-	-	-	-	-	-	-	-
3. Майно, роботи, послуги								
Чи будуть придбавати / передавати / списувати рухоме/нерухоме майно?	-	-	-	-	-	-	-	-
Чи планується отримання майна у натуральній формі, яке потребуватиме у подальшому обслуговування?	+	-	-	-	-	-	-	-
Чи треба буде здійснювати публічні закупівлі товарів, робіт і послуг?	+	-	+	-	+	-	+	-
Чи треба буде розробляти вебсайт / онлайн-системи / курси / реєстри тощо?	+	-	+	-	+	-	+	-
Чи треба буде проводити комунікаційні заходи та/або заходи з інформування щодо нових	-	-	-	-	-	-	-	-

процедур і правил для працівників?								
Чи будуть зменшуватися або збільшуватися видатки на зв'язок, оплату комунальних послуг, оренду, поточний ремонт тощо?	+	-	+	-	+	-	+	-
Чи треба буде проводити базове навчання для працівників?	-	-	+	-	+	-	+	-
4. Доходи								
Чи буде введено, змінено чи скасовано наявні податки, збори та інші доходи?	-	-	-	-	-	-	-	-
Чи буде змінено структуру наявних податків, зборів та інших доходів?	-	-	-	-	-	-	-	-
Чи будуть змінюватись джерела здійснення видатків та надання кредитів з бюджету?	-	-	-	-	-	-	-	-
Чи будуть будь-кому надаватись пільги в оподаткуванні?	-	-	-	-	-	-	-	-
5. Боргові зобов'язання та гарантії								
Чи відбудеться вплив на обсяг державного/місцевого боргу та гарантованого державою / Автономною Республікою Крим, обласною радою чи територіальною громадою міста боргу?	-	-	-	-	-	-	-	-
6. Повноваження								
Чи будуть передаватись повноваження на	-	-	-	-	-	-	-	-

здійснення видатків з державного до місцевих та/або з місцевих до державного бюджетів?								

6. Базові показники

6.1. Заінтересовані сторони, на забезпечення інтересів яких спрямовано реалізацію акта

од.

Заінтересовані сторони	**Кількість**			
	Поточний рік (2024)	**Рік (2025)**	**Рік (2026)**	**Рік (2027)**
Кваліфіковані надавачі електронних довірчих послуг включно з надавачами ЗЦ	29	31	32	33

Перелік показників	**Поточний рік (2024)**	**Рік (2025)**	**Рік (2026)**	**Рік (2027)**
Прямі витрати:	**18 150,3**	**7 149,3**	**7 149,3**	**7 149,3**
Оплата праці з нарахуваннями	5 164,5	6 104,9	6 104,9	6 104,9
Предмети, матеріали, обладнання та інвентар	79,3	91,6	91,6	91,6
Послуги сторонніх організацій	5 137,3	952,8	952,8	952,8
Капітальні видатки одержувачів	7 769,2	-	-	-
Непрямі витрати:	**948,1**	**278,9**	**278,9**	**278,9**
Оренда офісу, комунальні послуги та енергоносії	948,1	278,9	278,9	278,9

6.2. Прямі та непрямі витрати

7. Зведені фінансово-економічні розрахунки

Вид бюджету державний

7.1. Видатки на здійснення заходів, передбачених проектом акта, та доходи бюджету - доходів до бюджету не передбачено

тис.грн

Показники	**Поточний рік (2024)**			**Рік (2025)**			**Рік (2026)**			**Рік (2027)**		
	загальний фонд	**спеціальний фонд**	**разом**	**загальний фонд**	**спеціальний фонд**	**Разом**	**загальний фонд**	**спеціальний фонд**	**разом**	**загальний фонд**	**спеціальний фонд**	**разом**
1	2	3	4	5	6	7	8	9	10	11	12	13
1. Видатки бюджету згідно з проектом акта, усього (підпункт 1.1 + підпункт 1.2)	-	-	-	-	-	-	-	-	-	-	-	-
у тому числі:	-	-	-	-	-	-	-	-	-	-	-	-
1.1. Збільшення	-	-	-	-	-	-	-	-	-	-	-	-

видатків (+), усього												
з них: за бюджетною програмою												
1.2. Зменшення видатків (-), усього	-	-	-	-	-	-	-	-	-	-	-	-
2. Доходи бюджету згідно з проектом акта, усього (підпункт 2.1 + підпункт 2.2)	-	-	-	-	-	-	-	-	-	-	-	-
у тому числі:	-	-	-	-	-	-	-	-	-	-	-	-
2.1. Збільшення доходів (+), усього	-	-	-	-	-	-	-	-	-	-	-	-
з них: (розписати за кодами бюджетної класифікації)	-	-	-	-	-	-	-	-	-	-	-	-

2.2. Зменшення доходів (-), усього	-	-	-	-	-	-	-	-	-	-	-	-
з них: (розписати за кодами бюджетної класифікації)	-	-	-	-	-	-	-	-	-	-	-	-
3. Видатки бюджету згідно з проектом акта, які наявні у бюджеті, усього	**19 098,4**		**19 098,4**	**7 428,2**		**7 428,2**	**7 428,2**		**7 428,2**	**7 428,2**		**7 428,2**
з них: за бюджетною програмою												
КПКВК 2901030	19 098,4		19 098,4	7 428,2		7 428,2	7 428,2	-	7 428,2	7 428,2	-	7 428,2
КЕКВ 2281 "Дослідження і розробки, окремі заходи розвитку по реалізації	11 329,2	-	11 329,2	7 428,2		7 428,2	7 428,2	-	7 428,2	7 428,2	-	7 428,2

державних (регіональних) програм"												
КЕКВ 3210 "Капітальні трансферти підприємствам (установам, організаціям)"	7 769,2		7 769,2									
4. Доходи бюджету згідно з проектом акта, які наявні у бюджеті, усього	-	-	-	-	-	-	-	-	-	-	-	-
з них: (розписати за кодами бюджетної класифікації)	-	-	-	-	-	-	-	-	-	-	-	-
5. Загальна сума додаткових бюджетних коштів, необхідна для	-	-	-	-	-	-	-	-	-	-	-	-

реалізації проекту акта (пункт 1 - пункт 2 - пункт 3 - пункт 4)												
6. Джерела покриття загальної суми додаткових бюджетних коштів (пункт 5), необхідних для реалізації проектом акта, усього (підпункт 6.1 + підпункт 6.2)	-	-	-	-	-	-	-	-	-	-	-	-
у тому числі за рахунок:	-	-	-	-	-	-	-	-	-	-	-	-
6.1. Зменшення видатків бюджету (-), усього	-	-	-	-	-	-	-	-	-	-	-	-

з них: за бюджетними програмами (КПКВК або ТПКВКМБ), КЕКВ (розписати за кодами бюджетної класифікації)	-	-	-	-	-	-	-	-	-	-	-	-
6.2. Збільшення доходів бюджету (+), усього	-	-	-	-	-	-	-	-	-	-	-	-
з них: (розписати за кодами бюджетної класифікації)	-	-	-	-	-	-	-	-	-	-	-	-
7.2. Повернення кредитів до бюджету та розподіл надання кредитів з бюджету												

тис. грн

Показники	**Поточний рік (2024)**			**Рік (2025)**			**Рік (2026)**			**Рік (2027)**		
	загальний фонд	**спеціальний фонд**	**разом**	**загальний фонд**	**спеціальний фонд**	**разом**	**загальний фонд**	**спеціальний фонд**	**разом**	**загальний фонд**	**спеціальний фонд**	**разом**

1	2	3	4	5	6	7	8	9	10	11	12	13
1. Кредитування, усього (підпункт 1.1 + підпункт 1.2)	-	-	-	-	-	-	-	-	-	-	-	-
у тому числі:	-	-	-	-	-	-	-	-	-	-	-	-
1.1. Надання кредитів (+),	-	-	-	-	-	-	-	-	-	-	-	-
усього	-	-	-	-	-	-	-	-	-	-	-	-
з них: за бюджетними програмами КПКВК або ТПКВКМБ та ККК	-	-	-	-	-	-	-	-	-	-	-	-
(розписати за кодами бюджетної класифікації)	-	-	-	-	-	-	-	-	-	-	-	-
1.2. Повернення кредитів (-), усього	-	-	-	-	-	-	-	-	-	-	-	-
з них: за бюджетними програмами КПКВК або ТПКВКМБ та ККК	-	-	-	-	-	-	-	-	-	-	-	-

7.3. Гарантії

№ з/п	Найменування суб'єкта господарювання	Мета / інвестиційний проєкт	Рік набрання чинності гарантійною угодою	Гарантійні зобов'язання			
				сума гарантованого кредиту (позики) в іноземній валюті		сума гарантованого кредиту (позики) в національній валюті	додаткові зобов'язання, виконання яких гарантуються
				код валюти	Сума		
	-	-	-	-	-	-	-
	-	-	-	-	-	-	-
	-	-	-	-	-	-	-
Разом		x	x	x	X	x	x

7.4. Запозичення

№ з/п	Ініціатор залучення кредиту (позики) / кінцевий позичальник	Мета / інвестиційний проєкт, на реалізацію якого запозичуються кошти	Вибірка кредиту (позики)		Сума кредиту (позики)			Умови кредиту (позики)
					сума у валюті кредиту (позики)		сума в національній валюті	
			рік	сума у	код валюти	сума		

				валюті кредиту (позики)					
1	-	-	поточний (n)		-	-	-	термін кредиту (позики)	
			(n+1)					відсоткова ставка	
			(n+2)					комісійні платежі	
			(n+3)					інші обов'язкові платежі	
			-					штрафні санкції	
Разом		X	x		X	x		x	x

8. Обґрунтування та припущення щодо оцінки прямого та опосередкованого впливу проєкту акта на надходження та витрати державного та/або місцевого бюджетів, перелік ризиків, у тому числі фіскальних

Поточний рік (2024)

Реалізація проекту акта не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів. Фінансування видатків, необхідних для реалізації проекту акта, буде здійснюватися в межах видатків, передбачених Державним бюджетом України на відповідний бюджетний період за бюджетною програмою «Електронне урядування (код 2901030) для функціонування та розвитку інформаційно-комунікаційної системи центрального засвідчувального органу (далі – ЦЗО), обсяг витрат на функціонування якої складає 19 098,4 тис. гривень.

Очікуваними результатами реалізації проєкту акта є встановлення, зокрема вимог до надавачів послуг електронної ідентифікації, електронних довірчих послуг (у тому числі вимог з безпеки та захисту інформації та вимог до працівників надавача електронних довірчих послуг) та їхніх відокремлених пунктів реєстрації, а також порядку перевірки їх дотримання, забезпечення функціонування Довірчого списку.

Ризики, у тому числі фіскальні, відсутні.

2025 рік

Реалізація проекту акта не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів. Фінансування видатків, необхідних для реалізації проекту акта, буде здійснюватися в межах видатків, передбачених Державним бюджетом України на відповідний бюджетний період за бюджетною програмою «Електронне урядування (код 2901030) для функціонування та розвитку ЦЗО, прогнозований обсяг витрат на функціонування якої складе 7 428,2 тис. гривень (забезпечено у межах граничних показників видатків, доведених Мінфіном листом від 07.08.2023 № 04110-08-2/21527).

Визначений обсяг видатків забезпечує всі необхідні для забезпечення належного рівня технічного забезпечення та функціонування (технічного адміністрування) ЦЗО, що також враховує оренду додаткових місць резервного копіювання та зберігання даних на випадок руйнівних кібератак, а також проведення необхідних заходів з протидії, шляхом побудови комплексної системи захисту інформації. Очікуваними результатами реалізації проєкту акта є забезпечення функціонування Довірчого списку. Уточнений обсяг видатків буде визначено під час опрацювання бюджетних пропозицій до Бюджетної декларації відповідно до статті 33 Бюджетного кодексу України.

Ризики, у тому числі фіскальні, відсутні.

2026 – 2027 роки

Реалізація проекту акта не потребує додаткових коштів та не матиме прямого чи опосередкованого впливу на надходження та витрати державного та/або місцевого бюджетів. Фінансування видатків, необхідних для реалізації проекту акта, буде здійснюватися в межах видатків, передбачених Державним бюджетом України на відповідний бюджетний період за бюджетною програмою «Електронне урядування (код

2901030) для функціонування та розвитку ЦЗО, прогнозований обсяг витрат на функціонування якої складе по 7 428,2 тис. гривень на відповідний рік. Очікуваними результатами реалізації проєкту акта є забезпечення функціонування Довірчого списку. Уточнений обсяг видатків буде визначено під час опрацювання бюджетних пропозицій до Бюджетної декларації відповідно до статті 33 Бюджетного кодексу України.

Ризики, у тому числі фіскальні, відсутні.

В.о. директора директорату розвитку цифровізації **Ірина ШОСТАК**

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту постанови Кабінету Міністрів України «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»
(далі – проект акта)

І. Визначення проблеми

Відповідно до абзацу другого пункту 1 Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, Мінцифри є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики, зокрема у сферах електронних довірчих послуг та електронної ідентифікації.

01 грудня 2022 р прийнято Закон України № 2801-IX «Про внесення змін до деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації», пунктом 1 розділу II «Прикінцеві та перехідні положення» якого передбачено, що цей Закон набирає чинності через один рік з дня його опублікування, крім підпунктів 25 і 44 пункту 64 розділу I цього Закону, які набирають чинності з дня, наступного за днем опублікування цього Закону.

Відповідно до підпункту 1 пункту 64 розділу I вищезазначеного Закону, зокрема, назву Закону України «Про електронні довірчі послуги» викладено в такій редакції: «Про електронну ідентифікацію та електронні довірчі послуги».

Згідно з пунктом 38 частини першої статті 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (далі – Закон) передбачено, що некваліфікований надавач електронних довірчих послуг – надавач електронних довірчих послуг, відомості про якого не внесені до Довірчого списку та який відповідає вимогам, визначеним Кабінетом Міністрів України до некваліфікованих надавачів електронних довірчих послуг.

Статтею 4^1 Закону передбачено, що фізичні особи, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг, під час отримання таких послуг мають право замість прізвища, власного імені та по батькові (за наявності) використовувати псевдонім у випадках, визначених законом, за умови обов’язкового зазначення про його використання у засобах електронної ідентифікації та сертифікатах відкритих ключів у порядку, визначеному Кабінетом Міністрів України.

Згідно зі статтею 11^2 Закону передбачено, що вимоги до надавачів послуг електронної ідентифікації, їхніх відокремлених пунктів реєстрації, у тому числі вимоги щодо безпеки та захисту інформації, а також порядок перевірки їх дотримання, порядок інформування контролюючого органу та користувачів

послуг електронної ідентифікації встановлюються Кабінетом Міністрів України.

Також статтею 13 Закону, зокрема, передбачено, що надавачі електронних довірчих послуг, серед іншого, мають право проводити під час формування та видачі кваліфікованих сертифікатів відкритих ключів перевірку інформації про осіб, яким видаються такі сертифікати, з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів за зверненнями громадян), Державного реєстру фізичних осіб – платників податків, Державного реєстру актів цивільного стану громадян, єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей щодо викрадених (втрачених) документів – за зверненнями громадян), Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України «Про публічні електронні реєстри», отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації в порядку, визначеному Кабінетом Міністрів України. Кваліфіковані надавачі електронних довірчих послуг, крім прав, визначених частиною першою цієї статті, також мають право самостійно обирати в рамках кожної послуги, які саме стандарти вони будуть застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, визначеного Кабінетом Міністрів України. Надавачі електронних довірчих послуг зобов’язані забезпечувати: інформування контролюючого органу та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли їм стало відомо про таке порушення, у порядку, встановленому Кабінетом Міністрів України; інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли їм стало відомо про таке порушення, у порядку, встановленому Кабінетом Міністрів України. Вимоги до надавачів електронних довірчих послуг (у тому числі вимоги з безпеки та захисту інформації та вимоги до працівників надавача електронних довірчих послуг) та їхніх відокремлених пунктів реєстрації, порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України. Перелік змін у наданні кваліфікованих електронних довірчих послуг, про які кваліфіковані надавачі зобов’язані поінформувати контролюючий орган та центральний засвідчувальний орган або засвідчувальний центр, встановлюються Кабінетом Міністрів України.

Статтею 18 Закону, зокрема, передбачено, що вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та

підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Також відповідно до частин другої, третьої статті 20 Закону, зокрема, передбачено, що формування та видача кваліфікованих сертифікатів відкритого ключа іншого призначення, ніж для автентифікації веб-сайту, створення електронного підпису та електронної печатки, здійснюються відповідно до вимог цього Закону з урахуванням особливостей, встановлених Кабінетом Міністрів України. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Згідно з частиною другою статті 21 Закону вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Статтею 22 Закону, серед іншого передбачено, що під час перевірки цивільної правоздатності та дієздатності юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки або автентифікації веб-сайту) чи фізичної особи – підприємця (з метою формування кваліфікованого сертифіката електронної печатки) кваліфікований надавач електронних довірчих послуг зобов’язаний використовувати інформацію про юридичну особу чи фізичну особу – підприємця, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб – підприємців та громадських формувань або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, а також пересвідчитися, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа або автентифікації веб-сайту. Порядок проведення перевірки, передбаченої цією частиною, визначається Кабінетом Міністрів України.

Статтею 23 Закону, зокрема, передбачено, що Порядок перевірки дотримання обов’язкових вимог до кваліфікованих сертифікатів відкритих ключів затверджується Кабінетом Міністрів України.

Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України (стаття 26 Закону).

Відповідно до частини другої статті 27 Закону вимоги до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

Статтею 28 Закону, зокрема, передбачено, що вимоги до надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих

електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України.

З огляду на зазначене проект акта забезпечить визначення вимог до надавачів послуг електронної ідентифікації, електронних довірчих послуг та послуг, що ними надаються, актуального переліку стандартів, які використовуватимуться цими надавачами під час надання електронних послуг, вимог з безпеки та захисту інформації та порядку їх перевірки, дозволить використання псевдонімів замість прізвища, власного ім'я та по батькові (за наявності) у визначених законодавством випадках, затвердження порядку інформування про порушення конфіденційності та/або цілісності інформації, порядку перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів та порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг.

З огляду на зазначене під регулювання проекту акта підпадають суб'єкти, які надаватимуть послуги електронної ідентифікації та електронні довірчі послуги.

Станом на сьогодні в Україні до Довірчого списку внесено 20 кваліфікованих надавачів електронних довірчих послуг, які за бажанням можуть бути потенційними надавачами послуг електронної ідентифікації (з них 12 є суб'єктами господарювання).

Питання, що пропонується врегулювати, є нагальним, оскільки сприятиме максимальному наближенню положень національного законодавства до європейських вимог у сферах електронної ідентифікації та електронних довірчих послуг.

Групи (підгрупи)	Так	Ні
Громадяни		Ні
Держава	Так	
Суб'єкти господарювання	Так	

II. Цілі державного регулювання

Проект акта розроблено з метою визначення організаційно-методологічних, технічних та технологічних умов, яких повинні дотримуватися надавачі послуг електронної ідентифікації (далі – надавачі ідентифікації), а також надавачі електронних довірчих послуг (кваліфіковані та некваліфіковані) (далі – надавачі), у тому числі з безпеки та захисту інформації, та їх відокремлені пункти реєстрації під час надання послуг електронної ідентифікації та електронних довірчих послуг, а також працівники надавача.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1 Прийняття проекту акта	Прийняття проекту акта передбачає продовження реформи законодавства у сфері електронного цифрового підпису, розпочатої у зв'язку з прийняттям Закону України «Про електронні довірчі послуги», шляхом розроблення законодавства у сферах електронної ідентифікації та електронних довірчих послуг Так, проектом акта пропонується затвердити: Вимоги до надавачів послуг електронної ідентифікації та електронних довірчих послуг; Порядок інформування контролюючого органу та користувачів послуг електронної ідентифікації, користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації; Порядок перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів з використанням відомостей інформаційних систем та публічних електронних реєстрів; Порядок використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг; Порядок проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг.
Альтернатива 2 Відсутність регулювання	Відсутність регулювання передбачає залишення існуючого стану справ: відсутність організаційно-методологічних, технічних та технологічних умов, яких повинні дотримуватися надавачі ідентифікації, надавачі, а також їх працівники під час надання послуг електронної ідентифікації та електронних довірчих послуг; відсутність вимог з безпеки та захисту інформації, під час надання послуг електронної ідентифікації та електронних довірчих послуг; актуалізація переліку стандартів, які використовуватимуться надавачами ідентифікації та надавачами під час надання ними послуг; відсутність процедури перевірки дотримання вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг; відсутність порядку використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; відсутність порядку інформування про порушення конфіденційності та/або цілісності інформації під час надання послуг електронної ідентифікації або електронних довірчих послуг, відсутність порядку перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів. ігнорування заходів щодо виконання статей 1, 4^1, 11^2, 13, 18, 20-23, 26-28, 33-33^2 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

2. Оцінка обраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати

Альтернатива 1 Прийняття проекту акта	Прийняття проекту акта матиме такий вплив на інтереси держави: надання послуг електронної ідентифікації та електронних довірчих послуг відповідно встановлення вимог до надавачів ідентифікації та надавачів, їх працівників цих послуг; надання послуг електронної ідентифікації та електронних довірчих послуг з дотриманням вимог з безпеки та захисту інформації; визначення переліку гармонізованих стандартів у сферах електронної ідентифікації та електронних довірчих послуг; врегулювання процедури перевірки дотримання вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг надавачами ідентифікації та надавачами; підвищення рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; підвищення рівня надійності та захищеності електронного документообігу, електронної ідентифікації та електронних довірчих послуг; популяризацію електронного документообігу, використання засобів електронної ідентифікації та електронних довірчих послуг.	Витрат не передбачається
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави	Відсутність регулювання передбачає залишення існуючого стану справ: відсутність встановлених вимог до надавачів ідентифікації, надавачів (у тому числі вимоги з безпеки та захисту інформації та вимоги до працівників надавача) та їхніх відокремлених пунктів реєстрації, а також процедури перевірки їх дотримання; ігнорування заходів щодо виконання статей 1, 4^1, 11^2, 13, 18, 20-23, 26-28, 33-33^2 Закону України

		«Про електронну ідентифікацію та електронні довірчі послуги».

Оцінка впливу на сферу інтересів громадян

Оцінка впливу проекту акта на сферу інтересів громадян не здійснювалася, оскільки такий вплив відсутній.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Оскільки, наразі невідомий кількісний склад суб'єктів господарювання, що мають намір надавати послуги електронної ідентифікації, – неможливо визначити кількісний склад суб'єктів господарювання, що підпадають під дію регулювання, але потенційними суб'єктами можуть стати надавачі.

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць	2	6	4	0	12
Питома вага групи у загальній кількості, відсотків	16,7	50	33,3	0	100

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проекту акта	Прийняття проекту акта в перспективі матиме такий вплив на інтереси суб'єктів господарювання: надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до встановлених вимог; визначення актуального переліку стандартів у сферах ідентифікації та електронних довірчих послуг; можливість використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; встановлення порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації; розширення спектру надання послуг електронної ідентифікації та електронних довірчих послуг; підвищення рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; збільшення кількості	Витрати суб'єктів господарювання на ознайомлення, а також із інформуванням контролюючого органу та користувачів послуг електронної ідентифікації та електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації.

	користувачів послуг електронної ідентифікації та електронних довірчих послуг; збільшення прибутку суб'єкта господарювання.	
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не матиме такого впливу на інтереси суб'єктів господарювання: надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до встановлених вимог; визначення актуального переліку стандартів у сферах ідентифікації та електронних довірчих послуг; можливість використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; встановлення порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації; розширення спектру надання послуг електронної ідентифікації та електронних довірчих послуг; підвищення рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; збільшення кількості користувачів послуг електронної ідентифікації та електронних довірчих послуг; збільшення прибутку суб'єкта господарювання.	Відсутність регулювання означає залишення існуючого стану справ, що не матиме збільшення прибутку суб'єкта господарювання

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1. Сумарні витрати для суб'єктів великого та середнього підприємництва згідно з додатком 2 до Методики та суб'єктів господарювання малого підприємництва згідно з додатком 4 до Методики	2730,00 * 8 = 21 840,00 грн 2730,00 * 4 = 10 920, 00 грн
Альтернатива 2. Сумарні витрати для суб'єктів великого та середнього підприємництва згідно з додатком 2 до Методики та	0,00

суб’єктів господарювання малого підприємництва згідно з додатком 4 до Методики	

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

За результатами аналізу альтернативних способів досягнення цілей державного регулювання здійснено вибір оптимального альтернативного способу з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Бал результативності визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей державного регулювання.

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1 Прийняття проекту акта	4	Прийняття проекту акта сприятиме: надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до встановлених вимог; визначенню актуального переліку стандартів у сферах ідентифікації та електронних довірчих послуг; можливості використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; встановленню порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації; розширенню спектру надання послуг електронної ідентифікації та електронних довірчих послуг; підвищенню рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; збільшенню кількості користувачів послуг електронної ідентифікації та електронних довірчих послуг; збільшенню прибутку суб’єкта господарювання.
Альтернатива 2 Відсутність регулювання	1	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для суб’єктів господарювання, а саме: надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до встановлених вимог; визначення актуального переліку стандартів у

		сферах ідентифікації та електронних довірчих послуг; можливість використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; встановлення порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації; розширення спектру надання послуг електронної ідентифікації та електронних довірчих послуг; підвищення рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; збільшення кількості користувачів послуг електронної ідентифікації та електронних довірчих послуг; збільшення прибутку суб'єкта господарювання.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1 Прийняття проекту постанови	Прийняття проекту акта сприятиме: наданню послуг електронної ідентифікації та електронних довірчих послуг відповідно до встановлених вимог; визначенню актуального переліку стандартів у сферах ідентифікації та електронних довірчих послуг; можливості використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; встановленню порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, електронних довірчих	Витрати суб'єктів господарювання у зв'язку із ознайомленням, а також із інформуванням контролюючого органу та користувачів послуг електронної ідентифікації та електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації.	Цілі, визначені стратегічним документами досягнуті

	послуг про порушення конфіденційності та/або цілісності інформації; розширенню спектру надання послуг електронної ідентифікації та електронних довірчих послуг; підвищенню рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; збільшенню кількості користувачів послуг електронної ідентифікації та електронних довірчих послуг; збільшення прибутку суб'єкта господарювання.		
Альтернатива 2 Відсутність регулювання	Відсутність регулювання означає залишення існуючого стану справ, що не передбачає жодних вигод для держави та суб'єктів господарювання	Відсутність регулювання передбачає залишення існуючого стану справ: відсутність встановлених вимог до надавачів ідентифікації, надавачів (у тому числі вимоги з безпеки та захисту інформації та вимоги до працівників надавача) та їхніх відокремлених пунктів реєстрації, а також процедури перевірки їх дотримання; ігнорування заходів щодо виконання статей 1, 4^1, 11^2, 13, 18, 20-23, 26-28, 33-33^2 Закону України «Про електронну ідентифікацію та електронні довірчі послуги»; надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до встановлених вимог; визначення актуального переліку стандартів у сферах	Недосягнення цілей, визначених стратегічними документами

		ідентифікації та електронних довірчих послуг; можливість використання псевдонімів у засобах електронної ідентифікації та сертифікатах відкритих ключів; встановлення порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації; розширення спектру надання послуг електронної ідентифікації та електронних довірчих послуг; підвищення рівня довіри до послуг електронної ідентифікації та електронних довірчих послуг; збільшення кількості користувачів послуг електронної ідентифікації та електронних довірчих послуг; збільшення прибутку суб'єкта господарювання.	

Рейтинг	Аргументи щодо обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1. Прийняття проекту наказу	Прийняття акту забезпечить баланс інтересів держави та суб'єктів господарювання.	Вплив зовнішніх чинників вбачається незначним, ризики низькі.
Альтернатива 1. Збереження ситуації, яка існує на цей час	Переваги обраної альтернативи відсутні.	Вплив зовнішніх чинників вбачається значним, ризики високі.

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Основним механізмом, який забезпечує розв’язання визначеної проблеми, є затвердження:

Вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг;

Порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації, користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації;

Порядку перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів з використанням відомостей інформаційних систем та публічних електронних реєстрів;

Порядку використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг;

Порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг.

Реалізація регуляторного акта не потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування державними органами.

Організаційні заходи впровадження регуляторного акта в дію:

1. Центральний орган виконавчої влади (Мінцифри):

розробка проекту акта;

забезпечення інформування громадськості шляхом його оприлюднення в засобах масової інформації на офіційному вебсайті Міністерства цифрової трансформації України;

погодження проекту акта із заінтересованими органами;

врахування зауважень та пропозицій до проекту акта, наданих фізичними та юридичними особами, зокрема заінтересованими органами;

подання проекту акта на розгляд Кабінету Міністрів України;

супровід проекту акта під час його розгляду в Кабінеті Міністрів України;

прийняття постанови Кабінету Міністрів України «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг».

2. Заходи, які необхідно здійснити суб’єктам господарювання – ознайомитися з вимогами регулювання:

пошук регуляторного акту в мережі Інтернет та його опрацювання;

інформування контролюючого органу та користувачів послуг електронної ідентифікації та електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації.

Ризику впливу зовнішніх факторів на дію регуляторного акта немає.

Досягнення цілей не передбачає додаткових організаційних заходів.

Можливої шкоди у разі очікуваних наслідків дії акта не прогнозується.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Прямі витрати на виконання вимог регуляторного акта з боку органів виконавчої влади або органів місцевого самоврядування відсутні.

Державне регулювання не передбачає утворення нового державного органу (або нового структурного підрозділу діючого органу).

Проведено розрахунок витрат на одного суб'єкта великого та середнього підприємництва згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта.

Проведено розрахунок витрат для суб'єктів малого підприємництва згідно з додатком 4 до Методики проведення аналізу впливу регуляторного акта (Тест малого підприємництва).

Можлива шкода у разі очікуваних наслідків дії акта не прогнозується.

Негативних наслідків у зв'язку з прийняттям регуляторного акту не очікується.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії проекту акта не обмежений у часі.

Зміна строку дії проекту акта можлива у разі прийняття змін до нього, прийняття змін до нормативно-правових актів, що мають вищу юридичну силу, які стосуються цієї сфери регулювання, або визнання зазначених актів такими, що втратили чинність.

Проект акта набирає чинності з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Показники результативності дії регуляторного акта:

розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта не передбачається.

кількість суб'єктів господарювання та/або фізичних осіб, на яких може поширюватись дія акта (12 надавачів);

розмір коштів і час, що витрачатимуться суб'єктами господарювання та/або фізичними особами, пов'язаними з виконанням вимог акта не передбачається;

рівень поінформованості суб'єктів господарювання та/або фізичних осіб з основних положень акта (високий, – оскільки проект акта розміщено на офіційному вебсайті Міністерства цифрової трансформації України, про що Міністерством цифрової трансформації України повідомлено 12 суб'єктів господарювання);

кількість надавачів ідентифікації;

кількість надавачів;

кількість скарг та пропозицій у зв'язку з дією регуляторного акта.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відповідно до законодавства здійснюється базове, повторне та періодичне відстеження результативності регуляторного акта у строки, встановлені статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Базове відстеження результативності проекту постанови буде здійснюватись через рік після набрання чинності зазначеним актом, оскільки планується використовувати статистичний метод відстеження та статистичні дані.

Повторне відстеження планується здійснити через рік після проведення базового відстеження на основі порівняння показників базового та повторного відстеження.

Періодичні відстеження планується здійснювати раз на три роки, починаючи з дня проведення повторного відстеження. Установлені показники результативності акта порівнюватимуться із значеннями аналогічних показників, що встановлені під час повторного відстеження.

Джерело даних: статистичні дані, отримані від надавачів ідентифікації та надавачів.

Виконавець заходів з відстеження результативності проекту акта – Міністерство цифрової трансформації України.

Віце-прем’єр-міністр України
з інновацій, розвитку освіти, науки
та технологій – Міністр цифрової
трансформації України **Михайло ФЕДОРОВ**

____ _____ 2024 р.

Додаток 2 до Методики проведення
аналізу впливу регуляторного акта

ВИТРАТИ
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

№ з/п	Витрати	За перший рік	**За п'ять років**
1	**Витрати робочого часу на ознайомлення та заповнення заяви (заробітна плата працівників)**	**2184,00**	**0,00**
1.1	Витрати у зв'язку із ознайомленням з проектом акта	2184,00 за 8 годин робочого часу (з розрахунку середньої заробітної плати 16 012,00 грн за місяць)	0,00
2	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам	**546,00**	**0,00**
2.1	Витрати у зв'язку із інформуванням контролюючого органу про порушення конфіденційності та/або цілісності інформації	273,00 за 3 години робочого часу (з розрахунку середньої заробітної плати 16 012,00 грн за місяць)	0,00
2.2	Витрати у зв'язку із інформуванням користувачів послуг електронної ідентифікації та електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації	273,00 за 3 години робочого часу (з розрахунку середньої заробітної плати 16 012,00 грн за місяць)	0,00
3	**РАЗОМ (сума рядків: 1 + 2), гривень**	**2730,00**	**2730,00 грн**
4	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць	**8**	
5	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання)	**21 840,00 грн**	**21 840,00 грн**

Додаток 4 до Методики проведення
аналізу впливу регуляторного акта

ТЕСТ
малого підприємництва (М-Тест)

1. Консультації з представниками мікро- та малого підприємництва щодо оцінки впливу регулювання.

Консультації щодо визначення впливу запропонованого регулювання на суб'єктів малого підприємництва та визначення детального переліку процедур, виконання яких необхідно для здійснення регулювання, проведено розробником у період з 18.10.2023 по 30.10.2023.

Порядковий номер	**Вид консультації (публічні консультації прямі (круглі столи, наради, робочі зустрічі тощо), інтернет-консультації прямі (інтернет-форуми, соціальні мережі тощо), запити (до підприємців, експертів, науковців тощо)**	**Кількість учасників консультацій, осіб**	**Основні результати консультацій (опис)**
1.	Запити до надавачів	12	Реалізацію регуляторного акта підтримано

2. Вимірювання впливу регулювання на суб'єктів малого підприємництва (мікро- та малі):

кількість суб'єктів малого підприємництва, на яких поширюється регулювання: 4;

питома вага суб'єктів малого підприємництва у загальній кількості суб'єктів господарювання, на яких проблема справляє вплив: 33,3%.

3. Розрахунок витрат суб'єктів малого підприємництва на виконання вимог регулювання

Порядковий номер	Найменування оцінки	У перший рік (стартовий рік впровадження регулювання)	Періодичні (за наступний рік)	Витрати за п’ять років
Оцінка вартості адміністративних процедур суб’єктів малого підприємництва щодо виконання регулювання та звітування				
1	Витрати у зв’язку із ознайомленням з проектом акта	2184,00 за 8 годин робочого часу (з розрахунку середньої заробітної плати 16 012,00 грн за місяць)		
2	Витрати у зв’язку із інформуванням контролюючого органу про порушення конфіденційності та/або цілісності інформації	273,00 за 3 години робочого часу (з розрахунку середньої заробітної плати 16 012,00 грн за місяць)		
3	Витрати у зв’язку із інформуванням користувачів послуг електронної ідентифікації та електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації	273,00 за 3 години робочого часу (з розрахунку середньої заробітної плати 16 012,00 грн за місяць)		
4	Разом, гривень	2 730,00	2 730,00 грн	2 730,00
5	Кількість суб’єктів господарювання, що повинні виконати вимоги регулювання, одиниць	4		
6	Сумарно, гривень	2 730,00* 4 = 10 920,00 грн	10 920	10 920,00 грн

4. Бюджетні витрати на адміністрування регулювання суб’єктів малого підприємництва

Додаткові витрати на виконання вимог регуляторного акту з боку органів виконавчої влади або органів місцевого самоврядування відсутні.

Витрати на виконання вимог регуляторного акту з боку органів виконавчої влади або органів місцевого самоврядування будуть відповідати витратам на

заробітну плату співробітників, які за функціональними обов'язками уже здійснюють та в подальшому здійснюватимуть відповідні заходи.

Державне регулювання не передбачає утворення нового державного органу або нового структурного підрозділу діючого органу.

5. Розрахунок сумарних витрат суб'єктів малого підприємництва, що виникають на виконання вимог регулювання.

№ п/п	Показник	Перший рік регулювання (стартовий)	За п'ять років
1	Оцінка "прямих" витрат суб'єктів малого підприємництва на виконання регулювання	0	0
2	Оцінка вартості адміністративних процедур для суб'єктів малого підприємництва щодо виконання регулювання та звітування	10 920,00 грн	0,00 (суб'єкт повинен виконувати вимоги регулювання лише в перший рік)
3	Сумарні витрати малого підприємництва на виконання запланованого регулювання	10 920,00 грн	0,00 (суб'єкт повинен виконувати вимоги регулювання лише в перший рік)
4	Сумарні витрати на виконання запланованого регулювання	10 920,00 грн	10 920,00 грн

6. Розроблення коригуючих (пом'якшувальних) заходів для малого підприємництва щодо запропонованого регулювання не передбачається.

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від __ _____ 2024 р. № ____

Київ

Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг

Відповідно до статей 4^1, 11^2, 13, 18, 20-23, 26-28 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” Кабінет Міністрів України **постановляє**:

1. Затвердити такі, що додаються:

Вимоги до надавачів послуг електронної ідентифікації та електронних довірчих послуг;

Порядок інформування контролюючого органу та користувачів послуг електронної ідентифікації, користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації;

Порядок перевірки інформації про осіб, яким видаються засоби електронної ідентифікації або кваліфіковані сертифікати відкритих ключів з використанням відомостей інформаційних систем та публічних електронних реєстрів;

Порядок використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг;

Порядок проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг.

2. Визнати такими, що втратили чинність, постанови Кабінету Міністрів України згідно з переліком, що додається.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від ____ _____ 2024 р. № _____

ПЕРЕЛІК
постанов Кабінету Міністрів України, що втратили чинність

1. Постанова Кабінету Міністрів України від 7 листопада 2018 р. № 992 “Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг” (Офіційний вісник України, 2018 р., № 98, ст. 3227).

2. Пункт 5 змін, що вносяться до постанов Кабінету Міністрів України, затверджених постановою Кабінету Міністрів України від 11 грудня 2019 р. № 1068 (Офіційний вісник України, 2020 р., № 2, ст. 68).

3. Постанова Кабінету Міністрів України від 30 березня 2023 р. № 289 “Про внесення змін до постанови Кабінету Міністрів України від 7 листопада 2018 р. № 992” (Офіційний вісник України, 2023 р., № 38, ст. 2020).

4. Пункт 1 постанови Кабінету Міністрів України від 4 квітня 2023 р. № 298 “Деякі питання здійснення ідентифікації у сфері електронних довірчих послуг” та пункт 2 змін, що вносяться до постанов Кабінету Міністрів України від 19 вересня 2018 р. № 749 і від 7 листопада 2018 р. № 992, затверджених постановою Кабінету Міністрів України від 4 квітня 2023 р. № 298 “Деякі питання здійснення ідентифікації у сфері електронних довірчих послуг” (Офіційний вісник України, 2023 р. № 39, ст. 2060).

Додаток
до вимог до надавачів послуг
електронної ідентифікації та
електронних довірчих послуг

(пункт 5 Вимог)

ПЕРЕЛІК СТАНДАРТІВ,
що застосовуються кваліфікованими надавачами електронних довірчих послуг для надання кваліфікованих електронних довірчих послуг

Стандарти, що визначають загальні вимоги до кваліфікованого надавача електронних довірчих послуг для надання кваліфікованих електронних довірчих послуг

1. ДСТУ ETSI TR 119 400:2017 (ETSI TR 119 400:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів провайдерами довірчих послуг, які підтримують цифрові підписи та пов’язані з ними послуги”.

2. ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.

3. ДСТУ ETSI EN 319 403-1:2021 (ETSI EN 319 403-1 V2.3.1 (2020-06), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг”.

4. ДСТУ ETSI TS 119 403-2:2021 (ETSI TS 119 403-2 V1.2.4 (2020-11), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 2. Додаткові вимоги до органів оцінювання відповідності, що перевіряють постачальників довірчих послуг, які видають довірчі сертифікати”.

5. ДСТУ ETSI TS 119 403-3:2021 (ETSI TS 119 403-3 V1.1.1 (2019-03), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 3. Додаткові вимоги до органів оцінювання відповідності, які оцінюють кваліфікованих постачальників довірчих послуг в ЄС”.

6. ДСТУ ETSI TS 119 441:2019 (ETSI TS 119 441 V1.1.1 (2018-08), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги політики стосовно TSP, що надає послуги щодо перевірення підписів”.

7. ДСТУ ETSI TS 119 461:2022 (ETSI TS 119 461 V1.1.1 (2021-07), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки компонентів довірчих послуг що забезпечують ідентифікацію особи суб’єктів довірчих послуг”.

8. ДСТУ ETSI TS 119 511:2019 (ETSI TS 119 511 V1.1.1 (2019-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг, що забезпечують тривале збереження цифрових підписів чи загальних даних, використовуючи методи цифрового підпису”.

9. ДСТУ ETSI TS 119 512:2021 (ETSI TS 119 512 V1.1.2 (2020-10), IDT) “Електронні підписи та інфраструктури (ESI). Протоколи для постачальників довірчих послуг, що надають послуги довгострокового зберігання даних”.

Стандарти, що визначають вимоги до Довірчого списку

10. ДСТУ ETSI TR 119 600:2016 (ETSI TR 119 600:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для провайдерів переліків стану довірчих послуг”.

11. ДСТУ ETSI TS 119 612:2016 (ETSI TS 119 612:2016, IDT) “Електронні підписи та інфраструктури. Довірчі списки”.

12. ДСТУ ETSI TS 119 614-1:2017 (ETSI TS 119 614-1:2016, IDT) “Електронні підписи та інфраструктури. Тестування довірених списків на відповідність та інтероперабельність. Частина 1. Специфікації для тестування на відповідність XML-подання довірених списків”.

13. ДСТУ ETSI TS 119 615:2021 (ETSI TS 119 615 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки. Процедури використання та тлумачення національних довірчих списків держав-членів Європейського Союзу”.

Стандарти, що визначають вимоги до надання кваліфікованих електронних довірчих послуг, пов'язаних із створенням, перевіркою та підтвердженням електронних підписів, печаток, а також зберіганням кваліфікованих електронних підписів, печаток, електронних позначок часу та відповідних сертифікатів відкритих ключів

14. ДСТУ ETSI TR 119 000:2017 (ETSI TR 119 000:2016, IDT) "Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Огляд".

15. ДСТУ ETSI TR 119 001:2017 (ETSI TR 119 001:2016, IDT) "Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Визначення понять та скорочення".

16. ДСТУ ETSI TR 119 100:2017 (ETSI TR 119 100:2016, IDT) "Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів для створення та валідації підпису".

17. ДСТУ ETSI TS 119 101:2016 (ETSI TS 119 101:2016, IDT) "Електронні підписи та інфраструктури. Вимоги та політики безпеки для додатків формування та перевірки підписів".

18. 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".

19. ДСТУ ETSI TS 119 102-2:2022 (ETSI TS 119 102-2 V1.3.1 (2021-09), IDT) "Електронні підписи та інфраструктури (ESI). Процедури створення та перевірки цифрових підписів AdES. Частина 2. Звіт про перевірку підпису".

20. 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".

21. ДСТУ ETSI TS 119 172-2:2021 (ETSI TS 119 172-2 V1.1.1 (2019-12), IDT) "Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 2. Формат XML для політики підписування".

22. ДСТУ ETSI TS 119 172-3:2021 (ETSI TS 119 172-3 V1.1.1 (2019-12), IDT) "Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 3. Формат ASN.1 для політики підписування".

23. ДСТУ ETSI TS 119 172-4:2021 (ETSI TS 119 172-4 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 4. Правила застосування підписів (політика перевірки) для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків”.

24. ДСТУ ETSI TS 119 441:2019 (ETSI TS 119 441 V1.1.1 (2018-08), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги політики стосовно TSP, що надає послуги щодо перевірення підписів”.

25. 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”.

26. ДСТУ ETSI EN 319 122-1:2021 (ETSI EN 319 122-1 V1.2.1 (2021-10), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES”.

27. ДСТУ ETSI EN 319 122-2:2021 (ETSI EN 319 122-2 V1.2.1 (2021-10), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES”.

18. 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”.

29. ДСТУ ETSI EN 319 132-2:2021 (ETSI EN 319 132-2 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES”.

30. ДСТУ ETSI EN 319 142-1:2016 (ETSI EN 319 142-1:2016, IDT) “Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 1. Структурні елементи та базові PAdES підписи”.

31. ДСТУ ETSI EN 319 142-2:2016 (ETSI EN 319 142-2:2016, IDT) “Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 2. Додаткові профілі підписів PAdES”.

32. ДСТУ ETSI EN 319 162-1:2021 (ETSI EN 319 162-1 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Контейнери пов’язаних підписів (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC”.

33. ДСТУ ETSI EN 319 162-2:2021 (ETSI EN 319 162-2 V.1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Контейнери пов’язаних підписів (ASiC). Частина 2. Додаткові контейнери ASiC”.

34. ДСТУ ETSI TS 119 132-3:2022 (ETSI TS 119 132-3 V1.1.1 (2021-01), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 3. Уведення механізмів синтаксису запису доказів (ERS) у XAdES”.

35. ДСТУ ETSI TS 119 182-1:2022 (ETSI TS 119 182-1 V1.1.1 (2021-03), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи JAdES. Частина 1. Структурні блоки та базові підписи JAdES”.

36. ДСТУ ETSI TS 119 192:2022 (ETSI TS 119 192 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Уніфікований ідентифікатор ресурсу, пов’язаний з AdES”.

37. ДСТУ ETSI TS 102 778-1:2015 (ETSI TS 102 778-1:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 1. Огляд серії PAdES - базові принципи PAdES”.

38. ДСТУ ETSI TS 102 778-2:2015 (ETSI TS 102 778-2:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 2. Базовий PAdES - профілі, що базуються на ISO 32000-1”.

39. ДСТУ ETSI TS 102 778-3:2015 (ETSI TS 102 778-3:2010, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 3. Посилений PAdES - профілі PAdES-BES і PadES-EPES”.

40. ДСТУ ETSI TS 102 778-4:2015 (ETSI TS 102 778-4:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 4. Довгостроковий PAdES - профіль PAdES LTV”.

41. ДСТУ ETSI TS 102 778-5:2015 (ETSI TS 102 778-5:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 5. PAdES для XML контенту - профілі для підписів XAdES”.

Стандарти, що визначають вимоги до надання кваліфікованих електронних довірчих послуг, пов'язаних з формуванням, перевіркою та підтвердженням чинності кваліфікованих сертифікатів електронного підпису, печатки, автентифікації веб-сайту

42. ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги".

43. ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС".

44. ДСТУ ETSI EN 319 412-4:2022 (ETSI EN 319 412-4 V1.2.1 (2021-11), IDT) "Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів вебсайтів".

45. ДСТУ ETSI TR 119 411-4:2021 (ETSI TR 119 411-4 V1.1.1 (2018-05), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг, які видають сертифікати. Частина 4. Контрольний список підтримки аудиту TSP на відповідність ETSI EN 319 411-1 чи ETSI EN 319 411-2".

Стандарти, що визначають вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження кваліфікованої електронної позначки часу

46. ДСТУ ETSI EN 319 421:2016 (ETSI EN 319 421:2016, IDT) "Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі".

47. ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT) "Електронні підписи та інфраструктури. Протокол мітки часу та профілі токенів мітки часу".

Стандарти, що визначають вимоги до засобів кваліфікованого електронного підпису чи печатки

48. ДСТУ EN 419211-1:2016 (EN 419211-1:2014, IDT) "Профілі захисту для пристроїв створення безпечного підпису. Частина 1. Огляд".

49. ДСТУ EN 419211-2:2016 (EN 419211-2:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 2. Пристрій з генерацією ключів”.

50. ДСТУ EN 419211-3:2016 (EN 419211-3:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 3. Пристрій з імпортом ключів”.

51. ДСТУ EN 419211-4:2016 (EN 419211-4:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 4. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування генерації сертифікатів”.

52. ДСТУ EN 419211-5:2016 (EN 419211-5:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 5. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування створення підпису”.

53. ДСТУ EN 419211-6:2016 (EN 419211-6:2014, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 6. Розширення для пристроїв з імпортом ключів та довіреним каналом для застосування створення підпису”.

54. ДСТУ ISO/IEC 19790:2015 (ISO/IEC 19790:2012, IDT) “Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів”.

55. ДСТУ EN 419221-5:2018 (EN 419221-5:2018, IDT) “Профілі захисту для криптографічних модулів TSP. Частина 5. Криптографічний модуль для довірчих послуг”.

56. ДСТУ CEN/TS 419221-6:2021 (CEN/TS 419221-6:2019, IDT) “Умови застосування EN 419221-5 як кваліфікованого пристрою для створення електронного підпису або печатки”.

57. ДСТУ EN 419231:2021 (EN 419231:2019, IDT) “Профіль захисту для надійних систем, що підтримують відмітку часу”.

58. ДСТУ EN 419241-1:2021 (EN 419241-1:2018, IDT) “Надійні системи, що підтримують підписи серверів. Частина 1. Загальні вимоги щодо безпеки системи”.

59. ДСТУ EN 419241-2:2021 (EN 419241-2:2019, IDT) “Надійні системи, що підтримують підписи серверів. Частина 2. Профіль захисту для QSCD для підписів серверів”.

60. ДСТУ ETSI TS 119 431-1:2022 (ETSI TS 119 431-1 V1.2.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 1. Компоненти сервісу TSP, що працюють віддаленим QSCD/SCDev”.

61. ДСТУ ETSI TS 119 431-2:2019 (ETSI TS 119 431-2 V1.1.1 (2018-12), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 2. Компоненти сервісу TSP, що підтримують створення цифрового підпису AdES”.

62. ДСТУ ETSI TS 119 432-2:2022 (ETSI TS 119 432 V1.2.1 (2020-10), IDT) “Електронні підписи та інфраструктури (ESI). Протоколи віддаленого створення цифрового підпису”.

63. ДСТУ ETSI TS 119 495:2022 (ETSI TS 119 495 V1.5.1 (2021-04), IDT) “Електронні підписи та інфраструктури (ESI). Секторальні специфічні вимоги. Профілі сертифікатів і вимоги політики TSP для відкритого банківського обслуговування”.

Стандарти, що визначають вимоги до кваліфікованих сертифікатів відкритих ключів

64. ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів”.

65. ДСТУ ETSI EN 319 412-1:2021 (ETSI EN 319 412-1 V1.4.4 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних”.

66. ДСТУ ETSI EN 319 412-2:2021 (ETSI EN 319 412-2 V2.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам”.

67. ДСТУ ETSI EN 319 412-3:2021 (ETSI EN 319 412-3 V1.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профілі сертифікатів, виданих юридичним особам”.

68. ДСТУ ETSI EN 319 412-4:2022 (ETSI EN 319 412-4 V1.2.1 (2021-11), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів вебсайтів”.

69. ДСТУ ETSI EN 319 412-5:2022 (ETSI EN 319 412-5 V2.3.1 (2020-04), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Розширення сертифікатів QCStatements”.

Стандарти, що визначають вимоги до надання кваліфікованої електронної довірчої послуги з реєстрованої електронної доставки

70. ДСТУ ETSI EN 319 521:2019 (ETSI EN 319 521 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для зареєстрованих постачальників послуг електронної пошти”.

71. ДСТУ ETSI EN 319 522-1:2018 (ETSI EN 319 522-1:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 1. Модель та архітектура”.

72. ДСТУ ETSI EN 319 522-2:2018 (ETSI EN 319 522-2:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 2. Семантика вмісту”.

73. ДСТУ ETSI EN 319 522-3:2018 (ETSI EN 319 522-3:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 3. Формати”.

74. ДСТУ ETSI EN 319 522-4-1:2021 (ETSI EN 319 522-4-1 V1.2.1 (2019-01), IDT) “Електронні підписи та інфраструктури (ESI). Електронні послуги реєстрованого доставляння. Частина 4. Прив'язки. Секція 1. Прив’язки доставляння повідомлень”.

75. ДСТУ ETSI TS 119 524-1:2021 (ETSI TS 119 524-1 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Перевірка відповідності та функційної сумісності електронних послуг реєстрованого доставляння. Частина 1. Перевірка відповідності”.

76. ДСТУ ETSI TS 119 524-2:2021 (ETSI TS 119 524-2 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Перевірка відповідності та функційної сумісності електронних послуг реєстрованого доставляння. Частина 2. Набори для тестування на функційну сумісність постачальників електронних послуг реєстрованого доставляння”.

77. ДСТУ ETSI EN 319 522-4-2:2018 (ETSI EN 319 522-4-2:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого

електронного доставляння. Частина 4. Прив’язки. Секція 2. Прив’язки доказів та ідентифікації”.

78. ДСТУ ETSI EN 319 522-4-3:2018 (ETSI EN 319 522-4-3:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 4. Прив’язки. Секція 3. Прив’язка можливостей/вимог”.

79. ДСТУ ETSI EN 319 531:2019 (ETSI EN 319 531 V1.1.1 (2019-01), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для провайдерів служби реєстрованої електронної пошти”.

80. ДСТУ ETSI EN 319 532-1:2018 (ETSI EN 319 532-1:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 1. Модель та архітектура”.

81. ДСТУ ETSI EN 319 532-2:2018 (ETSI EN 319 532-2:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 2. Семантика вмісту”.

82. ДСТУ ETSI EN 319 532-3:2022 (ETSI EN 319 532-3 V1.2.1 (2019-04), IDT) “Електронні підписи та інфраструктури (ESI). Послуги зареєстрованої електронної пошти (REM). Частина 3. Формати”.

83. ДСТУ ETSI EN 319 532-4:2022 (ETSI EN 319 532-3 V1.2.1 (2022-05), IDT) “Електронні підписи та інфраструктури (ESI). Послуги зареєстрованої електронної пошти (REM). Частина 4. Профілі сумісності”.

84. ДСТУ ETSI TS 119 534-1:2021 (ETSI TS 119 534-1 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Перевірка відповідності та функційної сумісності реєстрованих послуг електронної пошти. Частина 1. Перевірка відповідності”.

85. ДСТУ ETSI TS 119 534-2:2021 (ETSI TS 119 534-2 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Перевірка відповідності та функційної сумісності реєстрованих послуг електронної пошти. Частина 2. Набори для тестування на сумісність постачальників, що використовують однаковий формат та транспортні протоколи”.

Стандарти, що визначають вимоги до криптографічного захисту інформації

86. ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”.

87. ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”.

88. ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”.

89. ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”.

90. ДСТУ ETSI TR 103 570:2022 (ETSI TR 103 570 V1.1.1 (2017-10), IDT) “Кібербезпека. Квантово-безпечний обмін ключами”.

91. ДСТУ ETSI TR 103 616:2022 (ETSI TR 103 616 V1.1.1 (2021-09), IDT) “Кібербезпека. Квантово-безпечні підписи”.

92. ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021-10), IDT) “Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів”.

93. ДСТУ ETSI TR 119 300:2016 (ETSI TR 119 300:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для криптографічних комплектів”.

94. ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”.

95. ДСТУ ISO/IEC 14888-1:2015 (ISO/IEC 14888-1:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення”.

96. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

97. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі дискретного логарифмування”.

98. ДСТУ ISO/IEC 18032:2022 (ISO/IEC 18032:2020, IDT) “Інформаційні технології. Методи захисту. Генерування простого числа”.

99. ДСТУ ISO/IEC 18033-6:2022 (ISO/IEC 18033-6:2019, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 6. Гомоморфне шифрування”.

100. ДСТУ ISO/IEC 19772:2022 (ISO/IEC 19772:2020, IDT) “Інформаційна безпека. Автентифіковане шифрування”.

Стандарти, що визначають вимоги до інформаційної безпеки

101. ДСТУ ISO/IEC 18045:2015 (ISO/IEC 18045:2008, IDT) “Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ”.

102. ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель”.

103. ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки”.

104. ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення”.

105. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”.

106. ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”.

107. ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) “Методи безпеки. Розширення до ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови”.

108. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”.

Стандарти щодо тестування інтероперабельності

109. ДСТУ ETSI SR 003 186:2017 (ETSI SR 003 186:2016, IDT) “Електронні підписи та інфраструктури (ESI). Тестування інтероперабельності та заходи, необхідні для імплементації та популяризації моделі цифрових підписів”.

110. ДСТУ ETSI TS 119 124-4:2017 (ETSI TS 119 124-4:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Перевірка на відповідність і інтероперабельність. Частина 4. Тестування на відповідність базових підписів CAdES”.

111 ДСТУ ETSI TR 119 134-1:2017 (ETSI TR 119 134-1:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 1. Огляд”.

112. ДСТУ ETSI TS 119 134-2:2017 (ETSI TS 119 134-2:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність Частина 2. Набори тестів для тестування інтероперабельності базових підписів XAdES”.

113. ДСТУ ETSI TS 119 134-3:2017 (ETSI TS 119 134-3:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність Частина 3. Набори тестів для тестування інтероперабельності посилених підписів XAdES”.

114. ДСТУ ETSI TS 119 134-4:2017 (ETSI TS 119 134-4:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність Частина 4. Тестування на відповідність базовим підписам XAdES”.

115. ДСТУ ETSI TS 119 134-5:2017 (ETSI TS 119 134-5:2016; IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Тестування на відповідність та інтероперабельність. Частина 5. Тестування на відповідність посилених підписів XAdES”.

116. ДСТУ ETSI TR 119 144-1:2017 (ETSI TR 119 144-1:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 1. Огляд”.

117. ДСТУ ETSI TS 119 144-2:2017 (ETSI TS 119 144-2:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 2. Набори тестів для тестування інтероперабельності базових підписів PAdES”.

118. ДСТУ ETSI TS 119 144-3:2017 (ETSI TS 119 144-3:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 3. Набори тестів для тестування інтероперабельності додаткових підписів PAdES”.

119. ДСТУ ETSI TS 119 144-4:2017 (ETSI TS 119 144-4:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 4. Тестування відповідності базових підписів PAdES”.

120. ДСТУ ETSI TS 119 144-5:2017 (ETSI TS 119 144-5:2016, IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Тестування відповідності та інтероперабельності. Частина 5. Тестування відповідності додаткових підписів PAdES”.

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від ____ _____ 2024 р. № _____

ВИМОГИ
до надавачів послуг електронної ідентифікації та електронних довірчих послуг

Загальні положення

1. Ці вимоги визначають організаційно-методологічні, технічні та технологічні умови, яких повинні дотримуватися надавачі послуг електронної ідентифікації (далі – надавачі ідентифікації), а також надавачі електронних довірчих послуг (кваліфіковані та некваліфіковані) (далі – надавачі), у тому числі з безпеки та захисту інформації, та їх відокремлені пункти реєстрації під час надання послуг електронної ідентифікації та електронних довірчих послуг, а також працівники надавача.

2. Дія цих вимог не поширюється на надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Закон).

3. У цих вимогах терміни вживаються в такому значенні:

власник веб-сайту – користувач кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

геш-значення – фіксовані за обсягом електронні дані, утворені шляхом перетворення електронних даних із застосуванням криптографічного алгоритму;

заявник – фізична особа, у тому числі іноземець, фізична особа-підприємець, юридична особа та їх уповноважені представники, що звернулись до надавача ідентифікації чи надавача для отримання послуг електронної ідентифікації та електронних довірчих послуг;

інформаційно-комунікаційна система центрального засвідчувального органу – сукупність інформаційних та комунікаційних систем центрального засвідчувального органу, які у процесі обробки інформації діють як єдине ціле та об’єднують програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг, інші складові системи, що використовуються для ведення Довірчого списку, постачання передачі сигналів точного часу, синхронізованого із Всесвітнім координованим часом (UTC) з

використанням національної шкали часу UTC (UA), забезпечення інтероперабельності та технологічної нейтральності технічних рішень, взаємного визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг, досліджень поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень, визначених статтями 7 та 7^1 Закону, фізичне середовище, інформацію, що обробляється в цих системах, а також найманих працівників, які безпосередньо залучені в наданні послуг або обслуговують інформаційно-комунікаційну систему;

користувач засобу електронної ідентифікації – особа, якій надавач послуг електронної ідентифікації видав засіб електронної ідентифікації згідно із схемою, внесеною до переліку схем електронної ідентифікації;

онлайн-операція – будь-яка дія, технологічна схема якої передбачає наявність безперервного комунікаційного зв’язку в режимі реального часу під час її проведення;

перевірка – виїзний захід державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг, що здійснюється посадовими особами контролюючого органу відповідно до їх функціональних обов’язків за місцезнаходженням надавача, центрального засвідчувального органу або засвідчувального центру;

політика сертифіката – перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг (далі – кваліфікований надавач) у процесі надання кваліфікованих електронних довірчих послуг з формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;

положення сертифікаційних практик – перелік усіх практичних дій та процедур, які застосовуються для реалізації політики сертифіката кваліфікованого надавача;

програмний інтерфейс центрального засвідчувального органу – складова інформаційно-комунікаційної системи центрального засвідчувального органу для забезпечення інтероперабельності, дослідження поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень, визначених статтями 7 та 7^1 Закону;

публікація кваліфікованого сертифіката відкритого ключа – надання кваліфікованого сертифіката відкритого ключа користувачеві та, у разі його згоди, – іншим особам шляхом розміщення його на веб-сайті надавача;

розповсюдження інформації про статус кваліфікованого сертифіката відкритого ключа – надання вільного доступу до інформації про статус кваліфікованого сертифіката відкритого ключа;

список відкликаних сертифікатів відкритих ключів – сформований та опублікований надавачем, центральним засвідчувальним органом/засвідчувальним центром перелік кваліфікованих сертифікатів відкритих ключів, статус яких змінено на заблокований, поновлений або скасований;

статус кваліфікованого сертифіката відкритого ключа – стан кваліфікованого сертифіката відкритого ключа (чинний, заблокований, скасований) на певний момент часу;

управління статусом сертифіката – зміна статусу кваліфікованого сертифіката відкритого ключа надавачем.

4. Інші терміни 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”, “Про основні засади забезпечення кібербезпеки України”, “Про регулювання містобудівної діяльності”, постанові Кабінету Міністрів України від 11 серпня 2023 р. № 844 “Про затвердження вимог до Довірчого списку” (Офіційний вісник України 2023 р., № 79, ст. 4487) та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.

5. Формування сертифікатів відкритих ключів повинно здійснюватись з дотриманням таких стандартів:

ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів”.

ДСТУ ETSI EN 319 412-1:2021 (ETSI EN 319 412-1 V1.4.4 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних”.

ДСТУ ETSI EN 319 412-2:2021 (ETSI EN 319 412-2 V2.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам”.

ДСТУ ETSI EN 319 412-3:2021 (ETSI EN 319 412-3 V1.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профілі сертифікатів, виданих юридичним особам”.

ДСТУ ETSI EN 319 412-4:2022 (ETSI EN 319 412-4 V1.2.1 (2021-11), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів вебсайтів”.

Кваліфіковані надавачі мають право самостійно обирати в рамках кожної послуги, які саме стандарти вони будуть застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, що додається (далі – Перелік).

Вимоги до надавачів ідентифікації

6. Надавач ідентифікації надає послугу електронної ідентифікації за схемою, внесеною до переліку схем електронної ідентифікації.

7. Надавачі ідентифікації під час видачі засобів електронної ідентифікації мають право здійснювати перевірку інформації, яка міститься у засобі електронної ідентифікації, який видається особі, з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів – за зверненнями громадян), Державного реєстру фізичних осіб – платників податків, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України "Про публічні електронні реєстри", отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації відповідно до статті 11^2 Закону.

8. Надання послуг електронної ідентифікації надавачами ідентифікації має здійснюватись з дотриманням таких стандартів:

ДСТУ EN ISO/IEC 29100:2022 (EN ISO/IEC 29100:2020, IDT; ISO/IEC 29100:2011, including Amd 1:2018, IDT) "Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя";

ДСТУ ISO/IEC 29101:2018 (ISO/IEC 29101:2013, IDT) "Інформаційні технології. Методи захисту. Структура архітектури забезпечення прайвесі";

ДСТУ ISO/IEC 19989-1:2023 (ISO/IEC 19989-1:2020, IDT) "Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 1. Структура";

ДСТУ ISO/IEC 19989-2:2023 (ISO/IEC 19989-2:2020, IDT) "Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 2. Ефективність біометричного розпізнавання";

ДСТУ ISO/IEC 24745:2023 (ISO/IEC 24745:2022, IDT) "Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації";

ДСТУ ISO/IEC 30107-1:2023 (ISO/IEC 30107-1:2016, IDT) "Інформаційні технології. Виявлення атак на біометричне подання. Частина 1. Структура";

ДСТУ ISO/IEC 30107-2:2023 (ISO/IEC 30107-2:2017, IDT) "Інформаційні технології. Виявлення атак на біометричне подання. Частина 2. Формати даних";

ДСТУ ISO/IEC 30107-3:2023 (ISO/IEC 30107-3:2017, IDT) "Інформаційні технології. Виявлення атак на біометричне подання. Частина 3. Тестування та звітування";

ДСТУ ISO/IEC 30107-4:2023 (ISO/IEC 30107-4:2020, IDT) “Інформаційні технології. Виявлення атак на біометричне подання. Частина 4. Профіль для тестування мобільних пристроїв”;

ДСТУ ISO/IEC 29146:2023 (ISO/IEC 29146:2016, IDT) “Інформаційні технології. Методи безпеки. Структура керування доступом”;

ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель”;

ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки”;

ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення”;

ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності”;

ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки”;

ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ”;

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”;

ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”;

ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”;

ДСТУ ISO/IEC 27551:2023 (ISO/IEC 27551:2021, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Вимоги до автентифікації непов’язаних об’єктів на основі атрибутів”.

9. Надавачі ідентифікації забезпечують створення та функціонування свого веб-сайту.

10. Надавачі ідентифікації забезпечують розміщення на своєму веб-сайті актуальної інформації про умови отримання послуг електронної ідентифікації, а також можуть вести реєстрацію користувачів засобів електронної ідентифікації.

11. Надавачі ідентифікації під час надання послуг електронної ідентифікації мають забезпечувати дотримання положень, визначених статтею 11^2 Закону.

12. Засоби електронної ідентифікації, що надаються надавачами ідентифікації в рамках відповідних схем електронної ідентифікації, повинні відповідати рівням довіри, визначеним статтею 15 Закону.

13. Надання засобів електронної ідентифікації надавачем ідентифікації не внесених до переліку схем електронної ідентифікації забороняється.

14. Реєстрація користувачів засобів електронної ідентифікації може здійснюватися через відокремлені пункти реєстрації, які виконують свої функції з дотриманням вимог законодавства у сферах електронної ідентифікації та захисту інформації.

Вимоги до надавачів та їх працівників

15. Вимоги до працівників надавачів їх обов'язки, а також процеси та регламентні процедури, що пов'язані з генерацією та зберіганням особистих ключів надавача, визначаються з дотриманням таких стандартів:

ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг";

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги";

ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС";

ДСТУ ETSI EN 319 421:2016 (ETSI EN 319 421:2016, IDT) "Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі".

16. Кваліфікований надавач для надання електронних довірчих послуг призначає розпорядчим актом керівника кваліфікованого надавача, адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки, аудитора системи (далі – працівники надавача). Кваліфікований надавач має право призначити розпорядчим актом заступника керівника кваліфікованого, який виконує функції керівника

кваліфікованого надавача у разі його відсутності або за його письмовим дорученням.

17. Працівникам надавача забороняється суміщення посадових обов'язків адміністратора безпеки з посадами адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, аудитора системи.

18. Працівники надавача, повинні мати необхідні для надання електронних довірчих послуг знання, досвід і кваліфікацію.

Адміністратором сертифікації, системним адміністратором, аудитором системи може бути особа, яка має вищу освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом у зазначених сферах не менше трьох років.

Адміністратором реєстрації може бути будь-яка фізична особа, яка має навички роботи з комп'ютерною технікою.

Адміністратором безпеки може бути особа, яка має стаж роботи у сфері захисту інформації або кібербезпеки не менше трьох років та відповідає хоча б одній з умов:

1) має вищу освіту за спеціальністю у сферах кібербезпеки та захисту інформації;

2) має вищу освіту за спеціальністю у сфері інформаційних технологій та отримала сертифікат про підвищення кваліфікації у сфері кібербезпеки та захисту інформації.

19. Організаційно-правовий статус керівника і працівників надавача, їх завдання та функції, права та обов'язки, відповідальність, а також професійні знання, досвід і кваліфікація визначаються функціональними обов'язками.

Функціональні обов'язки повинні містити вимоги інформаційної безпеки.

20. Керівник і працівники надавача повинні бути ознайомлені з положеннями, якими передбачені їх функціональні обов'язки, та дотримуватись завдань та функцій, визначених такими положеннями.

21. Діяльність кваліфікованих надавачів здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів, або рахунок у Національному банку – для банків – кваліфікованих надавачів, кваліфікованого надавача, створеного Національним банком) для забезпечення відшкодування шкоди, яка може бути завдана користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем своїх зобов'язань або страхування відповідальності для забезпечення відшкодування такої шкоди у розмірі, визначеному частиною п'ятою статті 16 Закону.

Кваліфіковані надавачі повинні підтримувати розмір внеску на поточному рахунку із спеціальним режимом використання або розмір страхової суми в актуальному стані та у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання своїх зобов'язань, – відновити його протягом трьох місяців з дня настання таких змін.

22. Кваліфікований надавач надає кваліфіковані електронні довірчі послуги відповідно до вимог законодавства у сфері електронних довірчих послуг, а також регламенту роботи кваліфікованого надавача (далі – Регламент).

23. Регламент розробляється та затверджується до початку роботи кваліфікованого надавача.

24. Структура регламенту, у тому числі політика сертифіката та положення сертифікаційних практик, передбачені ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг", ДСТУ ETSI EN 319 411-1:2022 (ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021–05), IDT "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги".

25. Регламент роботи підлягає обов'язковому погодженню з Мінцифри або із Національним банком – для кваліфікованих надавачів, зазначених в абзаці першому частини першої статті 9 Закону, (далі – орган погодження).

Регламент надсилається органу погодження в електронній формі з дотриманням вимог законодавства у сферах електронного документообігу, електронної ідентифікації та електронних довірчих послуг.

До Мінцифри Регламент може надсилатись через програмний інтерфейс інформаційно-комунікаційної системи центрального засвідчувального органу.

До Національного банку Регламент може надсилатись на електронну поштову скриньку Національного банку nbu@bank.gov.ua або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку.

Строк погодження Регламенту становить 30 календарних днів після його надходження.

Підставами для відмови у погодженні Регламенту є:

виявлення у Регламенті недостовірних відомостей, пошкоджень, які не дають змоги однозначно тлумачити зміст, виправлень або дописок;

невідповідність структури Регламенту вимогам, зазначеним у пункті 24 цих Вимог.

Процедура погодження проекту регламенту проводиться безоплатно.

Регламент після погодження органом погодження затверджується ~~його~~ керівником кваліфікованого надавача та передається до органу погодження протягом десяти робочих днів з моменту його затвердження.

Копію затвердженого Регламенту орган погодження передає Адміністрації Держспецзв'язку протягом п'яти робочих днів з моменту його отримання.

26. Для погодження змін до Регламенту кваліфікованим надавачем надсилається до органу погодження текст відповідних змін та порівняльна таблиця у спосіб, визначений у пункті 25 цих вимог (порівняльна таблиця не надсилається у разі внесення змін до Регламенту шляхом викладення в новій редакції).

27. Кваліфікований надавач самостійно визначає обсяг положень Регламенту роботи та інших документів, що підлягають розміщенню на його веб-сайті для ознайомлення користувачів електронних довірчих послуг з інформацією про умови отримання кваліфікованих електронних довірчих послуг.

28. Заява про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що додаються до неї, можуть бути подані представником юридичної особи або фізичною особою – підприємцем, який має намір надавати кваліфіковані електронні довірчі послуги, в електронній формі:

до Мінцифри – через програмний інтерфейс центрального засвідчувального органу;

до засвідчувального центру – на електронну поштову скриньку Національного банку nbu@bank.gov.ua або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку.

29. Після вжиття вичерпних заходів для забезпечення ідентифікації та перевірки обсягу цивільної правоздатності та дієздатності представника юридичної особи або фізичної особи – підприємця, що має намір надавати кваліфіковані електронні довірчі послуги, центральний засвідчувальний орган/засвідчувальний центр розглядає заяву про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що до неї додаються, і за результатами їх розгляду приймає рішення в порядку та у строки, що встановлені Законом.

30. Перелік електронних довірчих послуг та кваліфікованих електронних довірчих послуг визначено частинами другою та третьою статті 16 Закону.

Кожна послуга, що входить до складу електронних довірчих послуг/кваліфікованих електронних довірчих послуг може надаватися надавачем окремо або в сукупності.

31. Електронні довірчі послуги надаються користувачам електронних довірчих послуг з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI TR 119 400:2017 (ETSI TR 119 400:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів провайдерами довірчих послуг, які підтримують цифрові підписи та пов’язані з ними послуги”.

ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.

ДСТУ ETSI TR 119 100:2017 (ETSI TR 119 100:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів для створення та валідації підпису”.

32. Ідентифікація заявника та перевірка обсягу його цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону та у відповідності до ДСТУ ETSI EN 319 411-1:2022 (ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021–05), IDT Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги, а також-ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021–11), IDT) Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС», Порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг, затвердженого цією постановою.

33. Реєстрація користувачів може здійснюватися через відокремлені пункти реєстрації з дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг, а для кваліфікованих надавачів з дотриманням вимог Регламенту.

34. Кваліфікований надавач повинен забезпечити створення можливості для ознайомлення заявників з інформацією про умови отримання кваліфікованої електронної довірчої послуги.

35. На своєму веб-сайті кваліфіковані надавачі повинні забезпечити публікацію такої інформації:

1) відомості про кваліфікованого надавача;

2) дані про внесення відомостей про кваліфікованого надавача до Довірчого списку;

3) кваліфіковані сертифікати відкритих ключів кваліфікованого надавача;

4) перелік кваліфікованих електронних довірчих послуг, які надає кваліфікований надавач;

5) дані про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;

6) форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;

7) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

8) відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів користувачами;

9) дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;

10) перелік актів законодавства у сфері електронних довірчих послуг.

Кваліфікований надавач забезпечує інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг, зокрема шляхом розміщення відповідної інформації на веб-сайті кваліфікованого надавача.

Інформація на веб-сайті кваліфікованого надавача повинна бути доступною для осіб з інвалідністю.

36. Кваліфікований надавач забезпечує вільний доступ до своїх приміщень, в яких здійснюється обслуговування користувачів, у тому числі створення належних умов для доступу до приміщень маломобільних груп населення.

Інформація про умови доступності таких приміщень для осіб з інвалідністю розміщується у місці, доступному для сприйняття користувачів.

37. Кваліфікований надавач зобов’язаний щороку до 15 січня подавати до Адміністрації Держспецзв’язку звіт про діяльність за попередній рік, що містить відомості про:

1) кількість укладених договорів про надання електронних довірчих послуг (окремо з фізичними та юридичними особами);

2) кількість сформованих та скасованих кваліфікованих сертифікатів відкритих ключів за звітний період із зазначенням причин скасування (у разі коли кваліфікований надавач забезпечує надання кваліфікованих електронних довірчих послуг, які передбачають обслуговування кваліфікованих сертифікатів відкритих ключів);

3) факти відшкодування шкоди користувачам електронних довірчих послуг та/або третім особам внаслідок неналежного виконання надавачем своїх зобов’язань (у разі наявності);

4) факти участі кваліфікованого надавача як позивача, відповідача або третьої сторони у судових справах з питань надання електронних довірчих послуг, предмет розгляду та прийняте рішення (у разі наявності);

5) факти порушення кваліфікованим надавачем вимог законодавства у сфері захисту інформації під час надання електронних довірчих послуг, їх причини та заходи, вжиті для усунення таких порушень.

38. Центральний засвідчувальний орган/засвідчувальний центр надає кваліфіковані електронні довірчі послуги кваліфікованим надавачам відповідно до регламенту роботи центрального засвідчувального органу/Регламенту роботи засвідчувального центру, цих вимог та з урахуванням положень, передбачених Законом.

39. Центральний засвідчувальний орган оприлюднює рішення про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку на своєму офіційному веб-сайті, а також повідомляє про його прийняття представникові юридичної особи або фізичній особі – підприємцю, що має намір надавати кваліфіковані електронні довірчі послуги, з використанням засобів поштового зв'язку або в електронній формі через програмний інтерфейс центрального засвідчувального органу протягом трьох робочих днів з дня його прийняття.

Засвідчувальний центр оприлюднює інформацію про прийняте рішення щодо внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку на своєму офіційному веб-сайті, а також повідомляє про прийняте рішення юридичну особу або фізичну особу – підприємця шляхом надсилання листа на електронну поштову скриньку, вказану у Заяві про внесення до Довірчого списку, або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку протягом трьох робочих днів з дня його прийняття.

40. Кваліфікований надавач у разі виникнення підстав, передбачених Законом для внесення змін відомостей про нього до Довірчого списку, зобов'язаний протягом п'яти робочих днів із дня настання таких підстав подати до органу, який приймав рішення про внесення відомостей про нього до Довірчого списку:

1) заяву про внесення змін до Довірчого списку разом з документами, що підтверджують відповідні зміни;

2) документи для формування кваліфікованих сертифікатів ключів кваліфікованого надавача (окремо для кожної кваліфікованої електронної довірчої послуги) відповідно до вимог Регламенту органу, який приймав рішення про внесення відомостей про нього до Довірчого списку, якщо зміни відомостей, що містяться в Довірчому списку про цього кваліфікованого надавача, пов'язані з формуванням нових сертифікатів ключів кваліфікованого надавача.

41. Кваліфікований надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг з підстав та в порядку, що визначені статтею 31 Закону.

42. Кваліфікований надавач, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, передає обслуговування користувачів електронних довірчих послуг з якими він уклав договори про надання кваліфікованих електронних довірчих послуг, а також документовану

інформацію про цих користувачів до іншого кваліфікованого надавача у порядку відповідно до частини шостої статті 31 Закону.

43. Кваліфіковані сертифікати відкритих ключів, що формуються кваліфікованими надавачами, центральним засвідчувальним органом, засвідчувальним центром під час надання кваліфікованих електронних довірчих послуг, повинні відповідати вимогам, установленим частинами першою – п’ятою статті 23 Закону, а також здійснюватися з дотриманням стандартів визначених пунктом 5 цих вимог та ДСТУ ETSI EN 319 412-5:2022 (ETSI EN 319 412-5 V2.3.1 (2020-04), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Розширення сертифікатів QCStatements”.

44. Кваліфікований надавач, центральний засвідчувальний орган, засвідчувальний центр який видав кваліфікований сертифікат відкритого ключа, забезпечує доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа через комунікаційні мережі загального користування.

45. Час, що використовується надавачем в інформаційно-комунікаційній системі надавача в процесі надання електронних довірчих послуг та в журналах аудиту подій в електронній формі повинен бути синхронізований із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA) з точністю до секунди.

Для кваліфікованих надавачів, відомості про яких вносяться до Довірчого списку за рішенням центрального засвідчувального органу, послуги з постачання передачі сигналів точного часу, синхронізованого із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA) надаються центральним засвідчувальним органом.

Вимоги до синхронізації часу у програмно-технічних комплексах кваліфікованих надавачів, зазначених в абзаці першому частини першої статті 9 Закону, встановлюються Національним банком.

46. Механізм синхронізації часу із Всесвітнім координованим часом (UTC) в програмно-технічному комплексі надавача та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA), що розробляється надавачем.

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA) кваліфікованого надавача, відомості про якого вносяться до Довірчого списку за рішенням центрального засвідчувального органу погоджується з Мінцифри.

Вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання

47. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печаток включає вчинення дій, передбачених частиною першою статті 18 Закону, а також здійснюється з дотриманням таких стандартів:

ДСТУ ETSI TR 119 000:2017 (ETSI TR 119 000:2016, IDT) “Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Огляд”.

ДСТУ ETSI TS 119 101:2016 (ETSI TS 119 101:2016, IDT) “Електронні підписи та інфраструктури. Вимоги та політики безпеки для додатків формування та перевірки підписів”.

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”.

ДСТУ ETSI TS 119 172-4:2021 (ETSI TS 119 172-4 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 4. Правила застосування підписів (політика перевірки) для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків”.

ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”.

48. Під час надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих електронних підписів чи печаток кваліфікованим надавачем забезпечується:

1) використання підписувачем або створювачем електронної печатки виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката електронного підпису чи печатки;

2) захист обміну інформацією між підписувачем або створювачем електронної печатки та кваліфікованим надавачем засобами електронних комунікаційних мереж загального користування;

3) створення умов для генерації пари ключів підписувача або створювача електронної печатки;

4) допомога під час генерації пари ключів підписувача або створювача електронної печатки у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

5) унікальність пари ключів підписувача або створювача електронної печатки;

6) зберігання особистого ключа підписувача або створювача електронної печатки у засобі кваліфікованого електронного підпису чи печатки;

7) захист від доступу сторонніх осіб до параметрів особистого ключа підписувача або створювача електронної печатки під час використання засобу кваліфікованого електронного підпису чи печатки.

49. У разі коли пара ключів була згенерована заявником поза приміщенням надавача та/або за відсутності відповідного персоналу, ідентифікація такого заявника, перевірка обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката відкритого ключа здійснюється кваліфікованим надавачем після перевірки факту володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа.

Перевірка факту володіння заявником особистим ключем здійснюється без розкриття його особистого ключа.

50. Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно кваліфікований надавач.

51. Кваліфікований надавач, який здійснює управління парою ключів підписувача або створювача електронної печатки, може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання за умови дотримання таких вимог:

1) рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;

2) кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

52. Кваліфікований електронний підпис чи печатка повинні відповідати таким вимогам:

1) бути однозначно пов’язаним (пов’язаною) з підписувачем або створювачем електронної печатки;

2) надавати можливість здійснити електронну ідентифікацію підписувача або створювача електронної печатки;

3) створюватися з використанням засобу кваліфікованого електронного підпису чи печатки,

4) базуватися на кваліфікованому сертифікаті відкритого ключа;

5) бути пов’язаним (пов’язаною) з електронними даними, на які накладено кваліфікований електронний підпис чи печатку, таким чином, щоб будь-яка наступна зміна таких даних могла бути виявлена.

53. Перевірка кваліфікованого електронного підпису чи печатки проводиться будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого електронного підпису чи печатки.

54. У процесі перевірки кваліфікованого електронного підпису чи печатки підтвердження таких підпису чи печатки здійснюється за умови дотримання вимог, визначених у частині другій статті 18 Закону та у пункті 52 цих вимог, на момент накладення підпису чи печатки на пов’язані електронні дані;

55. Надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток передбачає, що така послуга:

1) надається виключно кваліфікованим надавачем;

2) відповідає всім вимогам до перевірки кваліфікованих електронних підписів чи печаток, визначеним у пункті 54 цих вимог;

3) дає змогу отримувати результати перевірки із застосуванням щонайменше удосконаленого електронного підпису чи печатки надавача автоматизованим способом, який є надійним, ефективним та захищеним.

56. Державний нагляд (контроль) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг здійснює контролюючий орган.

Функції контролюючого органу виконує Державна служба спеціального зв’язку та захисту інформації України.

Контролюючий орган здійснює виїзні та невиїзні заходи державного нагляду (контролю).

Контролюючий орган може подати запит до органу з оцінки відповідності про надання аудиторського звіту щодо проведення процедури оцінки відповідності відповідно до вимог статті 32 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

57. Контролюючий орган здійснює позапланові заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг у випадках, визначених частиною третьою статті 33^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

У разі негативних результатів оцінки відповідності та/або наданих органом з оцінки відповідності рекомендацій контролюючий орган вживає заходи, передбачені частиною першою статті 33^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

58. Невиїзні заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та/або електронних довірчих послуг контролюючий орган здійснює відповідно до статті 34^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

59. Предметом перевірки надавача, центрального засвідчувального органу або засвідчувального центру є стан дотримання ними вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг.

Організація проведення перевірки контролюючим органом та оформлення її результатів здійснюються відповідно до статей 34^2 -34^7 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

60. Контролюючий орган за результатами проведення перевірок надавачів, засвідчувального центру, центрального засвідчувального органу вживає заходів реагування, передбачених статтями 33^2, 34^8-34^{10} Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

61. Контролюючий орган на підставах і в порядку, встановлених законами та міжнародними договорами України, у межах своїх повноважень співпрацює з уповноваженими органами іноземних держав, надає їм допомогу та звертається до них за отриманням допомоги з питань нагляду і контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг.

Вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання

62. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає вчинення дій, передбачених частиною першою статті 20 Закону, а також здійснюється з дотриманням таких стандартів:

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”;

ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”.

63. Формування кваліфікованого сертифіката електронного підпису чи печатки заявника може здійснюватися кваліфікованим надавачем на основі ідентифікаційних даних особи отриманих з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів за зверненнями громадян), Державного реєстру фізичних осіб – платників податків, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України “Про публічні електронні реєстри”, отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації відповідно до частини першої статті 13 Закону.

64. У разі зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, користувач електронних довірчих послуг протягом трьох робочих днів з дня настання таких змін повідомляє про це кваліфікованого надавача.

На підставі наданих користувачем електронних довірчих послуг документів, що підтверджують зміни відомостей, які містяться у кваліфікованому сертифікаті електронного підпису чи печатки, кваліфікований надавач здійснює повторне формування такого сертифіката та його публікацію у разі згоди користувача електронних довірчих послуг.

Повторне формування кваліфікованого сертифіката електронного підпису чи печатки користувача електронних довірчих послуг не продовжує строку його дії.

65. Сформований кваліфікований сертифікат електронного підпису чи печатки користувача електронних довірчих послуг скасовується або блокується кваліфікованим надавачем у разі наявності підстав, передбачених статтею 25 Закону.

Під час опрацювання заяви про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки кваліфікованим надавачем здійснюється ідентифікація та перевірка обсягу цивільної правоздатності і дієздатності користувача електронних довірчих послуг з дотриманням вимог щодо підтвердження особи, встановлених у Регламенті.

66. Кваліфікований сертифікат електронного підпису чи печатки користувача електронних довірчих послуг вважається скасованим або заблокованим з моменту зміни надавачем статусу кваліфікованого сертифіката електронного підпису чи печатки користувача електронних довірчих послуг на скасований або заблокований.

67. Користувач електронних довірчих послуг, статус кваліфікованого сертифіката електронного підпису чи печатки якого було змінено на скасований чи заблокований, повинен невідкладно бути поінформований про відповідну зміну статусу.

68. Скасований кваліфікований сертифікат електронного підпису чи печатки поновленню не підлягає.

69. Відомості про кваліфіковані сертифікати електронного підпису чи печатки, сформовані кваліфікованим надавачем, їх статус та списки відкликаних сертифікатів відкритих ключів містяться у реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів.

70. Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів електронних довірчих послуг здійснюється шляхом публікації повного та часткового списків відкликаних сертифікатів відкритих ключів на веб-сайті кваліфікованого надавача та забезпечення створення можливості перевірки статусу кваліфікованого

сертифіката електронного підпису чи печатки користувача електронних довірчих послуг в режимі реального часу через електронні комунікаційні мережі загального користування.

Список відкликаних сертифікатів відкритих ключів надавача повинен відповідати таким вимогам:

у кожному списку відкликаних сертифікатів відкритих ключів зазначається строк його дії до видання нового списку, якщо інше не передбачено Регламентом;

новий список відкликаних сертифікатів відкритих ключів може бути опубліковано до закінчення строку його дії та видання наступного списку;

на список відкликаних сертифікатів відкритих ключів повинен бути накладений кваліфікований електронний підпис чи печатка кваліфікованого надавача.

71. Управління статусом кваліфікованого сертифіката електронного підпису чи печатки та поширення відповідної інформації повинні бути доступні для користувача електронних довірчих послуг цілодобово.

72. Заява про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки фіксується та зберігається кваліфікованим надавачем протягом строку, визначеного законодавством у сфері архівної справи для зберігання документованої інформації.

73. Кваліфікований надавач повинен забезпечити цілісність та походження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки.

74. Формування кваліфікованого сертифіката електронного підпису чи печатки здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг.

75. Кваліфіковані надавачі отримують кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки від центрального засвідчувального органу.

Кваліфіковані надавачі, що вносяться до Довірчого списку за поданням засвідчувального центру, отримують кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки від засвідчувального центру.

76. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту, а також порядок перевірки їх дотримання

77. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту включає вчинення дій, передбачених частиною першою статті 21 Закону, та з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”.

ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”.

ДСТУ ETSI EN 319 412-4:2022 (ETSI EN 319 412-4 V1.2.1 (2021-11), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів вебсайтів”.

78. Формування кваліфікованого сертифіката автентифікації веб-сайту здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг.

79. Кваліфікований сертифікат автентифікації веб-сайту забезпечує:

1) автентифікацію власника веб-сайту;

2) гарантування:

шифрування інформації, обмін якою здійснюється через мережу Інтернет учасником онлайн-операції та веб-сайтом;

належного рівня довіри до власника веб-сайту щодо захисту від шахрайства в мережі Інтернеті;

захисту особистої інформації та персональних даних учасника онлайн-операції під час проведення такої операції.

80. Перевірка кваліфікованого сертифіката автентифікації веб-сайту може проводитися будь-якою особою з метою отримання інформації про власника веб-сайту та чинності кваліфікованого сертифіката автентифікації веб-сайту.

81. Під час перевірки кваліфікованого сертифіката автентифікації веб-сайту особа, що проводить перевірку, вчиняє такі дії:

1) отримує з кваліфікованого сертифіката автентифікації веб-сайту інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити власника веб-сайту та кваліфікованого надавача;

2) перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфікований сертифікат автентифікації веб-сайту, за допомогою чинного (на момент формування кваліфікованого сертифіката автентифікації веб-сайту) кваліфікованого сертифіката відкритого ключа надавача.

82. Кваліфікований сертифікат автентифікації веб-сайту вважається чинним у разі відповідності вимогам, установленим частиною першою статті 24 Закону.

83. Кваліфіковані надавачі отримують кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту від центрального засвідчувального органу.

84. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Особливості створення електронного підпису та електронної печатки іншого призначення

85. Кваліфіковані надавачі можуть формувати та видавати кваліфіковані сертифікати відкритого ключа іншого призначення, ніж для автентифікації веб-сайту, створення електронного підпису та електронної печатки.

86. У запиті на формування кваліфікованих сертифікатів відкритого ключа іншого призначення користувач електронних довірчих послуг вказує призначення такого ключа.

87. Процедура формування, блокування та скасування кваліфікованих сертифікатів відкритого ключа іншого призначення така ж як і для сертифікатів електронного підпису та електронної печатки.

Вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання

88. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає вчинення дій, передбачених частиною першою статті 26 Закону, та з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.

ДСТУ ETSI EN 319 421:2016 (ETSI EN 319 421:2016, IDT) “Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі”.

ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT) “Електронні підписи та інфраструктури. Протокол мітки часу та профілі токенів мітки часу”.

89. Перевірка кваліфікованої електронної позначки часу може проводитися будь-якою особою з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

90. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження кваліфікованої електронної позначки часу здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Вимоги до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки, а також порядок перевірки їх дотримання

91. Кваліфікована електронна довірча послуга реєстрованої електронної доставки повинна відповідати вимогам, передбаченим частиною першою статті 27 Закону, та з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI EN 319 521:2019 (ETSI EN 319 521 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для зареєстрованих постачальників послуг електронної пошти”.

ДСТУ ETSI EN 319 522-1:2018 (ETSI EN 319 522-1:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 1. Модель та архітектура”.

ДСТУ ETSI EN 319 522-2:2018 (ETSI EN 319 522-2:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 2. Семантика вмісту”.

ДСТУ ETSI EN 319 522-3:2018 (ETSI EN 319 522-3:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 3. Формати”.

92. Кваліфікована електронна довірча послуга реєстрованої електронної доставки повинна та включати такі дії:

1) відправку електронних даних із забезпеченням доказів відправки;

2) отримання електронних даних із забезпеченням доказів отримання.

93. Реєстрована електронна доставка здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг (відправника та/або отримувача електронних даних).

94. Перевірка електронних даних, що передаються в процесі реєстрованої електронної доставки, проводиться отримувачем електронних даних.

95. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Вимоги до надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, а також порядок перевірки їх дотримання

96. Кваліфікована електронна довірча послуга із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, повинна надаватись з дотриманням положень статті 28 Закону та стандартів ДСТУ ETSI TS 119 511:2019 (ETSI TS 119 511 V1.1.1 (2019-06), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг, що забезпечують тривале збереження цифрових підписів чи загальних даних, використовуючи методи цифрового підпису" та ДСТУ ETSI TS 119 512:2021 (ETSI TS 119 512 V1.1.2 (2020-10), IDT) "Електронні підписи та інфраструктури (ESI). Протоколи для постачальників довірчих послуг, що надають послуги довгострокового зберігання даних".

97. Зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг.

98. Під час надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів забезпечується:

1) цілісність всіх збережених об'єктів даних;

2) протоколювання подій на предмет зміни, видалення або додавання об'єктів даних;

3) покладення відповідальності за їх зберігання на одну чи декілька посадових осіб;

4) проведення перевірок дотримання зазначених вимог.

99. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Перелік змін у наданні кваліфікованих електронних довірчих послуг, про які кваліфіковані надавачі зобов'язані поінформувати контролюючий орган та центральний засвідчувальний орган або засвідчувальний центр

100. Кваліфіковані надавачі зобов'язані поінформувати контролюючий орган та центральний засвідчувальний орган або засвідчувальний центр, в тому числі, але не виключно у зв'язку із введенням надзвичайного стану, воєнного стану чи виникненням іншої надзвичайної ситуації, протягом 48 годин з моменту настання таких обставин в своїй діяльності:

1) припинення надання однієї чи декількох кваліфікованих електронних довірчих послуг, відомості про які внесені до Довірчого списку;

2) змін в складі інформаційно-комунікаційної системи кваліфікованого надавача, які відбулися з порушенням вимог документа про відповідність Надавача, отриманого за результатами проходження процедури оцінки відповідності у сфері електронних довірчих послуг;

3) отримання атестату відповідності комплексної системи захисту інформації інформаційно-комунікаційної системи, що діє протягом визначеного в ньому строку дії, але не більше п'яти років з дня набрання чинності Законом;

4) проходження додаткової державної експертизи комплексної системи захисту інформації, що діє протягом визначеного в ньому строку дії, але не більше п'яти років з дня набрання чинності Законом або процедури оцінки відповідності інформаційно-комунікаційної системи кваліфікованого надавача у разі модернізації апаратного, апаратно-програмного пристрою чи програмного забезпечення, що входять до складу програмно-технічного комплексу, яка не передбачена проектною чи експлуатаційною документацією до комплексної системи захисту інформації інформаційно-комунікаційної системи кваліфікованого надавача;

5) змін щодо способів ідентифікації особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа;

6) змін щодо процедури формування, блокування, скасування, поновлення кваліфікованих сертифікатів відкритих ключів користувачів електронних довірчих послуг;

7) змін щодо процедури надання інформації про статус кваліфікованих сертифікатів відкритих ключів користувачів електронних довірчих послуг;

8) змін щодо умови використання засобів кваліфікованого електронного підпису чи печатки;

9) укладення договору страхування відповідальності або поповнення/списання коштів на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів, або рахунку у Національному банку – для банків – кваліфікованих надавачів, кваліфікованого надавача, створеного Національним банком) для забезпечення відшкодування збитків, які

можуть бути заподіяні кваліфікованим надавачем користувачам електронних довірчих послуг внаслідок неналежного виконання своїх обов’язків.

101. Інформування контролюючого органу та центрального засвідчувального органу або засвідчувального центру про настання змін в діяльності кваліфікованого надавача здійснюється в паперовій або в електронній формі.

Вимоги з безпеки та захисту інформації надавачів та надавачів ідентифікації

102. Діяльність з безпеки та захисту інформації надавачів та надавачів ідентифікації (відокремлених пунктів реєстрації) організовується, постійно підтримується та координується службою захисту інформації з дотриманням вимог законодавства у сфері захисту інформації, електронної ідентифікації та електронних довірчих послуг, Регламенту, а також з дотриманням вимог таких стандартів:

ДСТУ EN 419211-1:2016 (EN 419211-1:2014, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 1. Огляд”.

ДСТУ EN 419211-2:2016 (EN 419211-2:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 2. Пристрій з генерацією ключів”.

ДСТУ EN 419211-3:2016 (EN 419211-3:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 3. Пристрій з імпортом ключів”.

ДСТУ EN 419211-4:2016 (EN 419211-4:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 4. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування генерації сертифікатів”.

ДСТУ EN 419211-5:2016 (EN 419211-5:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 5. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування створення підпису”.

ДСТУ EN 419211-6:2016 (EN 419211-6:2014, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 6. Розширення для пристроїв з імпортом ключів та довіреним каналом для застосування створення підпису”.

ДСТУ ISO/IEC 19790:2015 (ISO/IEC 19790:2012, IDT) “Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів”.

ДСТУ EN 419221-5:2018 (EN 419221-5:2018, IDT) “Профілі захисту для криптографічних модулів TSP. Частина 5. Криптографічний модуль для довірчих послуг”.

ДСТУ CEN/TS 419221-6:2021 (CEN/TS 419221-6:2019, IDT) “Умови застосування EN 419221-5 як кваліфікованого пристрою для створення електронного підпису або печатки”.

ДСТУ EN 419231:2021 (EN 419231:2019, IDT) “Профіль захисту для надійних систем, що підтримують відмітку часу”.

ДСТУ EN 419241-1:2021 (EN 419241-1:2018, IDT) “Надійні системи, що підтримують підписи серверів. Частина 1. Загальні вимоги щодо безпеки системи”.

ДСТУ EN 419241-2:2021 (EN 419241-2:2019, IDT) “Надійні системи, що підтримують підписи серверів. Частина 2. Профіль захисту для QSCD для підписів серверів”.

ДСТУ ETSI TS 119 431-1:2022 (ETSI TS 119 431-1 V1.2.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 1. Компоненти сервісу TSP, що працюють віддаленим QSCD/SCDev”.

ДСТУ ETSI TS 119 431-2:2019 (ETSI TS 119 431-2 V1.1.1 (2018-12), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 2. Компоненти сервісу TSP, що підтримують створення цифрового підпису AdES”.

ДСТУ ETSI TS 119 432-2:2022 (ETSI TS 119 432 V1.2.1 (2020-10), IDT) “Електронні підписи та інфраструктури (ESI). Протоколи віддаленого створення цифрового підпису”.

ДСТУ ETSI TS 119 495:2022 (ETSI TS 119 495 V1.5.1 (2021-04), IDT) “Електронні підписи та інфраструктури (ESI). Секторальні специфічні вимоги. Профілі сертифікатів і вимоги політики TSP для відкритого банківського обслуговування”.

ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”.

ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”.

ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”.

ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”.

ДСТУ ETSI TR 103 570:2022 (ETSI TR 103 570 V1.1.1 (2017-10), IDT) “Кібербезпека. Квантово-безпечний обмін ключами”.

ДСТУ ETSI TR 103 616:2022 (ETSI TR 103 616 V1.1.1 (2021-09), IDT) “Кібербезпека. Квантово-безпечні підписи”.

ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021-10), IDT) “Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів”.

ДСТУ ETSI TR 119 300:2016 (ETSI TR 119 300:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для криптографічних комплектів”.

ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”.

ДСТУ ISO/IEC 14888-1:2015 (ISO/IEC 14888-1:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення”.

ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі дискретного логарифмування”.

ДСТУ ISO/IEC 18032:2022 (ISO/IEC 18032:2020, IDT) “Інформаційні технології. Методи захисту. Генерування простого числа”.

ДСТУ ISO/IEC 18033-6:2022 (ISO/IEC 18033-6:2019, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 6. Гомоморфне шифрування”.

ДСТУ ISO/IEC 19772:2022 (ISO/IEC 19772:2020, IDT) “Інформаційна безпека. Автентифіковане шифрування”.

ДСТУ ISO/IEC 18045:2015 (ISO/IEC 18045:2008, IDT) “Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ”.

ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель”.

ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки”.

ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення”.

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”.

ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”.

ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) “Методи безпеки. Розширення до ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови”.

ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”.

103. Інформаційно-комунікаційні системи кваліфікованих надавачів та надавачів ідентифікації, що використовуються ними під час надання послуг електронної ідентифікації та електронних довірчих послуг повинні відповідати вимогам із захисту інформації шляхом впровадження комплексної системи захисту інформації або системи управління інформаційною безпекою з підтвердженою відповідністю з дотриманням вимог законодавства у сфері захисту інформації та цього розділу.

104. Надання кваліфікованих електронних довірчих послуг та здійснення реєстрації користувачів без чинних документів, що підтверджують відповідність комплексної системи захисту інформації або системи управління інформаційною безпекою з підтвердженою відповідністю, вимогам законодавства у сфері захисту інформації, забороняється.

105. Використання у засобах кваліфікованого електронного підпису криптографічних алгоритмів, визначених стандартами ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”; ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”; ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”; ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”, здійснюється у спосіб, встановлений ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”, шляхом вибору криптографічних параметрів відповідно до вимог до створення та перевірки удосконалених електронних підписів, що базуються на кваліфікованих сертифікатах відкритих ключів, затверджених відповідно до частини третьої статті 17^1 Закону.
