

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ 2024 р. № _____

Порядок проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг

1. Цей Порядок визначає механізм оцінки відповідності надавачів послуг електронної ідентифікації, кваліфікованих надавачів електронних довірчих послуг, центрального засвідчувального органу, засвідчувального центру та послуг, які вони надають, вимогам до надавачів послуг електронної ідентифікації, кваліфікованих надавачів електронних довірчих послуг, а також вимогам до послуг, які вони надають.

2. Дія цього Порядку не поширюються на:

іноземні органи з оцінки відповідності, акредитовані відповідно іноземними органами з акредитації, що є підписантами багатосторонньої угоди про визнання Міжнародного форуму з акредитації та/або Європейської кооперації з акредитації (EA MLA);

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”.

3. У цьому Порядку терміни вживаються у такому значенні:

замовник процедури оцінки відповідності – юридична особа, фізична особа – підприємець, яка має намір надавати послуги електронної ідентифікації, надавач послуг електронної ідентифікації, а також юридична особа, фізична особа – підприємець, яка має намір надавати кваліфіковані електронні довірчі послуги, кваліфікований надавач електронних довірчих послуг, центральний засвідчувальний орган, засвідчувальний центр;

об’єкт оцінки відповідності – юридична особа, фізична особа – підприємець, яка має намір надавати кваліфіковані електронні довірчі послуги, послуги електронної ідентифікації, надавач послуг електронної ідентифікації, кваліфікований надавач електронних довірчих послуг, центральний засвідчувальний орган або засвідчувальний центр та послуги, які вони надають, засоби кваліфікованого електронного підпису чи печатки, які будуть використовуватися або використовуються під час надання кваліфікованих електронних довірчих послуг.

Інші терміни, що використовуються в цьому Порядку, вживаються у значенні, наведеному в Законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про захист інформації в інформаційно-комунікаційних системах” та прийнятих відповідно до них нормативно-правових актах.

4. Оцінка відповідності у сферах електронної ідентифікації та електронних довірчих послуг (далі – оцінка відповідності) здійснюється з урахуванням вимог статті 32 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

5. Оцінка відповідності проводиться з метою підтвердження відповідності об’єкта оцінки відповідності вимогам, встановленим статтями 11², 13, 18-21, 26-28, 32 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”(далі – Вимоги).

6. Оцінка відповідності проводиться за рахунок замовника процедури оцінки відповідності.

Зміст договору між замовником процедури оцінки відповідності та органом з оцінки відповідності (далі – Договір) має містити умови щодо вартості робіт з проведення процедури оцінки відповідності Вимогам, строків його виконання та інших істотних умов відповідно до положень цивільного законодавства.

7. Замовник процедури оцінки відповідності може пройти процедуру оцінки відповідності та отримати аудиторський звіт в іноземному органі з оцінки відповідності, акредитованому відповідно іноземними органами з акредитації, що є підписантами багатосторонньої угоди про визнання Міжнародного форуму з акредитації та/або Європейської кооперації з акредитації (EA MLA).

Аудиторський звіт іноземного органу з оцінки відповідності, викладений іноземною мовою, повинен бути перекладений державною мовою. Вірність перекладу або справжність підпису перекладача засвідчується нотаріально.

8. Оцінка відповідності у сферах електронної ідентифікації та електронних довірчих послуг здійснюється органами з оцінки відповідності, акредитованими згідно з ДСТУ EN ISO/IEC 17065:2019 “Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг” (EN ISO/IEC 17065:2012, IDT; ISO/IEC 17065:2012, IDT), або відповідними європейськими чи міжнародними стандартами, на основі яких прийнято такий національний стандарт.

Органи з оцінки відповідності під час проведення оцінки відповідності у сфері електронних довірчих послуг повинні дотримуватися положень, визначених у стандартах 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”, 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”, 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”.

9. Орган з оцінки відповідності оформляє аудиторський звіт за результатами виконання усіх етапів процесу аудиту, визначених у стандартах ДСТУ ETSI EN 319 403-1:2021 та ДСТУ ETSI TS 119 403-2:2021.

10. Видача органом з оцінки відповідності аудиторського звіту замовнику процедури оцінки відповідності здійснюється в строк, визначений у Договорі, зазначеному в пункті 6 цього Порядку.

11. Оцінка відповідності проводиться у два етапи:

перший етап – передбачає проведення оцінки документації, в тому числі планування другого етапу шляхом визначення структури та об’єму послуг, що надаватиме замовник процедури оцінки відповідності;

другий етап – передбачає виїзний плановий або позаплановий захід, що здійснюється за місцезнаходженням замовника процедури оцінки відповідності та передбачає підтвердження результатів аудиторського звіту за результатами першого етапу, завершення аудиту перевірених послуг та погодження органом з оцінки відповідності плану корекційних дій замовника процедури оцінки відповідності (у разі подання замовником процедури оцінки відповідності плану корекційних дій відповідно до пункту 12 цього Порядку).

За результатами кожного з етапів складається відповідний звіт. Під час встановлення інтервалу між першим та другим етапами оцінки відповідності необхідно враховувати потреби замовника процедури оцінки відповідності для вирішення проблемних областей, виявлених під час проведення першого етапу.

Орган з оцінки відповідності після завершення другого етапу повинен у письмовій формі поінформувати замовника процедури оцінки відповідності про всі висновки, описані в аудиторському звіті, із зазначенням їх суттєвого впливу на безпеку та/або здатність надавати кваліфіковані електронні довірчі послуги чи послуги електронної ідентифікації.

Строк видачі органом з оцінки відповідності за результатами проведення оцінки відповідності аудиторського звіту не може бути більшим ніж шість місяців з дня укладення Договору.

12. Якщо замовник процедури оцінки відповідності, який отримав аудиторський звіт з висновком про невідповідність його діяльності Вимогам, виявив намір продовжити процедуру оцінки відповідності, він має у строк не більше 5 робочих днів з моменту отримання відповідного аудиторського звіту подати органу з оцінки відповідності план корекційних дій у письмовій формі шляхом надсилання його поштою за місцезнаходженням органу з оцінки відповідності чи іншим, узгодженим в Договорі способом.

Орган з оцінки відповідності повинен оцінити та погодити план корекційних дій, визначити строк на проведення корекційних дій, а також визначити додаткові завдання оцінки відповідності, які необхідно виконати для підтвердження того, що невідповідності були виправлені, та поінформувати про такі заходи замовника процедури оцінки відповідності у письмовій формі шляхом надсилання поштою за місцезнаходженням замовника процедури оцінки відповідності чи іншим, узгодженим в Договорі способом.

13. При незначній невідповідності, тобто невиконанні вимог, які не мають істотного впливу на безпеку та здатність надавача послуг електронної ідентифікації чи кваліфікованого надавача електронних довірчих послуг, надавати послуги електронної ідентифікації чи кваліфіковані електронні довірчі послуги, орган з оцінки відповідності повинен розглянути корекційні дії, здійснені замовником процедури оцінки відповідності, протягом:

трьох місяців після надання замовнику процедури оцінки відповідності аудиторського звіту з виявленими невідповідностями;

шести місяців після надання замовнику процедури оцінки відповідності аудиторського звіту з виявленими невідповідностями у разі надання замовником процедури оцінки відповідності до органу з оцінки відповідності документального підтвердження, що виконання корекційних дій потребує більш тривалого періоду часу у зв'язку із складністю їх виконання.

14. За результатами проведення оцінки відповідності органом з оцінки відповідності приймається одне з таких рішень:

1) про відповідність об'єкта оцінки відповідності у повному обсязі Вимогам;

2) про невідповідність об'єкта оцінки відповідності Вимогам.

15. У разі прийняття рішення про відповідність об'єкта оцінки відповідності Вимогам орган з оцінки відповідності видає замовнику процедури оцінки відповідності аудиторський звіт з висновками про відповідність.

16. У разі прийняття рішення про невідповідність об'єкта оцінки відповідності Вимогам орган з оцінки відповідності видає замовнику процедури оцінки відповідності аудиторський звіт з висновками про невідповідність з переліком недоліків.

Після усунення недоліків, зазначених в аудиторському звіті, замовник процедури оцінки відповідності на умовах та в строки, визначені в Договорі, може продовжити процедуру оцінки відповідності, у випадку визначеному пунктом 12 цього Порядку, або пройти процедуру оцінки відповідності повторно.

17. Аудиторський звіт повинен містити такі відомості:

1) найменування органу з оцінки відповідності;

2) інформацію про акредитацію органу з оцінки відповідності (дата та номер атестата про акредитацію);

3) прізвище (у разі наявності), власне ім'я, по батькові (у разі наявності) осіб, що проводили оцінку відповідності;

4) період проведення оцінки відповідності;

5) реквізити замовника процедури оцінки відповідності (найменування або прізвище (у разі наявності), власне ім'я та по батькові (у разі наявності), ідентифікаційні дані та контактна інформація);

6) сфера оцінки відповідності (визначений обсяг перевірки об'єкта оцінки відповідності встановленим Вимогам);

7) перелік послуг електронної ідентифікації чи кваліфікованих електронних довірчих послуг, які має намір надавати або надає замовник процедури оцінки відповідності;

8) найменування інформаційно-комунікаційної системи замовника процедури оцінки відповідності;

9) засоби кваліфікованого електронного підпису чи печатки, які будуть використовуватися або використовуються під час надання послуг електронної ідентифікації чи кваліфікованих електронних довірчих послуг;

10) інформацію про Вимоги, національні стандарти та/або технічні специфікації, щодо відповідності яким проводилася процедура оцінка відповідності;

11) висновок щодо відповідності чи невідповідності об'єкта оцінки відповідності Вимогам;

12) строк дії аудиторського звіту.

18. Процедура повторної (позапланової) оцінки відповідності проводиться у разі наявності обставин, визначених у стандартах ДСТУ ETSI EN 319 403-1:2021 та ДСТУ ETSI TS 119 403-2:2021, а також з урахуванням статей 32, 33¹ Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.
