

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ 2023 р. № _____

Порядок

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

1. Цей Порядок визначає механізм оцінки відповідності засобів електронної ідентифікації в контексті схем електронної ідентифікації низькому, середньому або високому рівню довіри, а також вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, які вони надають.

2. Дія цього Порядку не поширюється 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 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, які мають намір надавати послуги електронної ідентифікації, надавач послуг електронної ідентифікації, а також юридична особа, фізична особа – підприємець, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікований надавач електронних довірчих послуг.

об’єкт оцінки відповідності – засоби електронної ідентифікації в контексті схем електронної ідентифікації, а також юридичні особи, фізичні особи – підприємці, які мають намір надавати кваліфіковані електронні довірчі послуги, послуги електронної ідентифікації, надавач послуг електронної ідентифікації, кваліфікований надавач електронних довірчих послуг, інформаційно-комунікаційна система, засоби кваліфікованого електронного підпису чи печатки та кваліфіковані електронні довірчі послуги.

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 Технічному регламенту щодо вимог до засобів електронної ідентифікації в контексті схеми електронної ідентифікації та процедури, що застосовуються для визначення рівня довіри до засобів електронної ідентифікації, затвердженому відповідно до статті 15 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Технічний регламент), а також, вимогам до надавачів послуг електронної ідентифікації, їхніх відокремлених пунктів реєстрації, у тому числі вимогам щодо безпеки та захисту інформації, а також порядку перевірки їх дотримання, порядку інформування контролюючого органу та користувачів послуг електронної ідентифікації; вимогам до надавачів електронних довірчих послуг (у тому числі вимогам з безпеки та захисту інформації та вимогам до працівників надавача електронних довірчих послуг) та їхніх відокремлених пунктів реєстрації, порядку перевірки їх дотримання, які встановлюються відповідно до статей 11², 13 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Вимоги);

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

Вартість робіт з проведення оцінки відповідності визначається на договірних засадах.

Зміст договору між замовником процедури оцінки відповідності та органом з оцінки відповідності має містити умови щодо вартості робіт з проведення процедури оцінки відповідності Технічному регламенту чи 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. Органи з оцінки відповідності та замовники процедури оцінки відповідності під час проведення оцінки відповідності повинні дотримуватися положень, визначених у стандартах ДСТУ ETSI EN 319403-1:2021 (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” та 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” та 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).

Орган з оцінки відповідності перевіряє виконання Технічного регламенту, у тому числі обов’язкових елементів технічних специфікацій та процедур організаційних, методологічних, технічних та технологічних умов використання засобів електронної ідентифікації залежно від рівнів довіри до засобів електронної ідентифікації, чи Вимог за Методикою щодо оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг, визначеною Мінцифри, та дотримання положень, передбаченими 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” та 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”.

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 об’єкт оцінки відповідності;

другий етап – передбачає виїзний плановий або позаплановий захід, що здійснюється за місцезнаходженням об’єкта оцінки відповідності та передбачає підтвердження результатів попереднього аудиторського звіту та завершення аудиту перевірених послуг.

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 повинен інформувати 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.

12. У разі якщо замовник процедури оцінки відповідності виявив намір у продовженні процедури оцінки відповідності він має надати органу з оцінки відповідності план корекційних дій для усунення виявлених невідповідностей.

Орган з оцінки відповідності повинен оцінити корекційні дії та витрати часу на них, а також поінформувати замовника процедури оцінки відповідності про додаткові завдання оцінки відповідності, необхідні для підтвердження того, що невідповідності були виправлені.

13. Корекційні дії 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 кваліфіковані електронні довірчі послуги, повинні бути розглянуті протягом:

трьох місяців після інформування замовника процедури оцінки відповідності про невідповідність аудиторського звіту;

шести місяців після інформування замовника процедури оцінки відповідності про невідповідність аудиторського звіту у разі документального підтвердження органу з оцінки відповідності, що корекційні дії потребують більш тривалого періоду часу у зв'язку з їх складністю.

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 Технічному регламенту чи Вимогам;

2) про невідповідність об'єкта оцінки відповідності Технічному регламенту чи Вимогам.

15. У разі прийняття рішення про відповідність об'єкта оцінки відповідності Технічному регламенту чи 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 Технічному регламенту чи Вимогам орган з оцінки відповідності видає замовнику процедури оцінки відповідності аудиторський звіт з висновками про невідповідність з переліком недоліків.

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, 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, власне ім'я та по батькові, ідентифікаційні дані та контактна інформація);

6) сфера оцінки відповідності;

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;

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

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

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

12) строк дії документа про відповідність.

18. Орган з оцінки відповідності має визначити програму періодичного нагляду і повторної оцінки відповідності, яка включатиме виїзний захід для підтвердження того, що кваліфіковані надавачі електронних довірчих послуг та послуг, які вони надають, продовжують відповідати Технічному регламенту та Вимогам.

19. 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.
