ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 16 травня 2025 р. № 577

ТЕХНІЧНИЙ РЕГЛАМЕНТ
щодо вимог до засобів електронної ідентифікації
в контексті схеми електронної ідентифікації та процедури,
що застосовуються для визначення рівня довіри до
засобів електронної ідентифікації

1. Цей Технічний регламент встановлює вимоги до засобів електронної ідентифікації в контексті схеми електронної ідентифікації залежно від рівнів довіри до засобів електронної ідентифікації та процедури оцінки, що застосовуються для визначення відповідності цих засобів низькому, середньому або високому рівню довіри.

Цей Технічний регламент розроблено на основі Імплементаційного регламенту комісії (ЄС) 2015/1502 від 8 вересня 2015 року про встановлення мінімальних технічних специфікацій та процедур для рівнів надійності засобів електронної ідентифікації відповідно до статті 8(3) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку.

2. У цьому Технічному регламенті терміни вживаються у такому значенні:

адміністратори систем — юридичні особи, фізичні особи — підприємці, що здійснюють технічне та технологічне забезпечення функціонування інформаційно-комунікаційних систем;

вразлива інформація — відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних та/або юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов;

динамічна автентифікація — процес в електронній формі з використанням алгоритмів криптографічного захисту інформації та/або засобів технічного захисту інформації, який здійснюється для підтвердження того, що ідентифікаційні дані перебувають під контролем або у володінні особи, яка змінює свої вхідні параметри з початком кожного сеансу автентифікації;

достовірне джерело — документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи та ідентифікаційні дані, які обробляються в інформаційних ресурсах єдиної інформаційної системи МВС (відомості, що містяться в Єдиному державному демографічному реєстрі, та відомості щодо викрадених (втрачених) документів — за зверненнями), Державного реєстру фізичних

осіб — платників податків, Єдиного державного реєстру юридичних осіб, фізичних осіб — підприємців та громадських формувань, зокрема Державного реєстру актів цивільного стану громадян про державну реєстрацію смерті, а також інших публічних електронних реєстрів відповідно до Закону України “Про публічні електронні реєстри”, та які дають змогу встановити фізичну, юридичну особу або представника юридичної особи;

замовник — фізична особа, у тому числі іноземець та особа без громадянства, фізична особа — підприємець, юридична особа та їх уповноважені представники, що звернулися до надавача послуг електронної ідентифікації для отримання таких послуг;

ключова інформація (криптографічний матеріал) — конкретний стан деяких параметрів криптографічного алгоритму, які забезпечують вибір одного криптографічного перетворення із сукупності усіх можливих для такого криптографічного алгоритму;

система управління інформаційною безпекою — ряд процесів і процедур, призначених для управління прийнятними рівнями ризиків, пов’язаних з інформаційною безпекою;

фактор автентифікації — чинник, який підтверджено як такий, що пов’язаний з особою, яка проходить ідентифікацію (далі — особа).

Інші терміни вживаються у значенні, наведеному в Законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, “Про основні засади забезпечення кібербезпеки України”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про захист персональних даних” та “Про технічні регламенти та оцінку відповідності”.

3. Фактори автентифікації поділяються на такі групи:

на підставі права володіння — чинник автентифікації, коли від особи вимагають пред’явити документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи;

на підставі знання — чинник автентифікації, коли особі необхідно підтвердити знання інформації;

на підставі властивості — чинник автентифікації, коли особі потрібно надати біометричні дані.

4. Засоби електронної ідентифікації повинні відповідати вимогам до рівнів довіри, визначеним у додатку 1.

5. Специфікації та процедури, наведені в додатку 1, мають використовуватися для встановлення відповідності рівнів довіри до засобів

електронної ідентифікації в контексті схеми електронної ідентифікації шляхом встановлення надійності та якості таких елементів:

реєстрація користувачів засобів електронної ідентифікації відповідно до розділу I додатка 1;

управління засобами електронної ідентифікації відповідно до розділу II додатка 1;

автентифікація відповідно до розділу III додатка 1;

управління та організація роботи надавача послуг електронної ідентифікації відповідно до розділу IV додатка 1.

6. Засоби електронної ідентифікації, що можуть використовуватися в контексті схеми електронної ідентифікації, та пов’язані з ними процеси повинні відповідати вимогам таких стандартів в обсязі виконуваних функцій (за призначенням):

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 EN ISO/IEC 29101:2022 (EN ISO/IEC 29101:2021, IDT; ISO/IEC 29101:2018, 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”.

7. У разі коли засоби електронної ідентифікації, що видаються відповідно до схеми електронної ідентифікації, відповідають вимогам,

передбаченим для високого рівня довіри, вважається, що такі засоби відповідають аналогічним вимогам до середнього та низького рівнів довіри.

8. Відповідність засобів електронної ідентифікації, що видаються відповідно до схеми електронної ідентифікації, певному рівню довіри вважається встановленою за умови виконання всіх елементів та дотримання всіх процедур, визначених у додатку 1.

9. Для проведення процедури оцінки відповідності засобів електронної ідентифікації вимогам цього Технічного регламенту застосовується модуль H (відповідність на основі цілковитого забезпечення якості) згідно з постановою Кабінету Міністрів України від 13 січня 2016 р. № 95 “Про затвердження модулів оцінки відповідності, які використовуються для розроблення процедур оцінки відповідності, та правил використання модулів оцінки відповідності” (Офіційний вісник України, 2016 р., № 16, ст. 625).

10. Для перевірки достовірності повноважень щодо представництва юридичної особи її уповноваженим представником (далі — перевірка представництва) на основі ідентифікаційних даних юридичної особи та її уповноваженого представника відповідно до підрозділу 4 розділу I додатка 1 застосовуються такі умови:

встановлення строку дії представництва та припинення представництва здійснюються відповідно до цивільного законодавства;

уповноважений представник юридичної особи, ідентифікаційні дані якого пов’язані з ідентифікаційними даними юридичної особи, яку він представляє, може передати своє повноваження щодо представництва іншій фізичній особі відповідно до цивільного законодавства. При цьому відповідальною за збереження та достовірність ідентифікаційних даних юридичної особи є уповноважений представник юридичної особи, який передає своє повноваження.

11. Таблиця відповідності положень Імплементаційного регламенту комісії (ЄС) 2015/1502 від 8 вересня 2015 року про встановлення мінімальних технічних специфікацій та процедур для рівнів надійності засобів електронної ідентифікації відповідно до статті 8(3) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та цього Технічного регламенту наведена у додатку 2.

_____

Додаток 1
до Технічного регламенту

ТЕХНІЧНІ СПЕЦИФІКАЦІЇ
елементів та процедур до реєстрації користувачів засобів електронної ідентифікації, управління засобами електронної ідентифікації, автентифікації, управління та організації

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
I. Реєстрація користувачів засобів електронної ідентифікації	
1. Подання заявки на реєстрацію засобів електронної ідентифікації	
Низький	1) забезпечення інформування заявника про умови, пов'язані з використанням засобів електронної ідентифікації 2) забезпечення інформування заявника про заходи безпеки, пов'язані з використанням засобів електронної ідентифікації 3) збір відповідних ідентифікаційних даних, необхідних для підтвердження тотожності та ідентифікації заявника
Середній	такі самі, як для низького рівня довіри
Високий	такі самі, як для низького рівня довіри
2. Встановлення заявника, який є фізичною особою або його уповноваженим представником, та підтвердження їх ідентифікаційних даних	
Низький	1) володіння заявником інформацією, яка дає можливість відповідно до законодавства ідентифікувати фізичну особу та особу, яка її представляє 2) існує ймовірність, що ідентифікаційні дані є справжніми або такими, існування яких підтверджено достовірним джерелом 3) з достовірного джерела відомо, що ідентифікаційні дані належать фізичній особі. Існує ймовірність, що заявник і є фізичною особою, яку ідентифікували
Середній	виконання вимог до обов'язкових елементів та процедур низького рівня довіри та додаткове виконання однієї з таких вимог: 1) встановлення заявника як такого, якому належать ідентифікаційні дані, які відповідно до законодавства встановлюють особу, та здійснення перевірки відомостей на їх справжність (або з достовірного джерела відомо, що такі

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
	відомості існують та належать особі, яку ідентифікували), а також вжиття заходів для мінімізації ризиків відсутності тотожності фізичної особи із заявником з урахуванням ризиків втрати, викрадення чи закінчення строку дії документів, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи; 2) пред’явлення під час процедури реєстрації користувачів засобів електронної ідентифікації документа, що посвідчує особу, і встановлення, що такий документ належить особі, яка його пред’являє, та вжиття заходів для мінімізації ризиків відсутності тотожності фізичної особи із заявником з урахуванням ризиків втрати, викрадення чи закінчення строку дії документів, що посвідчують особу; 3) у разі коли процедури, що використовувалися раніше фізичними особами — підприємцями, юридичними особами незалежно від організаційно-правової форми та форми власності для цілей, відмінних від видачі засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у пунктах 1 і 2 підрозділу 2 розділу I для середнього рівня довіри до засобів електронної ідентифікації цього додатка, надавач послуг електронної ідентифікації не виконує повторно попередні процедури за умови, що їх рівноцінну надійність підтверджено органом з оцінки відповідності, акредитованим відповідно до законодавства у сфері акредитації або призначеним відповідно до законодавства про технічні регламенти та оцінку відповідності; 4) у разі коли засоби електронної ідентифікації видаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають середній або високий рівень довіри з урахуванням ризиків зміни ідентифікаційних даних, надавач послуг електронної ідентифікації не виконує повторно попередні процедури. У разі коли засоби електронної ідентифікації не належать до схеми електронної ідентифікації, відповідність таких засобів середньому та високому рівням довіри встановлюється органом з оцінки відповідності, акредитованим відповідно до законодавства у сфері акредитації або призначеним відповідно до законодавства про технічні регламенти та оцінку відповідності

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
Високий	виконання однієї з таких вимог: 1) крім обов’язкових елементів та процедур, які відповідають середньому рівню довіри до засобів електронної ідентифікації, додатково виконується одна з таких вимог: встановлення фізичної особи як такої, якій належать фотографічні зображення або біометричні дані, крім відцифрованих відбитків пальців рук, які відповідно до законодавства ідентифікують особу. Дійсність таких даних перевіряється за допомогою достовірного джерела. Фізичну особу встановлюють шляхом зіставлення біометричних даних, параметрів із даними з достовірного джерела; у разі коли процедури, що використовувалися раніше фізичними особами — підприємцями, юридичними особами незалежно від організаційно-правової форми та форми власності для цілей, відмінних від видачі засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у цьому пункті для високого рівня довіри до засобів електронної ідентифікації, надавач послуг електронної ідентифікації не виконує повторно попередні процедури за умови, що їх рівноцінну надійність підтверджено органом з оцінки відповідності, акредитованим відповідно до законодавства у сфері акредитації або призначеним відповідно до законодавства про технічні регламенти та оцінку відповідності. Додатково вживаються заходи, що дають змогу підтвердити результати процедур встановлення заявника та підтвердження ідентифікаційних даних фізичної особи для низького та середнього рівнів; у разі коли засоби електронної ідентифікації видаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають високий рівень довіри з урахуванням ризиків зміни ідентифікаційних даних, надавач послуг електронної ідентифікації не виконує повторно попередні процедури за умови, що додатково вживаються заходи, які дають змогу підтвердити результати процедур видачі засобів електронної ідентифікації, що належать до схеми електронної ідентифікації 2) у разі коли фізична особа не надає фотографічне зображення або біометричні дані, крім відцифрованих відбитків пальців рук,

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
	які відповідно до законодавства ідентифікують особу, застосовуються процедури отримання таких даних з достовірних джерел
3. Встановлення заявника, який є юридичною особою або його уповноваженим представником, та підтвердження їх ідентифікаційних даних	
Низький	1) встановлення юридичної особи на основі відомостей, які відповідно до законодавства ідентифікують таку особу та уповноваженого представника юридичної особи 2) відомості про юридичну особу є дійсними і можна припустити, що такі відомості є достовірними або такими, існування яких підтверджено достовірним джерелом 3) існує ймовірність, що такі відомості є достовірними або такими, існування яких підтверджено достовірним джерелом 4) у достовірному джерелі відсутні дані про перебування юридичної особи у процесі припинення, у процесі провадження у справі про банкрутство тощо, які б перешкоджали їй діяти як юридичній особі, про яку заявляється
Середній	виконання вимог до обов’язкових елементів та процедур низького рівня довіри та додатково виконання однієї з таких вимог: 1) встановлення юридичної особи на основі відомостей, які відповідно до законодавства ідентифікують таку особу, а також уповноваженого представника юридичної особи, а саме: найменування юридичної особи та ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб — підприємців та громадських формувань, здійснення перевірки відомостей на їх справжність (або з достовірного джерела відомо, що такі відомості існують та належать юридичній особі, яку ідентифікували), якщо внесення відомостей до достовірного джерела здійснено для підтвердження діяльності юридичної особи в межах сфери її діяльності, а також вжито заходів для мінімізації ризиків відсутності тотожності юридичної особи з юридичною особою, яку ідентифікували з урахуванням ризиків втрати або викрадення документів юридичної особи 2) у разі коли процедури, що використовувалися раніше фізичними особами — підприємцями, юридичними особами

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
	незалежно від організаційно-правової форми та форми власності для цілей, відмінних від видачі засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених пунктом 1 підрозділу 3 розділу I для середнього рівня довіри до засобів електронної ідентифікації цього додатка, надавач послуг електронної ідентифікації не виконує повторно попередні процедури за умови, що їх рівноцінну надійність підтверджено органом з оцінки відповідності, акредитованим відповідно до законодавства у сфері акредитації або призначеним відповідно до законодавства про технічні регламенти та оцінку відповідності 3) у разі коли засоби електронної ідентифікації видаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають середній або високий рівень довіри, надавач послуг електронної ідентифікації не виконує повторно попередні процедури. У разі коли засоби електронної ідентифікації не належать до схеми електронної ідентифікації, відповідність таких засобів до середнього та високого рівнів довіри встановлюється органом з оцінки відповідності, акредитованим відповідно до законодавства у сфері акредитації або призначеним відповідно до законодавства про технічні регламенти та оцінку відповідності
Високий	виконання вимог до обов’язкових елементів та процедур середнього рівня довіри та додатково виконання однієї з таких вимог: 1) встановлення юридичної особи на основі відомостей, які відповідно до законодавства ідентифікують таку особу, а також уповноваженого представника юридичної особи, а саме: найменування юридичної особи та ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб — підприємців та громадських формувань, здійснення перевірки відомостей на їх справжність за допомогою достовірного джерела 2) у разі коли процедури, що використовувалися раніше фізичними особами — підприємцями, юридичними особами незалежно від організаційно-правової форми та форми власності для цілей, відмінних від видачі засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
	процедур, визначених у пункті 1 підрозділу 3 розділу I для високого рівня довіри до засобів електронної ідентифікації цього додатка, надавач послуг електронної ідентифікації не повинен повторно виконувати такі процедури за умови, що їх рівноцінну надійність підтверджено органом з оцінки відповідності, акредитованим відповідно до законодавства у сфері акредитації або призначеним відповідно до законодавства про технічні регламенти та оцінку відповідності
	3) у разі коли засоби електронної ідентифікації видаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають високий рівень довіри, надавач послуг електронної ідентифікації не виконує повторно такі процедури. Додатково вживаються заходи, що дають змогу підтвердити результати попередніх процедур видачі засобів електронної ідентифікації, що належать до схеми електронної ідентифікації
4. Перевірка представництва на основі ідентифікаційних даних юридичної особи та її уповноваженого представника	
Низький	1) підтвердження ідентифікаційних даних уповноваженого представника юридичної особи здійснено за процедурами, які відповідають низькому, середньому або високому рівням довіри
	2) перевірка представництва на основі ідентифікаційних даних юридичної особи та її уповноваженого представника відповідно до цивільного законодавства
	3) відсутність у достовірному джерелі відомостей, які не дають права фізичній особі представляти юридичну особу
Середній	виконання вимог, зазначених у пункті 3 підрозділу 4 розділу I для низького рівня довіри до засобів електронної ідентифікації, а також вимог, зазначених у пунктах 1—3 підрозділу 4 розділу I для середнього рівня довіри до засобів електронної ідентифікації цього додатка
	1) підтвердження ідентифікаційних даних уповноваженого представника юридичної особи здійснено за процедурами, які відповідають середньому або високому рівню довіри
	2) перевірка достовірності на основі ідентифікаційних даних юридичної особи та її уповноваженого представника за

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до реєстрації користувачів засобів електронної ідентифікації
	допомогою процедур, визначених законодавством (на основі відомостей, отриманих із достовірного джерела) 3) підтвердження достовірності на основі ідентифікаційних даних уповноваженого представника та юридичної особи, яку представляє такий представник, на основі відомостей, отриманих із достовірного джерела
Високий	виконання вимог, зазначених у пункті 3 підрозділу 4 розділу I для низького рівня довіри до засобів електронної ідентифікації та у пунктах 2 і 3 підрозділу 4 розділу I для середнього рівня довіри до засобів електронної ідентифікації, а також вимог, зазначених у пунктах 1 і 2 підрозділу 4 розділу I для високого рівня довіри до засобів електронної ідентифікації цього додатка 1) підтвердження ідентифікаційних даних уповноваженого представника юридичної особи здійснено за процедурами, які відповідають високому рівню довіри 2) підтвердження зв’язку між ідентифікаційними даними юридичної особи та її уповноваженого представника за допомогою відомостей, отриманих із достовірного джерела, на основі унікального ідентифікатора

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління засобами електронної ідентифікації
	II. Управління засобами електронної ідентифікації
	1. Характеристики засобів електронної ідентифікації та їх використання
Низький	1) засоби електронної ідентифікації використовують щонайменше один із таких факторів автентифікації: на підставі знання; на підставі права володіння; на підставі властивості 2) засоби електронної ідентифікації розроблено для забезпечення технічної можливості надавачам послуг електронної ідентифікації вживати необхідних заходів для перевірки використання таких засобів під контролем або у користуванні особою, якій такі засоби належать
Середній	1) засоби електронної ідентифікації використовують щонайменше два фактори автентифікації, зазначені в пункті 1 підрозділу 1 розділу II для низького рівня довіри до засобів електронної ідентифікації цього додатка 2) засоби електронної ідентифікації розроблено так, щоб можна було припустити, що вони використовуються тільки під контролем особи, якій такі засоби належать
Високий	1) такі самі, як для середнього рівня довіри 2) засоби електронної ідентифікації захищено від дублювання та несанкціонованого доступу з боку порушників з високим потенціалом здійснення нападу 3) засоби електронної ідентифікації розроблено так, що фізична чи юридична особа, якій вони належать, може надійно захистити їх від несанкціонованого використання іншими особами
	2. Видача та активація засобів електронної ідентифікації
Низький	видача засобів електронної ідентифікації фізичній чи юридичній особі, яка їх замовила
Середній	видача засобів електронної ідентифікації особі, якій вони належать
Високий	у процесі активації засобу електронної ідентифікації здійснюється підтвердження видачі засобів електронної ідентифікації особі, якій вони належать

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління засобами електронної ідентифікації
3. Блокування, скасування та поновлення дії засобів електронної ідентифікації	
Низький	1) можливість блокування та/або скасування засобу електронної ідентифікації повинна бути забезпечена вчасно та ефективно 2) впровадження заходів із запобігання несанкціонованому блокуванню, скасуванню та/або поновленню дії засобів електронної ідентифікації 3) поновлення дії засобів електронної ідентифікації здійснюється за умови дотримання вимог, наведених у розділах I і II цього додатка
Середній	такі самі, як для низького рівня довіри
Високий	такі самі, як для низького рівня довіри
4. Поновлення та заміна ідентифікаційних даних користувача засобу електронної ідентифікації	
Низький	процедури поновлення або заміни ідентифікаційних даних користувача засобу електронної ідентифікації здійснюються відповідно до вимог, наведених у розділах I і II цього додатка
Середній	такі самі, як для низького рівня довіри
Високий	1) такі самі, як для низького рівня довіри 2) у разі коли поновлення та заміна ідентифікаційних даних користувача здійснюються з використанням засобу електронної ідентифікації, має бути здійснено ідентифікацію такого користувача з використанням достовірного джерела

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до автентифікації
	III. Автентифікація
	1. Вимоги до механізму автентифікації засобів електронної ідентифікації
Низький	1) перед передачею ідентифікаційних даних до інформаційно-комунікаційних систем здійснюється надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності 2) у разі зберігання ідентифікаційних даних як частини механізму автентифікації здійснюється захист такої інформації від ризику втрати, крадіжки, пошкодження або будь-яких несанкціонованих змін, зокрема захист від ризику втрати, крадіжки, пошкодження або будь-яких несанкціонованих змін у режимі оф-лайн 3) забезпечення механізмом автентифікації впровадження методів контролю безпеки для верифікації засобів електронної ідентифікації, направлених на зниження ймовірності порушення механізму шляхом реалізації атак підбору, перехоплення, повторного відтворення та підміни порушником з низькою ймовірністю здійснення атаки
Середній	1) такі самі, як для низького рівня довіри 2) перед передачею ідентифікаційних даних до інформаційно-комунікаційних систем здійснюється надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності за допомогою динамічної автентифікації 3) забезпечення механізмом автентифікації впровадження методів контролю безпеки для верифікації засобів електронної ідентифікації, направлених на якнайбільше зниження ймовірності порушення механізму шляхом реалізації атак підбору, перехоплення, повторного відтворення та підміни порушником з середньою ймовірністю здійснення атаки
Високий	1) такі самі, як для середнього рівня довіри 2) забезпечення механізмом автентифікації впровадження методів контролю безпеки для верифікації засобів електронної ідентифікації, направлених на якнайбільше зниження ймовірності порушення механізму шляхом реалізації атак підбору, перехоплення, повторного відтворення та підміни порушником з високою ймовірністю здійснення атаки

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління та організації роботи надавача послуг електронної ідентифікації
IV. Управління та організація роботи надавача послуг електронної ідентифікації	
	1. Адміністратори систем
Низький	1) адміністратори систем повинні мати визначену організаційну структуру та провадити діяльність у всіх сферах, пов’язаних з наданням послуг електронної ідентифікації 2) адміністратори систем повинні визначити своїми рішеннями функції витребовувати, перевіряти, обробляти та зберігати ідентифікаційні дані користувачів, отримані під час надання послуг електронної ідентифікації 3) адміністратори систем відповідають за шкоду, завдану користувачам послуг електронної ідентифікації надавачем послуг електронної ідентифікації, що реалізує схему електронної ідентифікації, а також повинні мати фінансові ресурси для продовження діяльності з видачі засобів електронної ідентифікації та експлуатації інформаційно-комунікаційних систем схем електронної ідентифікації 4) адміністратори систем відповідають за виконання функцій, переданих відокремленому пункту реєстрації, та за функціонування схеми електронної ідентифікації 5) адміністратори систем повинні мати план припинення діяльності з надання послуг електронної ідентифікації за схемою, внесеною до переліку схем електронної ідентифікації, який має містити належний порядок припинення обслуговування або продовження обслуговування користувачів іншим адміністратором системи, способи повідомлення відповідних державних органів та кінцевих користувачів, а також детальну інформацію про захист, зберігання, знищення записів відповідно до правил функціонування схеми
Середній	такі самі, як для низького рівня довіри
Високий	такі самі, як для низького рівня довіри

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління та організації роботи надавача послуг електронної ідентифікації
	2. Публікація повідомлень та інформація про надання послуг електронної ідентифікації для користувачів
Низький	1) на веб-сайті надавача послуг електронної ідентифікації повинно бути оприлюднено інформацію щодо процесів та процедур, пов’язаних із видачею та використанням засобів електронної ідентифікації, а також правила, умови експлуатації, обмеження щодо використання таких засобів, відомості про платежі. Також на веб-сайті повинно бути оприлюднено положення щодо захисту персональних даних користувачів послуг електронної ідентифікації відповідно до вимог Закону України “Про захист персональних даних”
	2) у діяльності надавача послуг електронної ідентифікації повинно бути реалізовано своєчасне (та у надійний спосіб) отримання користувачами інформації про будь-які зміни інформації щодо процесів та процедур, пов’язаних із видачею та використанням засобів електронної ідентифікації, правил, умов їх експлуатації
	3) надавач послуг електронної ідентифікації повинен надавати вичерпні відповіді на запити про надання інформації щодо видачі та використання засобів електронної ідентифікації
Середній	такі самі, як для низького рівня довіри
Високий	такі самі, як для низького рівня довіри
	3. Управління інформаційною безпекою
Низький	впровадження системи управління інформаційною безпекою та контролю за ризиками інформаційної безпеки
Середній	1) такі самі, як для низького рівня довіри
	2) впровадження системи управління інформаційною безпекою або комплексна система захисту інформації відповідно до вимог законодавства у сфері захисту інформації з урахуванням вимог національних стандартів щодо систем управління інформаційної безпеки
Високий	такі самі, як для середнього рівня довіри

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління та організації роботи надавача послуг електронної ідентифікації
	4. Зберігання даних
Низький	1) запис та зберігання даних, які обробляються в інформаційно-комунікаційній системі схеми електронної ідентифікації, здійснюються з використанням надійної системи управління записами 2) зберігання даних, які обробляються в інформаційно-комунікаційній системі схеми електронної ідентифікації, здійснюється протягом строків, визначених законодавством у сферах електронних комунікацій, захисту інформації та захисту персональних даних, впродовж яких вони будуть необхідні для аудиту та розслідування порушень вимог безпеки 3) після закінчення строку зберігання дані, які оброблялися в інформаційно-комунікаційній системі схеми електронної ідентифікації, знищуються у спосіб, який забезпечує відсутність можливості відновлення таких даних
Середній	такі самі, як для низького рівня
Високий	такі самі, як для низького рівня
	5. Об’єктовий контроль та вимоги до працівників надавача послуг електронної ідентифікації
Низький	1) визначення адміністратором системи процедур, які забезпечують перевірку наявності у працівників надавача послуг електронної ідентифікації (далі — працівники) належної підготовки, кваліфікації та досвіду, необхідних для виконання ними своїх обов’язків 2) наявність працівників, які забезпечують функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та видачу засобів електронної ідентифікації відповідно до вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28 червня 2024 р. № 764 (Офіційний вісник України, 2024 р., № 63, ст. 3762) 3) будівлі та приміщення, які використовуються для забезпечення функціонування інформаційно-комунікаційної

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління та організації роботи надавача послуг електронної ідентифікації
	системи схеми електронної ідентифікації та видачі засобів електронної ідентифікації, підлягають постійному моніторингу та захисту від пошкоджень, спричинених техногенними катастрофами, несанкціонованим доступом та іншими чинниками, які можуть вплинути на безпеку функціонування 4) у будівлях та приміщеннях, які використовуються для забезпечення функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та видачі засобів електронної ідентифікації, доступ до місць, у яких зберігаються та обробляються персональні дані, ключова інформація (криптографічний матеріал) або інша вразлива інформація надається працівникам відповідно до їх обов’язків адміністратором системи
Середній	такі самі, як для низького рівня довіри
Високий	такі самі, як для низького рівня довіри
	6. Технічний контроль
Низький	1) проведення пропорційного технічного контролю для управління ризиками, які загрожують безпеці обслуговування, захисту конфіденційності, цілісності та доступності інформації, що обробляється в інформаційно-комунікаційній системі 2) захист каналів зв’язку, які використовуються для обміну інформацією, що містить персональні дані, та вразливою інформацією, від несанкціонованого ознайомлення, модифікації та повторного відтворення інформації 3) доступ до ключової інформації (криптографічного матеріалу), якщо така (такий) використовується для видачі засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, обмежено програмами, які вимагають доступу залежно від обов’язків працівників. Забезпечується зберігання такого матеріалу відповідно до законодавства у сферах електронних комунікацій, захисту інформації та захисту персональних даних 4) існують процедури, які забезпечують підтримку цілісності та доступності інформації, що обробляється в

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління та організації роботи надавача послуг електронної ідентифікації
	інформаційно-комунікаційній системі надавача послуг електронної ідентифікації впродовж визначеного строку, і можливість реагувати на зміни рівнів ризику, інциденти та порушення безпеки
	5) усі засоби електронної ідентифікації, до яких внесено інформацію, що містить персональні дані, ключову інформацію (криптографічний матеріал) або іншу вразливу інформацію, зберігаються, передаються та знищуються відповідно до законодавства у сферах електронних комунікацій, захисту інформації та захисту персональних даних
Середній	1) такі самі, як для низького рівня довіри
	2) захист ключової інформації (криптографічного матеріалу), якщо така (такий) використовується для видачі засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, від несанкціонованого доступу та копіювання
Високий	такі самі, як для середнього рівня довіри
7. Аудит на відповідність 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	
Низький	проведення внутрішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-комунікаційної системи схеми електронної ідентифікації
Середній	1) такі самі, як для низького рівня довіри
	2) періодичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-комунікаційної системи схеми електронної ідентифікації
Високий	1) систематичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-комунікаційної системи схеми електронної ідентифікації
	2) проведення заходів державного контролю за станом технічного та криптографічного захисту інформації в

Рівні довіри до засобів електронної ідентифікації	Обов’язкові елементи та процедури до управління та організації роботи надавача послуг електронної ідентифікації
	інформаційно-комунікаційній системі схеми електронної ідентифікації

_____

Додаток 2
до Технічного регламенту

ТАБЛИЦЯ ВІДПОВІДНОСТІ
положень Імплементаційного регламенту комісії (ЄС) 2015/1502 від 8 вересня 2015 року про встановлення мінімальних технічних специфікацій та процедур для рівнів надійності засобів електронної ідентифікації відповідно до статті 8(3) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та Технічного регламенту щодо вимог до засобів електронної ідентифікації в контексті схеми електронної ідентифікації та процедури, що застосовується для визначення рівня довіри до засобів електронної ідентифікації

Положення Імплементаційного регламенту комісії (ЄС) 2015/1502	Положення Технічного регламенту
Пункт 1 статті 1	Пункт 4
Пункт 2 статті 1	Пункт 5
Пункт 3 статті 1	Пункт 7
Пункт 4 статті 1	Пункт 8
Секція 1 Додатка Імплементаційного регламенту комісії (ЄС) 2015/1502	Пункти 2 і 3
Секція 2 Додатка Імплементаційного регламенту комісії (ЄС) 2015/1502	Додаток 1
Секція 2.1 Додатка Імплементаційного регламенту комісії (ЄС) 2015/1502	Розділ I Додатка 1
Секція 2.2 Додатка Імплементаційного регламенту комісії (ЄС) 2015/1502	Розділ II Додатка 1
Секція 2.3 Додатка Імплементаційного регламенту комісії (ЄС) 2015/1502	Розділ III Додатка 1
Секція 2.4 Додатка Імплементаційного регламенту комісії (ЄС) 2015/1502	Розділ IV Додатка 1

_____