



ДЕРЖАВНЕ АГЕНТСТВО З ПИТАНЬ ЕЛЕКТРОННОГО УРЯДУВАННЯ УКРАЇНИ

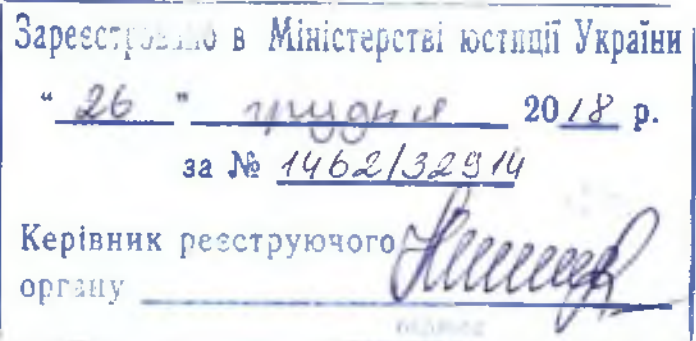
НАКАЗ

27.11.2018

м. Київ

№ 86

Про встановлення Вимог до засобів
електронної ідентифікації, рівнів
довіри до засобів електронної
ідентифікації для їх використання у
сфері електронного урядування



Відповідно до статті 10 Закону України «Про електронні довірчі послуги», пунктів 4, 8, 10 Положення про Державне агентство з питань електронного урядування України, затвердженого постановою Кабінету Міністрів України від 01 жовтня 2014 року № 492,

НАКАЗУЮ:

1. Затвердити Вимоги до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування, що додаються.

2. Генеральному департаменту цифрової трансформації (Маковський Д.В.) забезпечити:

1) подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому законодавством порядку;

2) оприлюднення цього наказу на офіційному веб-сайті Державного агентства з питань електронного урядування України.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Контроль за виконанням цього наказу покласти на першого заступника
Голови Вискуба О.А.

Голова

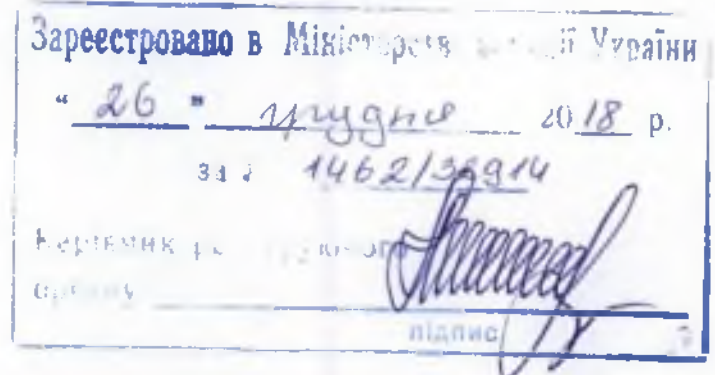
A handwritten signature in blue ink, consisting of a large, stylized capital letter 'R' followed by a horizontal stroke and a small loop at the end.

О. РИЖЕНКО

ЗАТВЕРДЖЕНО

Наказ Державного агентства з
питань електронного урядування
України

27 листопада 2018 року № 86



ВИМОГИ

до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування

1. Загальні положення

1. Ці Вимоги встановлюють організаційні, методологічні, технічні та технологічні умови використання засобів електронної ідентифікації у сфері електронного урядування залежно від рівнів довіри до засобів електронної ідентифікації.

2. Ці Вимоги обов'язкові для виконання надавачами електронних довірчих послуг, підприємствами, установами та організаціями незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями, експертними дослідженнями та експлуатацією засобів електронної ідентифікації, що видаються фізичним, юридичним особам або представникам юридичних осіб, та використовуються для автентифікації у сфері електронного урядування.

3. У цих Вимогах терміни вживаються у таких значеннях:

активація - процес, за допомогою якого обліковий запис або засоби для подання повноважень готові до використання;

атака підбору – процес повторних спроб підбору можливих значень облікових та ідентифікаційних даних зловмисником для виконання входу в систему;

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;

встановлення ідентичності - встановлення параметрів, пов'язаних з особою;

динамічна автентифікація – електронний процес з використанням алгоритмів криптографічного захисту інформації та (або) засобів технічного захисту інформації, який здійснюється для підтвердження того, що ідентифікаційні дані знаходяться під контролем особи або у її володінні, яка змінює свої вхідні параметри з початком кожного сеансу автентифікації;

достовірне джерело ідентифікаційних даних (достовірне джерело) - документи, що посвідчують особу, які оформлені та видані органами державної влади, органами місцевого самоврядування, іншими юридичними особами публічного права відповідно до законодавства, та ідентифікаційні дані, які оброблюються в інформаційних та інформаційно-телекомунікаційних системах, власниками та (або) держателями яких визначено такі органи та особи, та які дозволяють однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

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

компрометація - будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами криптографічного захисту інформації, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається;

компрометація в режимі офлайн – аналітична атака без виконання безпосередньо автентифікації на сервісі. Виконується за допомогою формування словника хеш-значень, що використовуються під час автентифікації;

орган оцінки відповідності - підприємство, установа, організація чи їх підрозділи, які провадять діяльність з оцінки відповідності, включаючи калібрування, випробування, сертифікацію та інспектування;

перевірка ідентичності – процес верифікації унікальних ідентифікаторів та їх прив'язування до особи;

підтвердження ідентичності – процес, за допомогою якого суб'єкт, відповідальний за реєстрацію, фіксує та перевіряє достатню інформацію для визначення особи з встановленим рівнем довіри;

порушник - умовне позначення суб'єкта, який може навмисно чи ненавмисно здійснити несанкціоновані дії щодо інформації в системі;

порушник з базовим потенціалом – порушник, який має обмежені кошти та самостійно створює засоби, розробляє методи атак на засоби криптографічного захисту інформації, а також інформаційно-телекомунікаційні системи із застосуванням поширених програмних засобів та електронно-обчислювальної техніки;

порушник з високим потенціалом – порушник, який має науково-технічний ресурс, що прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави;

порушник з середнім потенціалом – порушник корпоративного типу, який має змогу створення спеціальних технічних засобів, вартість яких співвідноситься з можливими фінансовими збитками, що виникатимуть від порушення конфіденційності, цілісності та підтвердження авторства інформації, зокрема при втраті, спотворенні та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

ризик інформаційної безпеки - наслідки при автентифікації та (або) неправильному використанні повноважень особи, шкода та вплив від таких випадків, а також вірогідність їх виникнення;

система управління записами - довірена сторона, яка створює, встановлює та (або) керує записами;

суб'єкт, відповідальний за встановлення ідентичності, - довірений суб'єкт, який встановлює та (або) підтверджує ідентичність особи для системи управління записами;

унікальний ідентифікатор - один чи декілька параметрів, які однозначно визначають особу і надаються в спеціальному вигляді;

фактор автентифікації – матеріальний або нематеріальний носій, інформація або фізичні ознаки, які однозначно пов'язані з особою.

Інші терміни вживаються у значеннях, наведених у Законах України “Про електронні довірчі послуги”, “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, у національному стандарті ДСТУ ISO/IEC 29115:2015 (ISO/IEC 29115:2013, IDT) “Інформаційні технології. Методи захисту. Структура гарантування автентифікації об'єктів” та національному нормативному документі ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT)

“Інформаційні технології. Методи захисту. Критерії оцінки. Частина I. Вступ та загальна модель”.

4. Фактор автентифікації поділяється на такі групи:

фактор автентифікації на підставі володіння – фактор автентифікації, зв'язок якого із особою встановлюється за результатом підтвердження володіння фактором автентифікації особою;

фактор автентифікації на підставі знання – фактор автентифікації, зв'язок якого із особою встановлюється за результатом підтвердження знання фактору автентифікації особою;

фактор автентифікації на підставі унікальної фізичної ознаки – фактор автентифікації, зв'язок якого із особою встановлюється за результатом підтвердження наявності в особи фактору автентифікації.

5. В інших випадках електронна ідентифікація фізичних осіб, юридичних осіб або представників юридичних осіб в інформаційно-телекомунікаційних системах сфери електронного урядування здійснюється з використанням схем та засобів електронної ідентифікації з високим або середнім рівнем довіри до засобів електронної ідентифікації.

6. Використання засобів електронної ідентифікації з низьким рівнем довіри в інформаційно-телекомунікаційних системах сфери електронного урядування допускається виключно для ідентифікації користувачів адміністративних послуг під час їх первинної реєстрації та доступу до складових систем – особистих кабінетів, через які здійснюється обмін інформацією про склад, порядок отримання послуг, статус розгляду заявок на отримання послуг та результати надання послуг в електронному вигляді.

7. Для визначення відповідності рівнів довіри до засобів електронної ідентифікації критеріям, передбаченим у статті 15 Закону України “Про

електронні довірчі послуги”, у розділі III цих Вимог наведено опис елементів технічних специфікацій та процедур.

8. Захист інформації, яка оброблюється в інформаційно-телекомунікаційних системах схем електронної ідентифікації, передається між такими системами та іншими системами сфери електронного урядування, здійснюється відповідно до вимог законодавства у сфері захисту інформації.

9. Відповідність засобів електронної ідентифікації, що видаються відповідно до схеми електронної ідентифікації, певному рівню довіри вважається встановленою за умови виконання всіх елементів технічних специфікацій та процедур, передбачених для певного рівня довіри цими Вимогами. Якщо засоби електронної ідентифікації, що видаються відповідно до схеми електронної ідентифікації, відповідають вимогам, передбаченим для високого рівня довіри, вважається, що ці засоби відповідають аналогічним вимогам до середнього та низького рівнів довіри.

II. Набори ідентифікаційних даних для сфери електронного урядування

1. Для підтвердження електронної ідентифікації фізичної, юридичної особи, представника юридичної особи під час електронної взаємодії у сфері електронного урядування установи та організації незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями, експертними дослідженнями та експлуатацією схем і засобів електронної ідентифікації, що видаються фізичним, юридичним особам та представникам юридичних осіб, мають використовувати обов'язкові та додаткові набори ідентифікаційних даних, визначені у цьому розділі.

2. Обов'язкові набори ідентифікаційних даних містять такі відомості:

1) для фізичних осіб:

прізвище, ім'я, по батькові (за наявності);

унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності);

реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті);

серія та номер посвідки на постійне (тимчасове) проживання або (за відсутності) серія (за наявності) та (або) номер паспорта громадянина іншої країни (посвідчення біженця) – для фізичних осіб, які не є громадянами України, - нерезидентів;

2) для юридичних осіб, фізичних осіб – підприємців:

найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України (далі – Єдиний державний реєстр);

прізвище, ім'я, по батькові фізичної особи – підприємця;

ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром;

реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті) для фізичної особи – підприємця;

3) для представників юридичних осіб:

відомості, визначені для фізичних осіб у підпункті 1 цього пункту;

унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності);

реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті);

серія та номер посвідки на постійне (тимчасове) проживання або (за відсутності) серія (за наявності) та (або) номер паспорта громадянина іншої країни (посвідчення біженця) – для фізичних осіб, які не є громадянами України, - нерезидентів.

2) для юридичних осіб, фізичних осіб – підприємців:

найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України (далі – Єдиний державний реєстр);

прізвище, ім'я, по батькові фізичної особи-підприємця;

ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром;

реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті) для фізичної особи-підприємця;

3) для представників юридичних осіб:

відомості, які визначені для фізичних осіб у підпункті 1) цього пункту;

найменування юридичної особи згідно з Єдиним державним реєстром, представником якої є фізична особа;

ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром, представником якої є фізична особа.

3. Додаткові набори ідентифікаційних даних не мають впливати на технологічну сумісність схем та засобів електронної ідентифікації з інформаційно-телекомунікаційними системами сфери електронного урядування та можуть містити такі відомості:

1) для фізичних осіб:

найменування установи, яка видала паспорт або інший документ, що посвідчує особу;

дата видачі паспорта або іншого документа, що посвідчує особу;

серія та (або) номер документа, що підтверджує право фізичної особи на здійснення діяльності у певній сфері;

місце народження;

місце проживання;

2) для юридичних осіб, фізичних осіб – підприємців:

місцезнаходження юридичної особи (область, населений пункт) згідно з Єдиним державним реєстром;

3) для представників юридичних осіб:

місцезнаходження юридичної особи (область, населений пункт) згідно з Єдиним державним реєстром, представником якої є фізична особа.

4. Для однозначного підтвердження електронної ідентифікації інформаційних або інформаційно-телекомунікаційних систем та (або)

походження і цілісності електронних даних під час електронної взаємодії у сфері електронного урядування установи та організації незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями, експертними дослідженнями та експлуатацією схем і засобів електронної ідентифікації, мають використовувати ідентифікаційні дані, що містяться у кваліфікованих сертифікатах електронних печаток, створювачами яких є учасники електронної взаємодії.

III. Технічні специфікації та процедури

1. Елементи технічних специфікацій та процедур, наведені у цьому розділі, мають використовуватись для встановлення відповідності рівнів довіри до засобів електронної ідентифікації критеріям, передбаченим у статті 15 Закону України "Про електронні довірчі послуги", до засобів електронної ідентифікації, випущених відповідно до схеми електронної ідентифікації.

2. Елементи технічних специфікацій та процедур до:

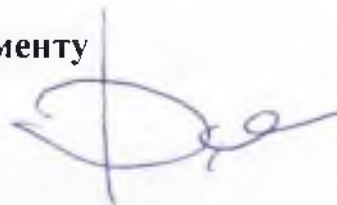
реєстрації власників засобів електронної ідентифікації наведені у додатку 1 до цих Вимог;

управління засобами електронної ідентифікації наведені у додатку 2 до цих Вимог;

автентифікації наведені у додатку 3 до цих Вимог;

управління та організації наведені у додатку 4 до цих Вимог.

Директор генерального департаменту
цифрової трансформації



Д. МАКОВСЬКИЙ

Додаток 1
до Вимог до засобів електронної
ідентифікації, рівнів довіри до
засобів електронної
ідентифікації для їх
використання у сфері
електронного урядування
(пункт 2 розділу III)

**ЕЛЕМЕНТИ ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ ТА ПРОЦЕДУР
до реєстрації власників засобів електронної ідентифікації**

Подання заявки на реєстрацію

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Забезпечення того, що особі відомі умови, пов'язані з використанням засобів електронної ідентифікації. 2. Забезпечення того, що особі відомі рекомендовані заходи безпеки, пов'язані з використанням засобів електронної ідентифікації. 3. Збір відповідних ідентифікаційних даних, необхідних для підтвердження та верифікації тотожності особи
Середній	Такі самі, як для низького рівня довіри
Високий	Такі самі, як для низького рівня довіри

Встановлення особи та підтвердження ідентифікаційних даних

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Встановлення особи може здійснюватися віддалено. 2. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих від особи
Середній	1. Встановлення особи здійснюється віддалено або за особистої присутності. 2. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих від особи. 3. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих із достовірного джерела
Високий	1. Встановлення особи здійснюється тільки за особистої присутності. 2. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих від особи. 3. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих із достовірного джерела

Встановлення ідентичності та підтвердження ідентифікаційних даних
фізичної особи

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Особа володіє інформацією, яка дозволяє відповідно до законодавства України встановити ідентичність фізичної особи та осіб, які представляють заявлену особу. 2. Існує ймовірність, що такі відомості є справжніми або такими, існування яких підтверджено достовірним джерелом. 3. З достовірного джерела відомо, що заявлена особа існує. Існує ймовірність, що особа, яка заявляє про ідентичність з нею, і є цією особою
Середній	Виконуються вимоги до обов'язкових елементів технічних специфікацій та процедур низького рівня довіри та додатково виконується одна з вимог, зазначених у пунктах 1–4. 1. Фізичну особу встановлено як таку, що володіє відомостями, які відповідно до законодавства України встановлюють ідентичність особи та представляють заявлену особу, та здійснено перевірку відомостей на їх справжність (або з достовірного джерела відомо, що такі відомості існують та належать до реальної особи), а також вжито заходів щодо мінімізації ризиків відсутності ідентичності фізичної особи із заявленою особою з урахуванням ризиків втрати, викрадення, призупинення дії,

відкликання чи закінчення терміну дії відомостей про особу.

2. Документ, що посвідчує фізичну особу, пред'являється під час процесу реєстрації і встановлюється, що такий документ належить особі, яка його пред'являє, та вживаються заходи щодо мінімізації ризиків відсутності ідентичності фізичної особи із заявленою особою з урахуванням ризиків втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії документів, що посвідчують особу.

3. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у пунктах 1 та 2 для середнього рівня довіри до засобів електронної ідентифікації, суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню 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. Якщо засоби електронної ідентифікації випускаються 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, суб'єкт, що реєструє, не повинен повторно виконувати попередні процедури. У разі якщо 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
Високий	Виконуються одна з вимог, зазначених у пунктах 1 та 2. 1. Крім обов'язкових елементів технічних специфікацій та процедур, які відповідають середньому рівню довіри до засобів електронної ідентифікації, додатково виконується одна з вимог, зазначених у підпунктах 1-3: 1) якщо фізичну особу встановлено як таку, що володіє біометричними даними, які відповідно до законодавства України підтверджують ідентичність особи, і ці дані представляють заявлену особу, дійсність таких даних перевіряється за допомогою достовірного джерела. Фізичну особу, яка заявляє про ідентичність, встановлюють шляхом зіставлення однієї або більше біометричних характеристик із даними з достовірного джерела; 2) якщо процедури, що використовувались раніше публічними або приватними суб'єктами для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених вище у цьому пункті для високого рівня довіри до засобів електронної ідентифікації, суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню 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 надають змогу підтвердити чинність результатів процедур встановлення ідентичності та підтвердження ідентифікаційних даних фізичної особи для низького та середнього рівнів; 3) якщо засоби електронної ідентифікації випускаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають високий рівень довіри з урахуванням ризиків зміни ідентифікаційних даних, суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що додатково вживаються заходи, які надають змогу підтвердити чинність результатів процедур випуску засобів електронної ідентифікації, що належать до схеми електронної ідентифікації. 2. Якщо фізична особа, яка заявляє про ідентичність, не надає біометричні дані, які відповідно до законодавства України підтверджують ідентичність особи, застосовуються процедури отримання таких даних з достовірних джерел
--	---

Встановлення ідентичності та підтвердження ідентифікаційних даних
юридичної особи

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Заявлену юридичну особу представлено на основі відомостей, які відповідно до законодавства України встановлюють ідентичність особи та які представляють заявлену особу. 2. Відомості про юридичну особу, ідентичність якої заявляється, є дійсними і можна припустити, що такі відомості є достовірними або такими, існування яких підтверджено достовірним джерелом, якщо внесення відомостей до достовірного джерела є добровільним та регулюється домовленістю між юридичною особою та достовірним джерелом. 3. Існує ймовірність, що такі відомості є достовірними або такими, існування яких підтверджено достовірним джерелом. 4. У достовірному джерелі відсутні дані щодо статусу юридичної особи, який би перешкоджав їй діяти як юридичній особі, ідентичність якої заявляється
Середній	Виконуються вимоги до обов'язкових елементів технічних специфікацій та процедур низького рівня довіри та додатково виконується одна з вимог, зазначених у пунктах 1-3. 1. Юридичну особу, ідентичність якої заявляється, представлено на основі відомостей, які відповідно до законодавства України встановлюють ідентичність особи та які представляють заявлену особу, у тому числі

найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України та ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України, здійснено перевірку відомостей на їх справжність (або з достовірного джерела відомо, що такі відомості існують та належать до реальної юридичної особи), якщо внесення відомостей до достовірного джерела здійснено для підтвердження повноважень юридичної особи в межах сфери її діяльності, а також вжито заходів щодо мінімізації ризиків відсутності ідентичності юридичної особи із заявленою особою з урахуванням ризиків втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії відомостей (документів) про особу.

2. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених пунктом 1 для середнього рівня довіри до засобів електронної ідентифікації, суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню 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. Якщо засоби електронної ідентифікації випускаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають

	середній або високий рівень довіри, суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури. У разі якщо 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	Виконуються вимоги до обов'язкових елементів технічних специфікацій та процедур середнього рівня довіри та додатково виконується одна з вимог, зазначених у пунктах 1, 2. 1. Юридичну особу, ідентичність якої заявляється, представлено на основі відомостей, які відповідно до законодавства України встановлюють ідентичність особи та які представляють заявлену особу, у тому числі найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України та ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України, здійснено перевірку відомостей на їх справжність за допомогою достовірного джерела. 2. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у пункті 1 для високого рівня довіри до засобів електронної ідентифікації, суб'єкт, відповідальний за

	реєстрацію, не повинен повторно виконувати ці процедури за умови, що їхню 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. Якщо засоби електронної ідентифікації випускаються з використанням інших засобів електронної ідентифікації, які належать до схеми електронної ідентифікації та мають високий рівень довіри, суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати ці процедури. Додатково вживаються заходи, що надають змогу підтвердити чинність результатів попередніх процедур випуску засобів електронної ідентифікації, що належать до схеми електронної ідентифікації
--	---

Встановлення зв'язку між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Підтвердження ідентифікаційних даних фізичної особи, яка представляє юридичну особу, здійснено за процедурами, які відповідають низькому, середньому або високому рівню довіри. 2. Зв'язок між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа, встановлюється за допомогою процедур, визначених

	законодавством (наприклад, про нотаріат, про державну реєстрацію тощо). 3. У достовірному джерелі відсутні дані щодо неможливості фізичній особі представляти юридичну особу
Середній	Виконуються вимоги, зазначені у пункті 3 обов'язкових елементів технічних специфікацій та процедур низького рівня довіри, а також вимоги, зазначені у пунктах 1-3. 1. Підтвердження ідентифікаційних даних фізичної особи, яка представляє юридичну особу, здійснено за процедурами, які відповідають середньому або високому рівню довіри. 2. Зв'язок між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа, встановлено за допомогою процедур, визначених законодавством (наприклад, про нотаріат, про державну реєстрацію тощо щодо реєстрації у (реєстрі, інформаційній системі) достовірному джерелі). 3. Зв'язок між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа, підтверджено за допомогою даних, отриманих із достовірного джерела
Високий	Виконуються вимоги, зазначені у пункті 3 обов'язкових елементів технічних специфікацій та процедур низького рівня довіри, пункті 2 обов'язкових елементів технічних специфікацій та процедур середнього рівня довіри, а також вимоги, зазначені у пунктах 1, 2.

	1. Підтвердження ідентифікаційних даних фізичної особи, яка представляє юридичну особу, здійснено за процедурами, які відповідають високому рівню довіри. 2. Зв'язок між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа, підтверджено за допомогою даних, отриманих із достовірного джерела, на основі унікального ідентифікатора
--	---



Додаток 2
до Вимог до засобів електронної
ідентифікації, рівнів довіри до
засобів електронної
ідентифікації для їх
використання у сфері
електронного урядування
(пункт 2 розділу III)

ЕЛЕМЕНТИ ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ ТА ПРОЦЕДУР
до управління засобами електронної ідентифікації

Характеристики засобів електронної ідентифікації та їх реалізація

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Засоби електронної ідентифікації використовують щонайменше один фактор автентифікації згідно з пунктом 4 розділу I Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування, затверджених наказом Державного агентства з питань електронного урядування України від 27 листопада 2018 року № 86. 2. Засоби електронної ідентифікації розроблено так, щоб суб'єкт, який їх видає, міг вживати необхідних заходів для перевірки використання таких засобів під контролем або у межах володіння особи, якій такі засоби належать
Середній	1. Засоби електронної ідентифікації використовують щонайменше два фактори автентифікації згідно з пунктом 4 розділу I Вимог до засобів електронної ідентифікації,

	рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування, затверджених наказом Державного агентства з питань електронного урядування України від 27 листопада 2018 року № 86. 2. Засоби електронної ідентифікації розроблено так, щоб можна було припустити, що вони використовуються тільки під контролем або у межах володіння особи, якій такі засоби належать
Високий	Такі самі, як для середнього рівня довіри. 1. Засоби електронної ідентифікації захищено від дублювання та несанкціонованого доступу з боку порушників з високим потенціалом здійснення нападу. 2. Засоби електронної ідентифікації розроблено так, що фізична чи юридична особа, якій вони належать, може надійно захистити їх від несанкціонованого використання іншими особами

Випуск, доставка та активація засобів електронної ідентифікації

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	Після випуску засобів електронної ідентифікації вони доставляються з використанням механізму, за допомогою якого, існує ймовірність, що ці засоби будуть доставлені фізичній чи юридичній особі, яка їх замовила

Середній	Після випуску засобів електронної ідентифікації вони доставляються у спосіб, за допомогою якого існує ймовірність, що ці засоби передаються у володіння тільки особі, якій вони належать
Високий	У процесі активації здійснюється підтвердження передання засобів електронної ідентифікації у володіння особі, якій вони належать

Призупинення, відкликання та поновлення дії засобів електронної
ідентифікації

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Має бути забезпечена можливість призупинення та (або) відкликання засобу електронної ідентифікації вчасно та ефективно. 2. Мають бути впроваджені заходи із запобігання несанкціонованого призупинення, відкликання та (або) поновлення дії засобів електронної ідентифікації. 3. Поновлення дії засобів електронної ідентифікації має здійснюватися за умови дотримання вимог до обов'язкових елементів технічних специфікацій та процедур, які відповідають початковій видачі засобів електронної ідентифікації
Середній	Такі самі, як для низького рівня довіри
Високий	Такі самі, як для низького рівня довіри

Поновлення та заміна ідентифікаційних даних

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	Процедури поновлення або заміни ідентифікаційних даних мають здійснюватися відповідно до обов'язкових елементів технічних специфікацій та процедур, які відповідають початковій видачі ідентифікаційних даних, опис якої наведено в додатку 1 до Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування, затверджених наказом Державного агентства з питань електронного урядування України від 27 листопада 2018 року № 86, та цьому додатку
Середній	Такі самі, як для низького рівня довіри
Високий	Такі самі, як для низького рівня довіри. Якщо поновлення та заміна здійснюються з використанням чинного засобу електронної ідентифікації, має бути здійснено встановлення особи з використанням достовірного джерела



Додаток 3

до Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування (пункт 2 розділу III)

**ЕЛЕМЕНТИ ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ ТА ПРОЦЕДУР
до автентифікації**

Вимоги до механізму автентифікації засобів електронної ідентифікації

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Перед переданням ідентифікаційних даних має здійснюватися надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності. 2. Якщо ідентифікаційні дані зберігаються як частина механізму автентифікації, має здійснюватися захист такої інформації від втрат та компрометації, у тому числі захист від втрат та компрометації у режимі офлайн. 3. Механізм автентифікації має забезпечувати 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 потенціалом здійснення нападу вище ніж базовий
Середній	Такі самі, як для низького рівня довіри.

	1. Перед переданням ідентифікаційних даних мають здійснюватися надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності за допомогою динамічної автентифікації. 2. Механізм автентифікації має забезпечувати 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 із середнім потенціалом здійснення нападу
Високий	Такі самі, як для середнього рівня довіри. Механізм автентифікації має забезпечувати 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 високим потенціалом здійснення нападу



Додаток 4

до Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування (пункт 2 розділу III)

ЕЛЕМЕНТИ ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ ТА ПРОЦЕДУР

до управління та організації

Адміністратори систем

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Адміністратори систем повинні бути зареєстрованими відповідно до Закону України “Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань”, мати визначену організаційну структуру та здійснювати діяльність у всіх сегментах, пов'язаних з наданням електронних довірчих послуг. 2. Адміністратори систем повинні мати повноваження витребувати, перевіряти та обробляти ідентифікаційні дані. 3. Адміністратори систем мають відповідати за збитки, а також мати достатні фінансові ресурси для продовження діяльності з видачі засобів електронної ідентифікації та експлуатації інформаційно-телекомунікаційних систем схем електронної ідентифікації. 4. Адміністратори систем відповідають за виконання будь-яких зобов'язань, переданих іншому суб'єкту (представництву), та за дотримання правил функціонування

	схеми електронної ідентифікації іншими суб'єктами (представництвами). 5. Адміністратори систем повинні мати план припинення діяльності, 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

Публікація повідомлень та інформація для користувачів

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Має бути забезпечено оприлюднення опису процесів та процедур, пов'язаних із видачею та використанням засобів електронної ідентифікації, який має містити усі правила, умови експлуатації та відомості про платежі, у тому числі будь-які обмеження щодо використання засобів. Опис також має містити правила захисту персональних даних. 2. Має бути впроваджено відповідну політику та процедури з метою своєчасного (та у надійний спосіб) отримання користувачами інформації про будь-які зміни в описі процесів та процедур, пов'язаних із видачею та

	використанням засобів електронної ідентифікації, правилах, умовах експлуатації та правилах захисту персональних даних. 3. Має бути впроваджено відповідну політику та процедури, які забезпечать надання вичерпних відповідей 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

Управління інформаційною безпекою

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	Впроваджена система управління інформаційною безпекою та контролю за ризиками інформаційної безпеки
Середній	Такі самі, як для низького рівня довіри. Впроваджена система управління інформаційною безпекою та комплексна система захисту інформації відповідно до вимог законодавства у сфері захисту інформації з урахуванням вимог національних стандартів у сфері управління інформаційної безпеки
Високий	Такі самі, як для середнього рівня довіри

Зберігання даних

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Запис та зберігання даних, які обробляються в інформаційно-телекомунікаційній системі схеми електронної ідентифікації, мають здійснюватися із використанням системи управління записами. 2. Зберігання даних, які оброблюються в інформаційно-телекомунікаційній системі схеми електронної ідентифікації, має здійснюватися протягом строків, визначених законодавством у сфері телекомунікацій, захисту інформації та персональних даних, впродовж яких вони будуть необхідні для цілей аудиту та розслідування порушень безпеки. 3. Після закінчення строку зберігання дані, які оброблялись в інформаційно-телекомунікаційній системі схеми електронної ідентифікації, мають знищуватись у гарантований спосіб, який забезпечує відсутність можливості відновлення таких даних
Середній	Такі самі, як для низького рівня
Високий	Такі самі, як для низького рівня

Об'єктовий контроль та персонал

У наведеній нижче таблиці зазначено вимоги щодо об'єктів (будівель і приміщень) та працівників, обов'язки яких безпосередньо пов'язані із

забезпеченням функціонування інформаційно-телекомунікаційної системи схеми електронної ідентифікації та випуском засобів електронної ідентифікації

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Визначення адміністратором системи процедур, які забезпечують перевірку наявності у працівників належної підготовки, кваліфікації та досвіду, необхідних для виконання ними своїх обов'язків. 2. Наявність кількості працівників, які належно забезпечать функціонування інформаційно-телекомунікаційної системи схеми електронної ідентифікації та випуск засобів електронної ідентифікації відповідно до прийнятих вимог, принципів та процедур. 3. Об'єкти (будівлі та приміщення), які використовуються для забезпечення функціонування інформаційно-телекомунікаційної системи схеми електронної ідентифікації та випуску 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. На об'єктах (у будівлях та приміщеннях), які використовуються для забезпечення функціонування інформаційно-телекомунікаційної системи схеми електронної ідентифікації та випуску засобів електронної ідентифікації, доступ до зон, у яких зберігаються та оброблюються персональні дані, ключова інформація

	(криптографічний матеріал) або інша вразлива інформація надається виключно уповноваженим адміністратором системи працівникам
Середній	Такі самі, як для низького рівня довіри
Високий	Такі самі, як для низького рівня довіри

Технічний контроль

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	1. Наявність пропорційного технічного контролю для управління ризиками, які загрожують безпеці обслуговування, захисту конфіденційності, цілісності та доступності інформації, що оброблюється в інформаційно-телекомунікаційній системі. 2. Канали зв'язку, які використовуються для обміну персональними даними та вразливою інформацією, захищено від несанкціонованого ознайомлення, модифікації та повторного відтворення інформації. 3. Доступ до вразливої ключової інформації (криптографічного матеріалу), якщо така (такий) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-телекомунікаційної системи схеми електронної ідентифікації, обмежено програмами, які чітко вимагають доступу залежно від кола посадових обов'язків.

	Забезпечується зберігання такого матеріалу у встановленому законодавством порядку. 4. Існують формалізовані процедури, які забезпечують підтримку безпеки впродовж визначеного терміну і можливість реагувати на зміни рівнів ризику, інциденти та порушення безпеки. 5. Усі засоби, що містять персональні дані, ключову інформацію (криптографічний матеріал) або іншу вразливу інформацію, зберігаються, передаються та знищуються у встановлений законодавством спосіб
Середній	Такі самі, як для низького рівня довіри. Вразливу ключову інформацію (криптографічний матеріал), якщо така (такий) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-телекомунікаційної системи схеми електронної ідентифікації, захищено від несанкціонованого доступу та копіювання
Високий	Такі самі, як для низького рівня довіри. Вразлива ключова інформація (криптографічний матеріал), яка (який) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-телекомунікаційної системи схеми електронної ідентифікації, захищається завдяки вбудованим апаратно-програмним засобам, що забезпечують захист записаних на них даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання

Відповідність вимогам та аудит

Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
Низький	Проведення внутрішніх аудитів інформаційної безпеки, які охоплюють усі сегменти інформаційно-телекомунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання встановлених вимог, принципів та процедур у визначені строки
Середній	Таки самі, як для низького рівня довіри. Періодичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-телекомунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання прийнятих вимог, принципів та процедур
Високий	1. Систематичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-телекомунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання встановлених вимог, принципів та процедур. 2. Проведення заходів державного контролю за станом технічного та криптографічного захисту інформації в інформаційно-телекомунікаційній системі схеми електронної ідентифікації

