ЗАТВЕРДЖЕНО
Наказ Міністерства цифрової трансформації України
_____ 2023 року № ____

Відомості
про засоби електронної ідентифікації в контексті схем електронної ідентифікації для їх використання у сфері електронного урядування

І. Загальні відомості про постачальника послуг з електронної ідентифікації

Назва схеми (у разі наявності) _____

Рівень надійності _____
(низький, середній або високий)

Постачальник послуг з електронної ідентифікації _____
(повне найменування юридичної особи згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб – підприємців та громадських формувань або прізвище, власне ім'я, по батькові (за наявності) фізичної особи - підприємця)

Керівник юридичної особи _____
(прізвище, власне ім'я, по батькові (за наявності) керівника юридичної особи, серія (за наявності) і номер паспорта громадянина України, ким і коли виданий)

або

Прізвище, власне ім’я, по батькові (за наявності) фізичної особи – підприємця_____

_____

(серія (за наявності) та номер паспорта громадянина України, ким і коли виданий)

_____

(реєстраційний номер облікової картки платника податків (за наявності)

_____

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

Контактна інформація юридичної особи або фізичної особи – підприємця _____

_____

(номери телефонів)

_____

(електронна адреса інформаційного ресурсу)

_____

(адреса електронної пошти)

ІІ. Набори ідентифікаційних даних для сфери електронного урядування*

1. Обов’язкові набори ідентифікаційних даних для встановлення фізичних осіб, фізичних осіб - підприємців

Прізвище, власне 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 громадянина України (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 громадянина України) ☐

Серія (за наявності) та/або номер посвідки на постійне (тимчасове) проживання або (за відсутності) серія (за наявності) та/або номер паспорта громадянина іншої країни (посвідчення біженця) – для фізичних осіб – нерезидентів ☐

2. Обов’язкові набори ідентифікаційних даних для встановлення юридичних осіб

Найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України ☐

Ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України ☐

3. Обов’язкові набори ідентифікаційних даних для встановлення представників юридичних осіб ☐

Відомості, що визначені для фізичних осіб ☐

Найменування юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України, представником якої є фізична особа ☐

Ідентифікаційний код юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України, представником якої є фізична особа ☐

4. Додаткові набори ідентифікаційних даних, які не мають впливати на технологічну сумісність схем та засобів електронної ідентифікації з інформаційно-комунікаційними системами сфери електронного урядування

Для встановлення фізичних осіб, фізичних осіб – підприємців

Уповноважений суб’єкт, що видав паспорт громадянина України або інший документ, що посвідчує особу ☐

Дата видачі паспорта громадянина України 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 (місце перебування) ☐

Для встановлення юридичних осіб, фізичних осіб – підприємців

Місцезнаходження юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України ☐

Для встановлення представників юридичних осіб

Місцезнаходження юридичної особи згідно з Єдиним державним реєстром підприємств та організацій України, представником якої є фізична особа ☐

III. Елементи
технічних специфікацій та процедур для реєстрації постачальників послуг з електронної ідентифікації та засобів електронної ідентифікації в контексті схеми електронної ідентифікації

№ з/п	Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур	Опис виконання процедур про відповідність	Позначка про відповідність (відповідає/ не відповідає)
1	2	3	4	5
1. Подання заявки на реєстрацію				
1	Низький	1.1 Забезпечення того, що особі відомі умови, пов'язані з використанням засобів електронної ідентифікації. 1.2. Забезпечення того, що особі відомі рекомендовані заходи безпеки, пов'язані з використанням засобів електронної ідентифікації. 1.3. Збір відповідних ідентифікаційних даних, необхідних для підтвердження та ідентифікації.		
2	Середній	2.1. Такі самі, як для низького рівня довіри.		
3	Високий	3.1. Такі самі, як для низького рівня довіри.		

2. Встановлення особи та підтвердження ідентифікаційних даних				
1	Низький	1.1. Встановлення особи може здійснюватися віддалено. 1.2. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих від особи.		
2	Середній	2.1. Встановлення особи здійснюється віддалено або за особистої присутності. 2.2. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих від особи. 2.3. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих із достовірного джерела.		
3	Високий	3.1. Встановлення особи здійснюється тільки за особистої присутності. 3.2. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих від особи. 3.3. Підтвердження ідентифікаційних даних особи здійснюється за допомогою даних, отриманих із достовірного джерела.		
3. Встановлення особи та підтвердження ідентифікаційних даних фізичної особи				
1	Низький	1.1. Особа володіє інформацією, яка дозволяє відповідно до законодавства України ідентифікувати фізичну особу та осіб, які представляють заявлену особу. 1.2. Існує ймовірність, що такі відомості є справжніми або такими, існування яких підтверджено достовірним джерелом.		

		1.3. З достовірного джерела відомо, що заявлена особа існує. Існує ймовірність, що особа, яка заявляє про ідентифікацію з нею, і є цією особою.		
2	Середній	Виконуються вимоги до обов'язкових елементів технічних специфікацій та процедур низького рівня довіри та додатково виконується одна з вимог, зазначених у підпунктах 2.1-2.4 цього пункту. 2.1. Фізичну особу встановлено як таку, що володіє відомостями, які відповідно до законодавства України встановлюють особу 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 фізичної особи із заявленою особою з урахуванням ризиків втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії відомостей про особу. 2.2. 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 фізичної особи із заявленою особою з урахуванням ризиків втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії документів, що посвідчують особу. 2.3. 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 підпунктах 2.1 та 2.2 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. 2.4. 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.		
3	Високий	Виконується одна з вимог, зазначених у підпунктах 3.1 та 3.2 цього пункту. 3.1. 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 3.1.1-3.1.2 цього пункту: 3.1.1. Якщо фізичну особу встановлено як таку, що володіє біометричними даними, які відповідно до законодавства України підтверджують особу, і ці дані представляють заявлену особу, дійсність таких даних перевіряється за допомогою достовірного джерела. Фізичну особу, яка заявляє про це, встановлюють шляхом зіставлення однієї або більше біометричних характеристик із даними з достовірного джерела. 3.1.2. 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. Додатково вживаються заходи, що надають змогу підтвердити чинність результатів процедур встановлення особи та підтвердження ідентифікаційних даних фізичної особи для низького та середнього рівнів. 3.1.3. 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. 3.2. Якщо фізична особа, яка заявляє про себе, не надає біометричні дані, які відповідно до законодавства України підтверджують особу, застосовуються процедури отримання таких даних з достовірних джерел.		
4. Встановлення особи та підтвердження ідентифікаційних даних юридичної особи				
1	Низький	1.1. Заявлену юридичну особу представлено на основі відомостей, які відповідно до законодавства України встановлюють особу та які представляють заявлену особу.		

		1.2. Відомості про юридичну особу, стосовно 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. 1.3. Існує ймовірність, що такі відомості є достовірними або такими, існування яких підтверджено достовірним джерелом. 1.4. У достовірному джерелі відсутні дані щодо статусу юридичної особи, який би перешкоджав їй діяти як юридичній особі, про яку заявляється.		
2	Середній	Виконуються вимоги до обов'язкових елементів технічних специфікацій та процедур низького рівня довіри та додатково виконується одна з вимог, зазначених у підпунктах 2.1-2.3 цього пункту. 2.1. Юридичну особу, про яку заявляється, представлено на основі відомостей, які відповідно до законодавства України встановлюють особу 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 юридичної особи із заявленою особою з		

		урахуванням ризиків втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії відомостей (документів) про особу. 2.2. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених підпунктом 2.1 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. 2.3. 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.		
3	Високий	Виконуються вимоги до обов'язкових елементів технічних специфікацій та процедур середнього рівня довіри та додатково виконується одна з вимог, зазначених у підпунктах 3.1-3.3 цього пункту. 3.1. Юридичну особу, про яку заявляється, представлено на основі відомостей, які відповідно до законодавства України встановлюють особу 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. 3.2. 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 підпункті 3.1 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. 3.3. 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.		
5. Встановлення зв'язку між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа				
1	Низький	1.1. Підтвердження ідентифікаційних даних фізичної особи, яка представляє юридичну особу, здійснено за процедурами, які відповідають низькому, середньому або високому рівням довіри.		

		1.2. 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). 1.3. У достовірному джерелі відсутні дані щодо неможливості фізичній особі представляти юридичну особу.		
2	Середній	Виконуються вимоги, зазначені у пункті 1 обов’язкових елементів технічних специфікацій та процедур низького рівня довіри, а також вимоги, зазначені у підпунктах 2.1-2.3 цього пункту. 2.1. Підтвердження ідентифікаційних даних фізичної особи, яка представляє юридичну особу, здійснено за процедурами, які відповідають середньому або високому рівню довіри. 2.2. 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). 2.3. Зв’язок між ідентифікаційними даними фізичної особи та юридичної особи, яку представляє ця фізична особа, підтверджено за допомогою даних, отриманих із достовірного джерела.		
3	Високий	Виконуються вимоги, зазначені у пункті 1 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 підпунктах 3.1, 3.2 цього пункту.		

		3.1. Підтвердження ідентифікаційних даних фізичної особи, яка представляє юридичну особу, здійснено за процедурами, які відповідають високому рівню довіри. 3.2. 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.		

IV. Елементи технічних специфікацій та процедур до управління засобами електронної ідентифікації

№ з/п	Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур	Опис виконання процедур про відповідність	Позначка про відповідність (відповідає/ не відповідає)
1	2	3	4	5
1. Характеристики засобів електронної ідентифікації та їх реалізація				
1	Низький	1.1. 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 Міністерства цифрової трансформації України від 05 грудня 2022 року № 130, зареєстрованих у Міністерстві юстиції України 20 січня 2023 року за № 129/39185.		

		1.2. 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.		
2	Середній	2.1. 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 Міністерства цифрової трансформації України від 05 грудня 2022 року № 130, зареєстрованих у Міністерстві юстиції України 20 січня 2023 року за № 129/39185. 2.2. Засоби електронної ідентифікації розроблено так, щоб можна було припустити, що вони використовуються тільки під контролем або у межах володіння особи, якій такі засоби належать.		
3	Високий	3.1. Такі самі, як для середнього рівня довіри. 3.2. Засоби електронної ідентифікації захищено від дублювання та несанкціонованого доступу з боку порушників з високим потенціалом здійснення нападу. 3.3. Засоби електронної ідентифікації розроблено так, що фізична чи юридична особа, якій вони належать, може надійно захистити їх від несанкціонованого використання іншими особами.		

2. Видача, доставка та активація засобів електронної ідентифікації				
1	Низький	1.1. Після випуску засобів електронної ідентифікації вони доставляються у спосіб, за допомогою якого існує ймовірність, що ці засоби будуть доставлені фізичній чи юридичній особі, яка їх замовила.		
2	Середній	2.1. 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.		
3	Високий	3.1. У процесі активації здійснюється підтвердження передання засобів електронної ідентифікації у володіння особі, якій вони належать.		
3. Призупинення, відкликання та поновлення дії засобів електронної ідентифікації				
1	Низький	1.1. Має бути забезпечена можливість призупинення та (або) відкликання засобу електронної ідентифікації вчасно та ефективно. 1.2. Мають бути впроваджені заходи із запобігання несанкціонованого призупинення, відкликання та/або поновлення дії засобів електронної ідентифікації. 1.3. 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.		

2	Середній	2.1. Такі самі, як для низького рівня довіри.		
3	Високий	3.1. Такі самі, як для низького рівня довіри.		
4. Поновлення та заміна ідентифікаційних даних				
1	Низький	1.1. 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 визначено вимогами до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування, затверджених наказом Міністерства цифрової трансформації України від 05 грудня 2022 року № 130, зареєстрованих у Міністерстві юстиції України 20 січня 2023 року за № 129/39185, та цих Відомостей.		
2	Середній	2.1. Такі самі, як для низького рівня довіри.		
3	Високий	3.1. Такі самі, як для низького рівня довіри. 3.2. Якщо поновлення та заміна здійснюються з використанням чинного засобу електронної ідентифікації, має бути здійснено встановлення особи з використанням достовірного джерела.		

V. Елементи
технічних специфікацій та процедур до автентифікації

№ з/п	Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур	Опис виконання процедур про відповідність	Позначка про відповідність (відповідає/ не відповідає)
1	2	3	4	5
1. Вимоги до механізму автентифікації засобів електронної ідентифікації				
1	Низький	1.1. Перед переданням ідентифікаційних даних має здійснюватися надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності. 1.2. 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 в режимі офлайн. 1.3. 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.		
2	Середній	2.1. Такі самі, як для низького рівня довіри.		

		2.2. Перед переданням ідентифікаційних даних мають здійснюватися надійна верифікація засобів електронної ідентифікації та встановлення їх дійсності за допомогою динамічної автентифікації. 2.3. 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 із середнім потенціалом здійснення нападу.		
3	Високий	3.1. Такі самі, як для середнього рівня довіри. 3.2. 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 з високим потенціалом здійснення нападу.		

VI. Елементи технічних специфікацій та процедур до управління та організації

№ з/п	Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур	Опис виконання процедур про відповідність	Позначка про відповідність (відповідає/ не відповідає)
1	2	3	4	5

1. Адміністратори систем**				
1	Низький	1.1. 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 послуг. 1.2. Адміністратори систем повинні мати повноваження витребувати, перевіряти та обробляти ідентифікаційні дані. 1.3. Адміністратори систем є відповідальними за шкоду заподіяну у сфері електронної ідентифікації, а також повинні мати достатні фінансові ресурси для продовження діяльності з видачі засобів електронної ідентифікації та експлуатації інформаційно-комунікаційних систем схем електронної ідентифікації. 1.4. Адміністратори систем є відповідальними за виконання будь-яких зобов'язань, переданих іншому суб'єкту (представництву), та за дотримання правил функціонування схеми електронної ідентифікації іншими суб'єктами (представництвами). 1.5. 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.		
2	Середній	2.1. Такі самі, як для низького рівня довіри.		

3	Високий	2.2. Такі самі, як для низького рівня довіри.		
2. Публікація повідомлень та інформація для користувачів				
1	Низький	1.1. 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. 1.2. 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. 1.3. Має бути впроваджено відповідну політику та процедури, які забезпечать надання вичерпних відповідей на запити про надання інформації щодо видачі та використання засобів електронної ідентифікації.		
2	Середній	2.1. Такі самі, як для низького рівня довіри.		
3	Високий	3.1. Такі самі, як для низького рівня довіри.		

3. Управління інформаційною безпекою				
1	Низький	1.1. Впроваджена система управління інформаційною безпекою та контролю за ризиками інформаційної безпеки.		
2	Середній	2.1. Такі самі, як для низького рівня довіри. 2.2. 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.		
3	Високий	3.1. Такі самі, як для середнього рівня довіри.		
4. Зберігання даних				
1	Низький	1.1. Запис та зберігання даних, які обробляються в інформаційно-комунікаційній системі схеми електронної ідентифікації, мають здійснюватися із використанням системи управління записами. 1.2. Зберігання даних, які оброблюються в інформаційно-комунікаційній системі схеми електронної ідентифікації, має здійснюватися протягом строків, визначених законодавством у сфері електронних комунікацій, захисту інформації та персональних даних, впродовж яких вони будуть необхідні для цілей аудиту та розслідування порушень вимог безпеки.		

		1.3. Після закінчення строку зберігання дані, які оброблялись в інформаційно-комунікаційній системі схеми електронної ідентифікації, мають знищуватись у гарантований спосіб, який забезпечує відсутність можливості відновлення таких даних.		
2	Середній	2.1. Такі самі, як для низького рівня.		
3	Високий	3.1. Такі самі, як для низького рівня.		
5. Об'єктовий контроль та персонал (у главі зазначено вимоги щодо об'єктів (будівель і приміщень) та працівників, обов'язки яких безпосередньо пов'язані із забезпеченням функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та випуском засобів електронної ідентифікації)				
1	Низький	1.1. Визначення адміністратором системи процедур, які забезпечують перевірку наявності у працівників належної підготовки, кваліфікації та досвіду, необхідних для виконання ними своїх обов'язків. 1.2. Наявність кількості працівників, які належно забезпечать функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та випуск засобів електронної ідентифікації відповідно до прийнятих вимог, принципів та процедур. 1.3. Об'єкти (будівлі та приміщення), які використовуються для забезпечення функціонування інформаційно-комунікаційної 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. 1.4. На об’єктах (у будівлях та приміщеннях), які використовуються для забезпечення функціонування інформаційно-комунікаційної 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.		
2	Середній	2.1. Такі самі, як для низького рівня довіри.		
3	Високий	3.1. Такі самі, як для низького рівня довіри.		
6. Технічний контроль				
1	Низький	1.1. Наявність пропорційного технічного контролю для управління ризиками, які загрожують безпеці обслуговування, захисту конфіденційності, цілісності та доступності інформації, що оброблюється в інформаційно-комунікаційній системі. 1.2. Канали зв’язку, які використовуються для обміну персональними даними та вразливою інформацією, захищено від несанкціонованого ознайомлення, модифікації та повторного відтворення інформації. 1.3. Доступ до вразливої ключової інформації (криптографічного матеріалу), якщо така (такий) використовується для випуску засобів електронної		

		ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, обмежено програмами, які чітко вимагають доступу залежно від кола посадових обов'язків. Забезпечується зберігання такого матеріалу у встановленому законодавством порядку. 1.4. Існують формалізовані процедури, які забезпечують підтримку безпеки впродовж визначеного терміну і можливість реагувати на зміни рівнів ризику, інциденти та порушення безпеки. 1.5. Усі засоби, що містять персональні дані, ключову інформацію (криптографічний матеріал) або іншу вразливу інформацію, зберігаються, передаються та знищуються у встановлений законодавством спосіб.		
2	Середній	2.1. Такі самі, як для низького рівня довіри. 2.2. Вразливу ключову інформацію (криптографічний матеріал), якщо така (такий) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, захищено від несанкціонованого доступу та копіювання.		
3	Високий	3.1. Такі самі, як для низького рівня довіри. 3.2. Вразлива ключова інформація (криптографічний матеріал), яка (який) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної 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.		

7. Технічний контроль				
1	Низький	1.1. Наявність пропорційного технічного контролю для управління ризиками, які загрожують безпеці обслуговування, захисту конфіденційності, цілісності та доступності інформації, що оброблюється в інформаційно-комунікаційній системі. 1.2. Канали зв'язку, які використовуються для обміну персональними даними та вразливою інформацією, захищено від несанкціонованого ознайомлення, модифікації та повторного відтворення інформації. 1.3. Доступ до вразливої ключової інформації (криптографічного матеріалу), якщо така (такий) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, обмежено програмами, які чітко вимагають доступу залежно від кола посадових обов'язків. Забезпечується зберігання такого матеріалу у встановленому законодавством порядку. 1.4. Існують формалізовані процедури, які забезпечують підтримку безпеки впродовж визначеного терміну і можливість реагувати на зміни рівнів ризику, інциденти та порушення безпеки. 1.5. Усі засоби, що містять персональні дані, ключову інформацію (криптографічний матеріал) або іншу вразливу інформацію, зберігаються, передаються та знищуються у встановлений законодавством спосіб.		
2	Середній	2.1. Такі самі, як для низького рівня довіри. 2.2. Вразливу ключову інформацію (криптографічний матеріал), якщо така (такий) використовується для випуску засобів електронної ідентифікації та в інших сегментах		

		інформаційно-комунікаційної системи схеми електронної ідентифікації, захищено від несанкціонованого доступу та копіювання.		
3	Високий	3.1. Такі самі, як для низького рівня довіри. 3.2. Вразлива ключова інформація (криптографічний матеріал), яка (який) використовується для випуску засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної 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.		
8. Відповідність вимогам та аудит				
1	Низький	1.1. Проведення внутрішніх аудитів інформаційної безпеки, які охоплюють усі сегменти інформаційно-комунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання встановлених вимог, принципів та процедур у визначені строки.		
2	Середній	2.1.Такі самі, як для низького рівня довіри. 2.2. Періодичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-комунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання прийнятих вимог, принципів та процедур.		
3	Високий	3.1. Систематичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові		

		інформаційно-комунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання встановлених вимог, принципів та процедур. 3.2. Проведення заходів державного контролю за станом технічного та криптографічного захисту інформації в інформаційно-комунікаційній системі схеми електронної ідентифікації.		

* Для однозначного підтвердження електронної ідентифікації інформаційних або інформаційно-комунікаційних 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.

** Адміністратори систем – юридичні особи, фізичні особи – підприємці, що здійснюють технічне та технологічне забезпечення функціонування інформаційно-комунікаційних систем.

Директор директорату
розвитку цифровізації

Анастасія ХАЛЄЄВА