ЗАТВЕРДЖЕНО

Наказ Міністерства цифрової

трансформації України

\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 року № \_\_\_\_

**ВИМОГИ**

**до засобів електронної ідентифікації, рівнів** **довіри до засобів електронної ідентифікації, що встановлюються схемами електронної ідентифікації для сфери електронного урядування**

**І. 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 постачальниками послуг з електронної ідентифікації, 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;

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 – 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-комунікаційних системах, власниками та/або держателями яких визначено такі органи та особи, та які забезпечують однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

електронне урядування ‒ форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів влади та органів місцевого самоврядування з використанням інформаційно-комунікаційних систем за допомогою яких надаються електронні публічні послуги, електронні сервіси, здійснюється відправлення і отримання електронних даних, зокрема для отримання електронних відображень інформації, що міститься у документах;

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, яка виконується за допомогою формування словника хеш-значень, що використовуються під час автентифікації;

користувачі ‒ власники засобів електронної ідентифікації, які отримують послуги електронної ідентифікації у постачальників таких послуг;

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-комунікаційні 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, із застосовуванням локальних обчислювальних мереж для розподілу обчислень при проведенні таких атак.

ризики інформаційної безпеки – наслідки при автентифікації та/абонеправильному 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 особи − довірений суб’єкт, який встановлює та/або підтверджує особу для системи управління записами;

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

фактор автентифікації ‒ ознака на основі знань (володіння інформацією (даними), що відома лише користувачу), володінь (застосування матеріального предмета, яким володіє лише користувач), властивостей (перевірка біометричних даних або інших властивостей (рис, характеристик), характерних лише користувачу, що відрізняють його від інших користувачів).

Термін «постачальник послуг з електронної ідентифікації» вживається у значенні, наведеному у Положенні про інтегровану систему електронної ідентифікації, затвердженому постановою Кабінету Міністрів України від 19 червня 2019 року № 546.

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 1. 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 фізичної властивості – фактор автентифікації, зв’язок якого із особою встановлюється за результатом підтвердження наявності фізичного атрибуту в особи фактору автентифікації.

5. Електронна взаємодія фізичних та юридичних осіб, а також їх автентифікація здійснюється відповідно до абзацу першого частини другої статті 17 Закону України «Про електронні довірчі послуги».

В інших випадках електронна ідентифікація фізичних осіб, юридичних осіб або представників юридичних осіб в інформаційно-комунікаційних 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-комунікаційних 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 статтею 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-комунікаційних 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 автентифікації 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, 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 (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 – нерезидентів;

2) для юридичних осіб:

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

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;

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-комунікаційними системами сфери електронного урядування та можуть містити такі відомості:

1) для фізичних осіб:

уповноважений суб’єкт, що видав паспорт або інший документ, що посвідчує особу (код);

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 (місце перебування);

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-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.

**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 статтею 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.

**В.о. директора директорату**

**розвитку цифровізації Аліна Куц-Карпенко**