

ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від _____ 2023 р. № _____

ТЕХНІЧНИЙ РЕГЛАМЕНТ

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

Загальна частина

1. Цей Технічний регламент встановлює вимоги до використання засобів електронної ідентифікації в контексті схеми електронної ідентифікації залежно від рівнів довіри до засобів електронної ідентифікації.

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

2. Дія цього Технічного регламенту поширюється на:

надавачів послуг електронної ідентифікації;

підприємства, 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, фізичним особам – підприємцям, юридичним особам або уповноваженим представникам юридичних осіб, та використовуються для автентифікації у сфері електронного урядування.

Дія цього Технічного регламенту не поширюється на надання послуг електронної ідентифікації відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

3. У цьому Технічному регламенті терміни вживаються у таких значеннях:

активація – процес, за допомогою якого обліковий запис або засоби для підтвердження 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 – 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-яка подія (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами криптографічного захисту інформації, що призвела або 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 надавачів таких послуг;

порушник з базовим потенціалом – суб'єкт, який може навмисно чи ненавмисно здійснити несанкціоновані дії щодо інформації в системі, а також 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 – суб'єкт, який може навмисно чи ненавмисно здійснити несанкціоновані дії щодо інформації в системі, а також має науково-технічний ресурс, що прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави;

порушник з середнім потенціалом – суб'єкт корпоративного типу, який може навмисно чи ненавмисно здійснити несанкціоновані дії щодо інформації в системі, а також 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/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 реєстрацію 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.

Інші терміни вживаються у значеннях, наведених у законах України «Про електронну ідентифікацію та електронні довірчі послуги», «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», «Про технічні регламенти та оцінку відповідності», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», у національному стандарті ДСТУ ISO/IEC 29115:2015 (ISO/IEC 29115:2013, IDT) «Інформаційні технології. Методи захисту. Структура гарантування автентифікації об'єктів», затвердженому наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 18 грудня 2015 № 193, 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», затвердженому наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 4 серпня 2017 р. № 207.

4. Фактор автентифікації поділяється на такі групи:

фактор автентифікації, зв'язок якого із особою встановлюється за результатом підтвердження знання інформацією, даними фактора автентифікації особи;

фактор автентифікації, зв'язок якого із особою встановлюється за результатом підтвердження володіння матеріальним предметом фактора автентифікації особи;

фактор автентифікації, зв'язок якого із особою встановлюється за результатом підтвердження біометричних даних наявності фізичного фактора автентифікації особи.

5. Електронна взаємодія здійснюється відповідно до частини першої статті 17 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

В інших випадках електронна ідентифікація фізичних, фізичних осіб – підприємців, юридичних осіб або уповноважених 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 електронній формі.

7. Для визначення відповідності рівнів довіри до засобів електронної ідентифікації критеріям, передбаченим статтею 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», у пунктах 14, 15 цього Технічного регламенту 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 цим Технічним регламентом. 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.

Набори ідентифікаційних даних для сфери електронного урядування

10. Для автентифікації фізичної, фізичної особи – підприємця, юридичної особи або уповноваженого представника юридичної особи під час електронної взаємодії у сфері електронного урядування підприємства, 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, фізичним особам – підприємцям, юридичним особам або уповноваженим представникам юридичних осіб, мають використовувати обов'язкові та додаткові набори ідентифікаційних даних, визначені у пунктах 11-13 цього Технічного регламенту.

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

1) для 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 (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 (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) 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;

3) для уповноважених 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, уповноваженим представником якої є фізична особа.

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

1) для фізичних осіб, фізичних осіб – підприємців:

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 на здійснення діяльності у певній сфері;

місце народження;

місце проживання (місце перебування);

2) для юридичних осіб, фізичних осіб – підприємців:

місцезнаходження згідно з Єдиним державним реєстром;

3) для уповноважених представників юридичних осіб:

місцезнаходження юридичної особи згідно з Єдиним державним реєстром, уповноваженим представником якої є фізична особа.

13. 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 підприємства, 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.

Технічні специфікації та процедури

14. Елементи технічних специфікацій та процедур, наведені у пункті 15 цього Технічного регламенту мають використовуватись для встановлення відповідності рівнів довіри до засобів електронної ідентифікації критеріям, передбаченим статтею 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», до засобів електронної ідентифікації, виданих відповідно до схеми електронної ідентифікації.

15. Елементи технічних специфікацій та процедур до:

реєстрації користувачів засобів електронної ідентифікації наведені у додатку 1 до цього Технічного регламенту;

управління засобами електронної ідентифікації наведені у додатку 2 до цього Технічного регламенту;

автентифікації наведені у додатку 3 до цього Технічного регламенту;

управління та організації наведені у додатку 4 до цього Технічного регламенту.

Таблиця відповідності

16. Таблиця відповідності положень Імплементаційного регламенту комісії (ЄС) 2015/1502 від 8 вересня 2015 року про встановлення мінімальних технічних специфікацій та процедур для рівнів надійності засобів електронної ідентифікації відповідно до статті 8(3) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та цього Технічного регламенту наведена у додатку 5 до цього Технічного регламенту.
