ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від ____ _____ 2023 р. № _____

ПОЛОЖЕННЯ
про інтегровану систему електронної ідентифікації

Загальні питання

1. Це Положення визначає порядок призначення, визначення структури, функціонування інтегрованої системи електронної ідентифікації (далі – система), її створення та використання.

2. У цьому Положенні терміни вживаються у такому значенні:

електронний сервіс (сервіс) – ідентифіковане за веб-адресою програмне забезпечення, що здійснює взаємодію інформаційних систем під час обміну даними, необхідними для надання електронних послуг, і має стандартизовані інтерфейси;

інтегрована система електронної ідентифікації – це інформаційно-комунікаційна система, призначена для технологічного забезпечення зручної, доступної та безпечної електронної ідентифікації та автентифікації її користувачів, сумісності та інтеграції схем електронної ідентифікації, їх взаємодії з інформаційними та інформаційно-комунікаційними системами органів державної влади, органів місцевого самоврядування, юридичних осіб, фізичних осіб – підприємців та осіб, які провадять незалежну професійну діяльність, забезпечення захисту інформації та персональних даних з використанням єдиних вимог, форматів, протоколів та класифікаторів, а також задоволення інших потреб, визначених законодавством;

користувачі системи – фізичні та юридичні особи, фізичні особи – підприємці, які звертаються до інформаційно-комунікаційних систем суб'єктів взаємодії та проходять електронну ідентифікацію за допомогою системи з використанням засобів електронної ідентифікації, функціонування яких забезпечується системою;

маркер (ідентифікатор) доступу – об'єкт з унікальним атрибутом, що визначає повноваження суб'єкта взаємодії для доступу до інформаційного ресурсу;

програмний інтерфейс – набір визначених підпрограм та протоколів обміну інформацією для взаємодії різних програмних компонентів;

протокол визначення статусу сертифіката – протокол обміну інформацією під час інтерактивного визначення статусу сертифіката відкритого ключа за запитами користувачів системи;

протокол обміну інформацією – перелік форматів переданих блоків даних, набір правил їх обробки і правил взаємодії інформаційно-комунікаційних систем на одному рівні;

протокол управління сертифікатом – протокол обміну інформацією під час інтерактивного отримання сертифіката та відомостей про його статус за запитами користувачів системи;

транскордонна електронна ідентифікація – електронна ідентифікація користувачів системи, які розташовані в іншій країні, ніж надавач послуг електронної ідентифікації;

прикладний програмний інтерфейс – інтерфейс програмування, призначений для підключення інформаційно-комунікаційних систем суб'єктів взаємодії до інтегрованої системи електронної ідентифікації.

Інші терміни вживаються у значенні, наведеному в Законах України "Про інформацію", "Про Національну програму інформатизації", "Про захист інформації в інформаційно-комунікаційних системах", "Про електронні комунікації", "Про захист персональних даних", "Про електронну ідентифікацію та електронні довірчі послуги", "Про основні засади забезпечення кібербезпеки України", "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус", "Про публічні електронні реєстри".

Це Положення не поширюється на здійснення електронної ідентифікації відповідно до положень абзацу другого частини першої статті 2 Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

3. Метою системи є забезпечення відповідно до схем електронної ідентифікації доступу користувачів системи до електронних послуг, які надаються органами державної влади, органами місцевого самоврядування, юридичними особами і фізичними особами – підприємцями, та їх сервісів, функціонування електронного документообігу, провадження іншої діяльності із застосуванням електронної ідентифікації.

4. Система є складовою частиною інформаційно-комунікаційної інфраструктури, що забезпечує електронну взаємодію суб'єктів взаємодії з користувачами системи та забезпечує:

проведення регламентних процедур та електронної ідентифікації користувачів системи для отримання ними електронних послуг, доступу до сервісів;

взаємодію та сумісність з інформаційно-комунікаційними системами, які реалізують схеми електронної ідентифікації, та інформаційно-комунікаційними системами;

дотримання вимог законодавства щодо захисту інформації та персональних даних;

розвиток системи у напрямі приєднання до інформаційно-комунікаційних систем для транскордонної електронної ідентифікації;

приєднання інформаційно-комунікаційних систем суб'єктів взаємодії до системи.

5. Власником системи є держава в особі Мінцифри.

Держателем системи є Мінцифри (далі – держатель системи).

Володільцем інформації, що обробляється в системі, є держатель системи.

Держатель системи:

приймає взаємоузгоджені управлінські рішення стосовно подальшого розвитку та вдосконалення системи;

здійснює контроль за дотриманням суб'єктами взаємодії вимог законодавства щодо використання інформаційних ресурсів;

здійснює методичне та методологічне забезпечення функціонування системи;

проводить систематичний моніторинг та аналіз ефективності функціонування системи;

організовує приєднання державних інформаційних систем до системи;

проводить аналіз структури та змісту інформаційних ресурсів системи з метою підвищення рівня інформаційної взаємодії її суб'єктів.

6. Адміністратором та технічним адміністратором системи (далі – адміністратор) є державне підприємство «ДІЯ».

7. Адміністратор здійснює технічне та технологічне забезпечення виконання таких функцій:

функціонування інтегрованої системи електронної ідентифікації та захисту інформації, що в ній обробляється, відповідно до вимог законодавства;

функціонування офіційного веб-сайту інтегрованої системи електронної ідентифікації;

функціонування на офіційному веб-сайті інтегрованої системи електронної ідентифікації електронного сервісу, призначеного для створення, перевірки та підтвердження електронного підпису та електронної печатки;

використання інтегрованої системи електронної ідентифікації для взаємного визнання схем електронної ідентифікації;

обробка та публікація результатів аналізу поточного стану та перспектив розвитку у сферах електронної ідентифікації та електронних довірчих послуг;

формування, підтримка в актуальному стані та публікація на веб-сайті інтегрованої системи електронної ідентифікації переліку схем електронної ідентифікації;

укладання договорів щодо приєднання інформаційних та інформаційно-комунікаційних систем до інтегрованої системи електронної ідентифікації.

8. Адміністратор відповідно до визначених функцій:

1) забезпечує:

створення, модернізацію та розвиток, адміністрування і забезпечення функціонування системи, впровадження комплексної системи захисту інформації з підтвердженою відповідністю;

електронну взаємодію користувачів системи, суб'єктів та об'єктів взаємодії;

здійснення заходів щодо захисту системи;

доступ суб'єктів взаємодії до системи відповідно до цього Положення;

збереження інформації, що обробляється в системі;

2) здійснює:

модернізацію програмного забезпечення системи;

позбавлення доступу суб'єктів взаємодії до системи відповідно до законодавства;

ведення електронного обліку суб'єктів взаємодії, які приєднані до системи, з фіксуванням відомостей про дату і час отримання доступу, обсяг інформації, до якої отримано доступ;

технічну та інформаційну підтримку суб'єктів взаємодії та користувачів системи за допомогою веб-ресурсів, телефонного інформаційного центру тощо;

3) проводить:

постійний моніторинг технічного стану системи;

навчання суб'єктів взаємодії та користувачів системи під час її функціонування та удосконалення;

4) здійснює інші заходи, пов'язані з функціонуванням системи.

9. Суб'єктами взаємодії є:

органи державної влади, органи місцевого самоврядування, їх посадові особи;

юридичні особи і фізичні особи – підприємці;

надавачі електронних довірчих послуг та надавачі послуг електронної ідентифікації;

адміністратори проміжних вузлів електронної ідентифікації (хабів);

адміністратор;

держатель системи.

10. Об’єктами взаємодії є:

засоби електронної ідентифікації в контексті схем електронної ідентифікації, які використовують користувачі системи для здійснення процедур електронної ідентифікації;

інформаційно-комунікаційні системи органів державної влади, органів місцевого самоврядування;

інформаційно-комунікаційні системи юридичних осіб і фізичних осіб – підприємців;

інформаційно-комунікаційні системи, які реалізують схеми електронної ідентифікації;

інформаційно-комунікаційні системи, які реалізують схеми електронної ідентифікації в рамках транскордонної електронної ідентифікації.

11. Система функціонує цілодобово сім днів на тиждень.

12. Доступ до системи здійснюється через відкритий інформаційний ресурс, який має офіційну адресу в Інтернеті (https://id.gov.ua).

13. Обробка та захист інформації в системі здійснюються відповідно до вимог Законів України “Про захист персональних даних”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, а також інших нормативно-правових актів.

Суб’єкти взаємодії здійснюють обробку і забезпечують захист персональних даних користувачів системи, а також фізичних і юридичних осіб, фізичних осіб – підприємців, відомості щодо яких отримуються та верифікуються за допомогою системи, у власних інформаційно-комунікаційних системах відповідно до вимог законодавства України про захист персональних даних.

Завдання та функціональні можливості системи

14. Завданнями системи є:

створення сучасної інфраструктури електронної ідентифікації в Україні та забезпечення її сталого розвитку;

забезпечення інтероперабельності (технологічної сумісності) засобів електронної ідентифікації, проміжних вузлів електронної ідентифікації (хабів) та схем електронної ідентифікації;

створення довірчого середовища у кіберпросторі України та мотивування суб’єктів взаємодії та користувачів системи до використання електронних послуг;

захист інформаційних ресурсів, які обробляються в системі.

15. Функціональні можливості системи забезпечують:

захист даних від несанкціонованого доступу, знищення, модифікації шляхом здійснення організаційних і технічних заходів, упровадження засобів та методів технічного захисту інформації;

розмежування та здійснення контролю за доступом користувачів та суб'єктів взаємодії до інформації;

реєстрацію подій, що стосуються безпеки системи;

наявність зрозумілих для суб'єктів взаємодії та користувачів системи програмних інтерфейсів;

електронну ідентифікацію та автентифікацію користувачів та суб'єктів взаємодії, створення та перевірку кваліфікованого електронного підпису;

отримання та передачу відомостей щодо користувачів системи з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань;

верифікацію з використанням інформації Єдиного державного демографічного реєстру відомостей щодо користувачів системи;

отримання та передачу відомостей про викрадені (втрачені) документи за зверненнями громадян з єдиної інформаційної системи МВС для встановлення факту втрати або викрадення паспортів громадянина України;

верифікацію реєстраційних даних щодо користувачів системи з Державного реєстру фізичних осіб – платників податків;

використання інформації з інших публічних електронних реєстрів, в тому числі верифікацію відомостей про смерть з Державного реєстру актів цивільного стану громадян;

електронну інформаційну взаємодію з публічними електронними реєстрами відповідно до Закону України «Про публічні електронні реєстри», зазначеними в цьому пункті.

16. Доступ суб'єктів взаємодії до системи надається на підставі договору, укладеного з адміністратором системи з урахуванням частини четвертої статті 15^3 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

17. Суб'єкти взаємодії використовують прикладні програмні інтерфейси, доступ до яких надає адміністратор.

18. Система має функціональні можливості для електронної комунікації в режимі реального часу користувачів системи та суб'єктів взаємодії.

Структура системи

19. Система розміщується на програмно-апаратному комплексі держателя системи та адміністратора системи.

Програмно-апаратні комплекси (основний та резервний) і технічні засоби системи розміщуються у приміщеннях держателя системи, адміністратора або іншому приміщенні на підставі договору, укладеного з власником приміщення, з дотриманням вимог щодо захисту інформації.

20. Система створюється із забезпеченням технологічної сумісності та взаємодії з іншими інформаційними системами та мережами і забезпечує можливість отримання ідентифікаційних даних із засобів електронної ідентифікації, виданих у різних схемах електронної ідентифікації.

21. Система складається з:

підсистеми взаємодії із схемами електронної ідентифікації кваліфікованих надавачів електронних довірчих послуг;

підсистем взаємодії із схемами електронної ідентифікації;

підсистеми верифікації відомостей щодо фізичних і юридичних осіб, фізичних осіб – підприємців, які є користувачами системи;

підсистеми управління;

комплексної системи захисту інформації.

Функції підсистем

22. Підсистема взаємодії із схемами електронної ідентифікації кваліфікованих надавачів електронних довірчих послуг забезпечує виконання таких функцій:

автентифікацію інформаційно-комунікаційних систем суб’єктів взаємодії;

автентифікацію кваліфікованих надавачів електронних довірчих послуг;

автентифікацію користувачів системи, які звертаються до інформаційно-комунікаційних систем, з використанням особистих ключів та кваліфікованих сертифікатів відкритих ключів за запитами інформаційно-комунікаційних систем;

захищений обмін інформацією з інформаційно-комунікаційними системами кваліфікованих надавачів електронних довірчих послуг;

передачу ідентифікаційних даних користувачів системи, які успішно пройшли автентифікацію, до інформаційно-комунікаційних систем;

взаємодію з кваліфікованими надавачами електронних довірчих послуг за протоколами визначення статусу сертифікатів та додатково за протоколом управління сертифікатами.

23. Підсистеми взаємодії із схемами електронної ідентифікації забезпечують виконання таких функцій:

автентифікацію інформаційно-комунікаційних систем суб’єктів взаємодії;

автентифікацію інформаційно-комунікаційних систем схем електронної ідентифікації;

автентифікацію користувачів системи, які звертаються до інформаційно-комунікаційних систем, з використанням засобів електронної ідентифікації за запитами інформаційно-комунікаційних систем;

захищений обмін інформацією із схемами електронної ідентифікації;

передачу ідентифікаційних даних користувачів системи, які успішно пройшли автентифікацію за допомогою схем електронної ідентифікації, до інформаційно-комунікаційних систем надання електронних послуг;

взаємодію з кваліфікованими надавачами електронних довірчих послуг.

24. Підсистема верифікації відомостей щодо фізичних і юридичних осіб, фізичних осіб – підприємців, які є користувачами системи, забезпечує:

отримання та передачу відомостей щодо користувачів системи з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань;

верифікацію з використанням інформації Єдиного державного демографічного реєстру відомостей щодо користувачів системи;

отримання та передачу відомостей про викрадені (втрачені) документи за зверненнями громадян з єдиної інформаційної системи МВС для встановлення факту втрати або викрадення паспортів громадянина України;

отримання та передачу відомостей щодо користувачів системи з Державного реєстру фізичних осіб – платників податків.

25. Підсистема управління забезпечує виконання таких функцій:

надання програмних інтерфейсів взаємодії, маркерів (ідентифікаторів) доступу та забезпечення управління потоками цифрових даних між суб’єктами взаємодії;

управління технічними ресурсами системи;

управління засобами електроживлення та життєзабезпечення;

реєстрацію подій в системі та сповіщення про виникнення аварійної ситуації.

Вимоги до захисту інформації, яка обробляється в системі

26. Інформація, яка обробляється в системі, повинна бути захищена відповідно до вимог законодавства у сфері захисту інформації.

27. Захист інформації, яка оброблюється в системі, забезпечується комплексною системою захисту інформації системи з підтвердженою відповідністю.

28. Комплексна система захисту інформації системи повинна забезпечувати виконання таких основних функцій:

розмежування доступу користувачів системи та суб'єктів взаємодії до захищених ресурсів системи;

регламентацію дій користувачів системи та суб'єктів взаємодії під час доступу та обробки захищених ресурсів системи;

ідентифікацію та автентифікацію користувачів системи та суб'єктів взаємодії, у тому числі під час транскордонної електронної ідентифікації;

перевірку повноважень користувачів системи та суб'єктів взаємодії і надання їм права на виконання певних дій з обробки захищених ресурсів;

реєстрацію подій, пов'язаних з доступом до захищених ресурсів системи, результатів ідентифікації та автентифікації користувачів системи та суб'єктів взаємодії, фактів зміни повноважень користувачів системи та суб'єктів взаємодії, результатів перевірки цілісності засобів захисту інформації, транскордонної електронної ідентифікації тощо;

блокування несанкціонованих дій щодо захищених ресурсів системи;

захист захищених ресурсів системи під час їх передачі через незахищене середовище;

захист системи від мережевих атак з Інтернету;

антивірусний захист інформації, яка обробляється в системи;

цілісність програмного забезпечення, яке використовується для обробки захищених ресурсів системи.

29. Робоча документація щодо комплексу засобів захисту від несанкціонованого доступу повинна містити описи таких процедур:

інсталяції та ініціалізації комплексу;

налагодження всіх механізмів розмежування доступу користувачів системи та суб'єктів взаємодії до інформації та апаратних ресурсів системи;

здійснення контролю за діями користувачів системи та суб'єктів взаємодії;

формування та актуалізації баз даних захисту;

здійснення контролю за цілісністю програмного забезпечення і баз даних захисту.

30. Забезпечення конфіденційності, цілісності і доступності інформації, яка обробляється в системі, розмежування доступу користувачів системи та суб'єктів взаємодії до захищених ресурсів системи здійснюється згідно з планом захисту інформації в системі.

31. Організація та проведення робіт із захисту інформації в системі здійснюються службою захисту інформації, яка визначає вимоги до захисту інформації в системі, проектує, розробляє та модернізує комплексну систему захисту інформації, а також виконує роботи з її експлуатації та контролює стан захищеності інформації.

32. Функції служби захисту інформації покладаються на адміністратора.

33. Фінансове забезпечення заходів, пов'язаних із створенням, модернізацією, розвитком системи, а також адмініструванням, супроводженням та технічним обслуговуванням, здійснюється за рахунок коштів державного бюджету, а також коштів міжнародної технічної допомоги та інших джерел, не заборонених законодавством.

Фінансове забезпечення адміністратора інтегрованої системи електронної ідентифікації для технічного та технологічного виконання функцій, визначених статтею 7^1 Закону України "Про електронну ідентифікацію та електронні довірчі послуги", здійснюється за рахунок коштів державного бюджету.
