НАЦІОНАЛЬНА СТРАТЕГІЯ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ УКРАЇНИ

Біла книга з електронного урядування

Під редакцією О. Потія та Ю. Козлова

ЗМІСТ

ВСТУП

Біла книга – документ, який використовується урядами для проведення публічних консультацій щодо пропонованого змісту політики на останньому етапі її розробки. Вона описує конкретні цілі та інструменти державної політики у відповідній сфері як задля інформування суспільства про деталізовані наміри уряду, так і з метою виявлення розбіжності у позиціях різних зацікавлених сторін щодо змісту пропонованої політики. За результатами обговорення Білої книги готується остаточне рішення щодо державної політики у відповідній сфері, яке згодом реалізується у низці нормативно-правових актів (законах, постановах, наказах тощо), стратегій, програм та інших рішень центральних та місцевих органів виконавчої влади.

Біла книга «Національна стратегія електронної ідентифікації України» є публічно доступним документом, який є продовженням Зеленої книги електронного урядування України[1] розроблюється за участю українських та міжнародних експертів галузі електронного урядування.

Терміни

У цьому документі за основу взято терміни Регламенту ЄС №910/2014 Європейського Парламенту та Ради від 23 липня 2014 «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЄС»[2], які вживаються у такому значенні:

(1) "електронна ідентифікація" - процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну або юридичну особу або фізичну особу, що представляє юридичну особу;

(2) "засіб електронної ідентифікації"- матеріальний, та/або нематеріальний елемент, який містить ідентифікаційні дані особи і використовується для автентифікації в он-лайн послугах;

(3) "ідентифікаційні дані особи" - набір даних, який дозволяє встановити ідентичність фізичної або юридичної особи, або фізичної особи, яка представляє юридичну особу;

(4) "ідентифікатор" - унікальний атрибут, який дозволяє встановити ідентичність фізичної або юридичної особи;

---

[1] http://etransformation.org.ua

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

(5) "схема електронної ідентифікації" - система електронної ідентифікації, в якій засоби електронної ідентифікації видаються особам, які зазначені в пункті (1);

(6) "автентифікація" - електронний процес, що дозволяє підтвердити електронну ідентифікацію фізичної або юридичної особи; або походження та цілісність електронних даних;

(7) "сторона, яка довіряє" - фізична або юридична особа, яка покладається на електронну ідентифікацію;

(8) "гарантія електронної ідентифікації" - ступінь довіри, отриманий в ході автентифікації, до того, що фізична або юридична особа є тією, яка вона є за її ствердженням, або тією, на яку очікується.

Інші терміни вживаються у значеннях міжнародних стандартів та рекомендацій, та які для зручності використання винесено в окремий Додаток А до цього документу.

Передумови підготовки документу

Після громадсько-політичних подій кінця 2013 - початку 2014 року, обрання нового Президента України у травні 2014 року та парламентських виборів у жовтні 2014 року, новостворений Уряд України активно проводить програму реформ, які спрямовують країну шляхом європейської інтеграції до відкритої та прозорої демократії.

Серед головних пріоритетів реформи є децентралізація, боротьба з корупцією, відкриті принципи державного управління, прозорість, підзвітність і ефективність влади. Електронне урядування визначено в якості одного з найважливіших інструментів для досягнення цих цілей. У червні 2014 року, уряд України утворив Державне агентство з питань електронного урядування України (Агентство) при Міністерстві регіонального розвитку, будівництва та житлово-комунального господарства України. Головним завданням Агентства визначено реалізацію державної політики у сфері електронного урядування, що передбачає комплексний підхід до розбудови та розвитку цієї сфери.

Першим кроком, зробленим Агентством, стало внесення на розгляд громадськості проекту Зеленої книги електронного урядування України в листопаді 2014 року. Зелена книга розглядається як запрошення урядом широкого кола зацікавлених сторін до публічного обговорення, подальшого уточнення у формі

консультативного процесу і розробки остаточної політики у сфері електронного урядування, включаючи цілий ряд публічних форумів та інших механізмів популяризації.

Зелена книга електронного урядування України розроблялась за участі широкого кола зацікавлених сторін, що включає політиків, чиновників усіх рівнів (центрального, обласного, районного та місцевого), представників сфери інформаційно-комунікаційних технологій та інших галузей, наукового співтовариства, громадських неурядових організацій. Процес консультацій з громадськістю передбачав проведення інтерактивних консультації через соціальні медіа-канали.

Паралельно з процесом консультацій щодо Зеленої книги (і беручи до уваги результати консультативного процесу), започатковано розробку пакету Білих книг. Біла книга є документом, що містить державні політичні пріоритети та передує прийняттю актів законодавства. Білі Книги з електронного урядування будуть охоплювати різні напрями реалізації державної політики в сфері інформатизації, в тому числі надання електронних послуг, доступ до публічної інформації у форматі відкритих даних, інтероперабельність і стандартизація та електронна демократія.

Після прийняття Білих книг зацікавленими сторонами, Агентством будуть підготовлені та через Уряд представлені на розгляд Парламенту законопроекти (зміни до існуючих та нові закони).

Крім того, передбачається розробка та прийняття нормативно-правових актів Уряду, профільних міністерств та відомств, які в тій чи іншій мірі нестимуть відповідальність за безпосередню реалізацію прийнятих законодавчих актів.

Передбачається, що паралельно з процесом розробки Білих книг, буде розроблюватись План дій щодо реалізації електронного урядування у форматі Державної цільової програми на 2015-2020 роки, яка виступить в якості основного документа планування діяльності.

Мета підготовки документу

Впровадження сучасних засобів та схем електронної ідентифікації в Україні із забезпеченням високого рівня гарантій електронної ідентифікації, відкриває можливості для громадян та жителів України на новому якісному рівні здійснювати взаємодію з державними та місцевими органами влади та отримувати електронні

адміністративні послуги, що являє собою одне із основних завдань для Уряду України у впровадженні електронного урядування[3].

Обраний державою курс на євроінтеграцію однозначно передбачає таке впровадження у відповідності до нормативних актів, стандартів та процедур, прийнятих в країнах Європейського Союзу як загальні для всіх держав-членів. Тому впровадження сучасних засобів та схем електронної ідентифікації потребує детального аналізу різних аспектів стану та трендів галузі як в Україні, так і в державах-членах Європейського Союзу.

Такий аналіз повинен надати можливості обрати оптимальний варіант вирішення завдання із побудови нормативно-правового та технологічного підґрунтя для схем електронної ідентифікації, що будуть використовуватись як у сфері електронного урядування під час взаємодії громадян з органами влади, так і у сфері взаємодії громадян із бізнесом та суб'єктів бізнесу у своєму середовищі.

Більш того, однією із ключових цілей розробки Білої книги постає питання висвітлення аспектів забезпечення правової, організаційної, семантичної та технологічної сумісності (інтероперабельності) створюваних схем електронної ідентифікації та процесів, пов'язаних з їх використанням, як на території України, так і в крос-кордонному просторі.

Покладаючись на розуміння виникнення не тільки політичного, економічного, юридичного та науково-технологічного ефектів від впровадження сучасних засобів та схем електронної ідентифікації в Україні, слід пам'ятати також і про соціальні та психологічні аспекти підготовки до такого впровадження, пов'язані із ставленням суспільства до питань електронної взаємодії із державою взагалі, бажанням мати додаткові засоби, які ідентифікують громадян, втрачати час та, можливо, й кошти на їх отримання тощо.

Усвідомлюючи необхідність спрямування зусиль на досягнення кінцевого результату, автори Білої книги передбачають визначення переліку та значень показників очікуваного результату та ефективності реалізації проекту, блоків завдань та заходів, спрямованих на досягнення кожного із показників, прогнозованих строків виконання проекту із розрахунком на певні фінансові, матеріально-технічні та трудові ресурси.

[3] http://zakon2.rada.gov.ua/laws/show/26-19

Врахування цих та інших контекстів, що містяться в Білій книзі, повинно надати можливість побудови «дорожньої карти», яки по суті є планом-графіком проекту у разі його схвалення. При цьому така дорожня карта повинна враховувати вимоги чинного законодавства щодо прийняття проекту такого масштабу на рівні Уряду після його узгодження із профільними установами та пройти відповідні громадські обговорення.

Резюме

Біла книга «Національна стратегія електронної ідентифікації України» передбачає своїм існуванням надання одного із інструментів державної політики у сфері електронного урядування із пропозиціями щодо її практичної реалізації шляхом виконання конкретних завдань та заходів у певні строки визначеним колом суб'єктів.

ОСНОВНА ЧАСТИНА

1. Опис проблеми

1.1. Формулювання проблеми

Протягом років незалежності України різними урядами країни та каденціями органів місцевого самоврядування здійснювались заходи щодо створення тих або інших інформаційних систем загальнодержавного або місцевого масштабу для надання адміністративних послуг в електронному вигляді.

Надання таких послуг передбачає он-лайн взаємодію між громадянином та органом, що надає послугу через певні інтерфейси інформаційної системи з використанням механізмів електронної ідентифікації та автентифікації, які мають бути засновані на принципах безпеки та гарантій впевненості в ідентичності обох сторін такої взаємодії.

«Для отримання багатьох послуг дуже важливо визначити та встановити фізичну або юридичну особу, якій надається відповідна послуга. Технології електронної ідентифікації та сервіси із встановлення особи є дуже важливими для забезпечення безпеки електронних транзакцій (як у державному, так і в приватному секторі). Нині найбільш розповсюдженим способом автентифікації є використання паролів, але потреба у розробці більш безпечних рішень, які будуть захищати приватність, є очевидною. Необхідно налагодити більш ефективну адміністративну співпрацю ... для розробки та започаткування ... державних он-лайн послуг, які в тому числі будуть містити практичні рішення щодо електронної ідентифікації та автентифікації особи».

Наведена цитата з документу «Європейський план дій із електронного урядування на 2011-2015 рр. Використання ІКТ для сприяння інтелектуальному, сталому та інноваційному врядуванню»[4] відображає актуальність проблеми впровадження надійної та безпечної системи електронної ідентифікації для країн Європи.

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF

Вочевидь, що створення такої системи для України також є нагальним з огляду на вектори політичної та економічної інтеграції держави з Європейським Союзом, а також зважаючи на зростаюче проникнення в життя людей інформаційних технологій, цифровізації суспільства та економіки.

Географічні та демографічні показники України, її адміністративно-територіальний та державний устрій, нормативно-правова система, стан економіки та рівень розвитку суспільства вимагають стратегічного підходу та комплексного рішення будь-яких завдань, пов'язаних із впровадженням тих або інших технологій, у тому числі, інформаційних.

Відсутність такого підходу до вирішення питання електронної ідентифікації в Україні призвело до ситуації, коли в інформаційних системах різного призначення та масштабу використовуються засоби та механізми електронної ідентифікації користувачів без урахування таких основних принципів, як безпека, захист персональних даних, достовірність ідентифікації, інтероперабельність та комфортність використання.

Незважаючи на високий відсоток використання таких засобів електронної ідентифікації, як засоби електронного цифрового підпису, в Україні згаданий механізм електронної ідентифікації у самому масовому застосуванні направлений на вирішення здебільшого лише одного завдання - подання електронної звітності суб'єктами підприємництва до фіскальних органів та органів статистики, під час якого електронний цифровий підпис водночас виступає як аналог власноручного на документах звітності.

Другою за обсягами та кількістю користувачів сферою застосування електронного цифрового підпису, як механізму електронної ідентифікації, є системи доступу до державних інформаційних ресурсів та відомчих (корпоративних) мереж. Слід зазначити, що у цьому випадку користувачі таких систем підтверджують свою ідентичність та повноваження здебільшого як посадова особа та як автор електронного документу.

Переваги засобів електронного цифрового підпису, заснованого на алгоритмах криптографії та нормативно закріпленими досить жорсткими процедурами встановлення особи користувача шляхом особистого контакту під час його реєстрації та видання сертифіката, перевірені часом та досвідом. Проте, на сьогодні і у сфері електронного цифрового підпису наявні недоліки організаційного та

технологічного характеру, котрі полягають у відсутності єдиних політик щодо верифікації електронних підписів, визначення часу транзакцій та застосування ідентифікаторів для підтвердження учасника транзакції (суб'єкта електронної ідентифікації), брак інтероперабельності між засобами електронного цифрового підпису різних постачальників тощо.

Банківський сектор, враховуючи загрози хибної ідентифікації, крадіжки та використання чужої ідентичності, ризики фінансових втрат та дискредитації фінансових установ, використовує ґрунтовний підхід до управління електронною ідентифікацією та використання механізмів автентифікації. При цьому, первинна реєстрація користувачів електронних банківських та платіжних послуг здійснюється у відповідності до правил, що передбачають встановлення особи під час особистого контакту. Проте, процедури автентифікації передбачають різні механізми, що варіюються у спектрі від використання пари «логін/пароль» до засобів криптографії.

Поряд з цим, користувачі публічних інформаційних систем у статусі громадянина та представника юридичної особи, постають перед фактом використання менш безпечних механізмів електронної ідентифікації у вигляді пари «логін/пароль». При цьому, в системах, не пов'язаних між собою, відсутні єдині підходи до процедур реєстрації, використання ідентифікаторів, управління обліковими записами та повноваженнями користувачів, захисту їх ідентичності, а користувачам доводиться проходити процедури отримання прав доступу до інформації у відповідності до різних політик.

Також вагомим недоліком відсутності взаємодії між інформаційними системами надання електронних послуг є унеможливлення повторного використання користувачами атрибутів доступу, отриманих в одній системі, для доступу в іншу.

Одним із найгостріших питань надання електронних послуг провайдерами різних сфер на сьогодні постає питання захисту персональних даних споживачів таких послуг. Надання користувачем згоди на обробку його персональних даних під час реєстрації в інформаційній системі, часто використовується як механізм позбавлення від відповідальності власника системи, який формально виконав вимоги Закону України «Про захист персональних даних». Проте, жодним чином не забезпечуються інші вимоги закону щодо обсягів даних про особу, що збираються під час реєстрації, термінів обробки та зберігання таких даних провайдером тощо.

Відсутність єдиної нормативної та технічної політики використання та захисту ідентифікаційних даних користувачів, загальних процедур та алгоритмів автентифікації та захисту інформації в системах, механізмів забезпечення інтероперабельності та ефективної взаємодії інформаційних систем, стає стримуючим чинником для розвитку систем надання он-лайн послуг, зміцнення довіри громадян до таких послуг та до цифрових технологій взагалі, а необхідність подолання таких перешкод вимагає зваженого комплексного підходу до створення в Україні єдиної інфраструктури електронної ідентифікації, інтегрованої до систем електронного урядування, електронної медицини, надання адміністративних послуг в електронній формі, електронної торгівлі тощо.

1.2. Аналіз причин виникнення проблеми та обґрунтування необхідності прийняття змін шляхом розробки та впровадження Стратегії

Причини відсутності в Україні сталої інфраструктури електронної ідентифікації та їх наслідки розглядаються в таких контекстах:

- організаційний контекст;
- нормативно-правовий контекст;
- соціально-економічний контекст;
- технологічний контекст.

Серед основних чинників виникнення проблеми організаційного характеру та наслідків їх дії слід визначити такі:

- відсутність дієвого механізму виконання завдань розвитку інформаційного суспільства, у наслідок чого реалізація органами виконавчої влади плану заходів з виконання завдань, передбачених Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» затвердженого розпорядженням Кабінету Міністрів України від 15 серпня 2007 р. № 653[5], не забезпечила створення умов для розвитку інформаційного суспільства в Україні в цілому та окремих секторів, у тому числі сфери електронної ідентифікації в система надання електронних послуг;

[5] http://zakon4.rada.gov.ua/laws/show/653-2007-%D1%80

– неефективність роботи Міжгалузевої ради з питань розвитку електронного урядування, утвореної відповідно до постанови Кабінету Міністрів України від 14 січня 2009 р. № 4[6], що призвело до відсутності узгоджених дієвих пропозицій Уряду країни щодо реалізації державної політики з питань розвитку електронного урядування та інтеграції України до глобального інформаційного простору;

– низький рівень взаємодії замовників Національної програми інформатизації щодо погодження Генеральним державним замовником Національної програми інформатизації завдань (проектів) створення державними органами інформаційно-телекомунікаційних систем, призначених для надання адміністративних послуг населенню, наслідком чого стало виникнення безсистемності та неузгодженості їх побудови, правової, організаційної та технологічної несумісності;

– відсутність організаційно-політичного центру відповідальності за постановку завдання створення інфраструктури електронної ідентифікації, що унеможливлює розробку цільової програми та практичну реалізацію інфраструктури з урахуванням світового та європейського досвіду, стану інформаційно-телекомунікаційних систем в Україні, наявних та перспективних он-лайн сервісів;

– низький рівень систематизації нормативних та технологічних підходів до принципів та механізмів ідентифікації фізичних та юридичних осіб в он-лайн середовищі у співвідношенні до аналогічних процесів у «нецифровому» світі та житті країни, що призводить до розбалансування правових наслідків нетотожної ідентифікації, виникненню ризиків репутаційного та фінансового характеру, порушення конфіденційності інформації, загроз особистій безпеці громадян, вчиненню адміністративних та кримінальних злочинів;

– відсутність дієвої політики по відношенню до захисту персональних даних громадян, визнаних конкретних механізмів запобігання крадіжки ідентичності, що спричиняє недбалому ставленню власників інформаційних систем, які збирають персональні дані користувачів під час їх реєстрації в системі, позбавляючись відповідальності шляхом отримання згоди

[6] http://zakon4.rada.gov.ua/laws/show/4-2009-%D0%BF

громадянина на обробку та розповсюдження даних про його особистість;

– недостатній рівень взаємодії із зарубіжними інституціями та організаціями, діяльність яких пов'язана із вирішенням завдань розбудови інфраструктур довірчих послуг та електронної ідентифікації, наслідком чого є відсутність повного доступу до інформації, пов'язаної із нормативним та технічним регулюванням галузі, сучасними тенденціями розвитку схем електронної ідентифікації та вимог щодо взаємного їх визнання суб'єктами створюваного єдиного цифрового ринку Європи.

Серед основних чинників виникнення проблеми нормативно-правового характеру та наслідків їх дії слід визначити такі:

– відсутність чіткої нормативно-правової бази, що визначала б повноваження та компетенції державних органів щодо нормативного та технічного регулювання сфери електронної ідентифікації, що стало причиною використання власниками та розпорядниками інформаційних систем засобів та механізмів ідентифікації та автентифікації користувачів поза будь-яких норм;

– відсутність систематизованого нормативного визначення процесів електронної ідентифікації та автентифікації, а також підходів до вибору та забезпечення конкретного рівня гарантій електронної ідентифікації користувачів інформаційних систем, заснованого на оцінці ризиків хибної автентифікації, що унеможливлює впровадження засобів та систем, належним чином адаптованих до загроз безпеці інформації;

– відсутність в нормативному полі України поняття електронного паспорта громадянина України як документа, що посвідчує особу, що перешкоджає подальшому створенню правового підґрунтя для впровадження електронних посвідчень особи як складової інфраструктури електронної ідентифікації;

– вкрай недостатнє покриття національними стандартами та технічними специфікаціями сфери електронної ідентифікації, що фактично унеможливило побудову безпечних та інтероперабельних схем електронної ідентифікації, діючих в рамках єдиних вимог до реалізацій та процедур використання.

Серед основних чинників виникнення проблеми соціально-економічного характеру та наслідків їх дії слід визначити такі:

– економічна криза, що призвела до зменшення обсягу фінансування робіт у рамках виконання Національної програми інформатизації, внаслідок чого зменшився вплив програми на процеси інформатизації в державі та посилилася децентралізація підходів до здійснення заходів з розбудови інформаційного суспільства відповідними державними органами;

– брак бюджетних коштів, гарантованості повного ресурсного забезпечення національних програм та проектів розвитку інформаційного суспільства, відсутність належних умов для залучення приватних інвестицій до вирішення завдань інформатизації, що призвели до відсторонення задач створення систем управління електронною ідентифікацією від пріоритетних напрямків;

– відсутність соціальної спрямованості систем надання електронних послуг із акцентом на розв'язання проблем підвищення рівня та якості життя, проблем безробіття, посилення соціального захисту населення, поліпшення умов праці, розвиток охорони здоров'я та освіти, наслідком чого є недостатня затребуваність у засобах електронної ідентифікації та безпечному їх використанні;

– відсутність адекватного ціноутворення на засоби електронної ідентифікації, які використовуються на сьогоднішній день під час надання тих чи інших електронних послуг, що призводить до значного дисбалансу цін від безкоштовних до надмірно завищених та до порушення принципів добросовісної конкуренції;

- недостатній рівень комп'ютерної та інформаційної грамотності населення та цифрова нерівність, наслідком чого є відсутність мотивації громадян до використання надійних засобів електронної ідентифікації, нерозуміння та нехтування принципами захисту інформації та персональних даних;

- низька ефективність використання кадрових ресурсів, спрямованих на інформатизацію та впровадження технологій захисту інформації у соціальну сферу, що призводить до створення систем надання електронних послуг з низьким рівнем орієнтації на користувача.

Серед основних чинників виникнення проблеми технологічного характеру та наслідків їх дії слід визначити такі:

– зростання кіберзлочинності в умовах збільшення кількості інформаційних систем, що здійснюють оброблення даних про особистість у масштабах, які дозволяють контролювати життя людей у віддаленому доступі та, як наслідок, відсутність достатнього рівня довіри населення до отримання он-лайн послуг через їх недостатню захищеність;

– відсутність захищеного обміну ідентифікаційними даними фізичних та юридичних осіб, які обробляються в інформаційних системах органів державної влади та приватного сектору, неузгодженість у виборі ідентифікаторів, брак адекватної верифікації ідентифікаційних даних, що призводять до побудов технологічно відокремлених систем ідентифікації, надлишкового або недостатнього обсягу збору даних про особистість користувачів, необхідних для їх достовірної ідентифікації, неможливості перевірити справжність ідентифікаційних даних;

- використання у системах реєстрації та контролю доступу технологічно несумісних механізмів, алгоритмів та протоколів електронної ідентифікації та автентифікації, що унеможливлює інтеграційні процеси та використання засобів електронної ідентифікації різних типів в залежності від вибору користувачів;

- відсутність технологічних платформ для проведення випробувань на предмет інтероперабельності різних схем та засобів електронної ідентифікації, що призводить до ізольованості розробників, виробників таких схем та засобів, а також провайдерів послуг електронної ідентифікації.

Наведені причини та наслідки відсутності умов побудови в Україні довірчої інфраструктури електронної ідентифікації дає підстави стверджувати про те, що вирішення проблеми засобами територіального чи галузевого управління є неефективним з огляду на необхідність надання значної частини електронних послуг централізовано в рамках належного нормативного та технічного регулювання, в умовах узгодження заходів, направлених на вирішення проблеми, із загальною концепцією розбудови інформаційного суспільства, кібернетичної безпеки, соціально-економічними програмами, націленості на перспективу інтеграції із єдиним цифровим ринком Європи, гарантованого ресурсного забезпечення,

Вирішення проблеми потребує державної підтримки, координації діяльності центральних і місцевих органів виконавчої

влади та органів місцевого самоврядування, розробки низки нормативно-правових актів та прийняття управлінських рішень на рівнях суб'єктів законодавчої ініціативи та центральних органів виконавчої влади, узгодження дій суб'єктів, визначених відповідальними за розробку архітектурних та функціональних рішень, налагодження взаємодії між державою, бізнесом та громадськістю, міжнародної співпраці з інститутами Європейського Союзу та участі у його галузевих програмних проектах.

Шляхом розв'язання проблем недосконалості існуючих схем електронної ідентифікації в України вбачається розробка та публічне обговорення проекту, узгодження та затвердження Урядом Національної стратегії електронної ідентифікації України (далі – Стратегія) як складової частини концепції побудови та розвитку інформаційного суспільства з урахуванням існуючих недоліків, сучасних тенденцій та особливостей розвитку України в перспективі до 2020 року.

1.3. Місія стратегії та значущість прийняття та реалізації Стратегії для суспільства та держави

Місія Стратегії – побудова такої інфраструктури електронної ідентифікації в Україні, завдяки якій громадяни можуть безперешкодно отримувати доступ до інформації та он-лайн послуги з різних джерел – урядових, приватних, від інших фізичних осіб та за межами державних кордонів – із максимально зниженим ризиком розкрадання персональних даних або шахрайства, з низькою ймовірністю втрати доступу до критично важливих послуг та даних, без необхідності управляти декількома обліковими записами та паролями.

Фізичні особи зможуть проводити широкий спектр он-лайн операцій та довіряти ідентифікаційним даним інших осіб та організацій, з якими вони взаємодіють.

Громадяни будуть знати, яку інформацію збирають про них постачальники електронних послуг, та як вони її використовують.

У громадянина буде існувати можливість вибору використання різних засобів електронної ідентифікації, орієнтованих на користувача, якими він управляє та використовує для підтвердження своєї ідентичності (автентифікації) в Інтернеті та інших мережах.

Громадяни будуть мати доступ до більш широкого спектру електронних послуг, що економить їх матеріальні витрати та час.

В такому орієнтованому на користувача середовищі суб'єкти підприємництва зможуть ефективно вести бізнес, а державні установи - реалізовувати свої повноваження та надавати адміністративні послуги у мережі на основі довіри до ідентифікації та автентифікації особи, яка здійснюється іншою особою та комп'ютерним середовищем, де здійснюються ці операції. Це повинно усунути надлишкові процеси, пов'язані зі збором, управлінням, автентифікацією, авторизацією та верифікацією ідентифікаційних даних. Завдяки застосуванню відповідної схеми електронної ідентифікації для конкретної транзакції будуть знижені втрати, спричинені шахрайством або крадіжкою електронних даних.

Впровадження надійних засобів та схем електронної ідентифікації також розглядається однією із необхідних умов вступу України до Європейського Союзу, в якому концепція побудови єдиного ринку, у тому числі цифрового, є пріоритетним напрямком розвитку, визначеним документами та програмними діями стратегічного характеру[7].

Стратегія та пов'язані з нею дії спрямовані на перетворення існуючого середовища електронної ідентифікації громадян до бажаного цільового стану – довірча інфраструктура електронної ідентифікації. Довірча інфраструктура електронної ідентифікації об'єднає учасників процесів надання електронних послуг та інтероперабельну інфраструктуру для впровадження надійних засобів електронної ідентифікації різного типу. Інфраструктура буде уявляти собою гармонізовану частину Інтернет середовища, в якому окремі особи, організації та служби та зможуть довіряти один одному завдяки достовірній та безпечній ідентифікації та автентифікації.

Інфраструктура електронної ідентифікації має забезпечити:

- безпеку, шляхом зниження ризиків доступу зловмисників до електронних послуг та даних;
- ефективність, яка заснована на зручності для громадян, які будуть використовувати меншу кількість облікових записів та паролів та для підприємств, які скоротять витрати на паперовий документообіг та організацію обліку;

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0245R(01)&from=EN

– простоту у використання технічних рішень електронної ідентифікації за рахунок впровадження таких технічних рішень електронної ідентифікації (протоколів та засобів), які не вимагають додаткової спеціальної підготовки;

– гарантії того, що засобі електронної ідентифікації (електронні посвідчення, старт-картки, токени тощо) є захищеними, що, в свою чергу, надає більш широкі можливості використання Інтернет технологій для надання електронних послуг;

– конфіденційність даних фізичних осіб, які мають бути впевнені у збереженні своїх даних та регулярно інформуватись про те, хто мав доступ до даних та з якою метою;

– захист персональних даних та забезпечення анонімності за рахунок збереження ідентифікації у секреті та обміном тільки тієї інформації, яка необхідна для завершення електронної транзакції або отримання електронної послуги;

– можливість вибору засобів електронної ідентифікації, що надаються постачальниками (провайдерами) послуг електронної ідентифікації;

– можливості для інновацій за рахунок того, що постачальники послуг електронної ідентифікації розширюють спектр та покращують якість електронних послуг.

1.4. Відповідність Стратегії пріоритетам державної політики

Основні засади внутрішньої та зовнішньої політики України, що стосуються питань, порушених у цій Стратегії, викладено у нормативно-правових актах держави різних рівнів.

Так, Законом України «Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони» від 16 вересня 2014 року № 1678-VII[8] ухвалено угоду, умовами якої серед іншого є:

– розвиток електронної торгівлі, яка має здійснюватися за умови забезпечення повної відповідності найвищим міжнародним

[8] http://zakon4.rada.gov.ua/laws/show/1678-18

стандартам захисту інформації з метою забезпечення довіри користувачів електронної торгівлі;

– визнання сертифікатів електронних підписів, виданих населенню, та сприяння розвитку послуг транскордонної сертифікації;

– співробітництво у сферах впровадження он-лайн послуг, зокрема електронного бізнесу, електронного уряду, електронної охорони здоров'я і електронного навчання.

Законом України «Про захист персональних даних"[9] визначені такі основні вимоги обробки персональних даних:

– персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки;

– склад та зміст персональних даних мають бути відповідними, адекватними та не надмірними стосовно визначеної мети їх обробки;

– не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Стратегією розвитку інформаційного суспільства в Україні, затвердженою розпорядженням Кабінету Міністрів України від 15.05.2013 №386-р[10] серед інших принципів розвитку інформаційного суспільства визначено такі:

– рівноправне партнерство державних органів, громадян і бізнесу;

– правомірність одержання, використання, поширення, зберігання та захисту інформації;

– інформаційна безпека.

Програмою діяльності Кабінету Міністрів України, схваленою Постановою Верховної Ради України від 11 грудня 2014 року № 26-VIII[11] серед основних цілей визначено Нову політику державного управління, котра серед інших заходів передбачає запровадження електронного урядування із досягненням таких показників:

---

[9] http://zakon4.rada.gov.ua/laws/show/2297-17

[10] http://zakon4.rada.gov.ua/laws/show/386-2013-p/page

[11] http://zakon2.rada.gov.ua/laws/show/26-19

– запровадження надання електронних безконтактних послуг (2015-2016 роки);

– електронна ідентифікація та електронний підпис громадянина (до 2017 року);

– відмова від паперового документообігу (2015-2016 роки);

– розроблення та сприяння прийняттю закону про єдину систему електронної взаємодії (2015 рік);

– розроблення та сприяння прийняттю закону про відкриті дані (2015 рік).

Отже, розробка Стратегії узгоджується із пріоритетами, принципами, цілями та завданнями зовнішньої та внутрішньої державної політики, у тому числі, із планом діяльності Уряду на найближчі роки.

2. Оцінка поточного стану сфери електронної ідентифікації

2.1 Стан вітчизняної нормативно-правової бази та стандартизації щодо електронної ідентифікації

Основними нормативно-правовими актами, які на сьогодні створюють засади для впровадження та розвитку інфраструктури електронної ідентифікації в Україні слід розглядати:

- Податковий кодекс України[12];
- Цивільний кодекс України[13];
- Закон України «Про державний реєстр виборців»[14];
- Закон України «Про державну реєстрацію актів цивільного стану»[15];
- Закон України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців»[16];
- Закон України «Про електронний цифровий підпис»[17];
- Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[18];
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»[19];
- Закон України «Про захист персональних даних»[20],
- Закон України «Про загальнообов'язкове державне пенсійне страхування»[21].

[12] http://zakon4.rada.gov.ua/laws/show/2755-17
[13] http://zakon4.rada.gov.ua/laws/show/435-15
[14] http://zakon4.rada.gov.ua/laws/show/698-16
[15] http://zakon4.rada.gov.ua/laws/show/2398-17
[16] http://zakon4.rada.gov.ua/laws/show/755-15
[17] http://zakon4.rada.gov.ua/laws/show/852-iv
[18] http://zakon4.rada.gov.ua/laws/show/5492-17
[19] http://zakon4.rada.gov.ua/laws/show/80/94-вр
[20] http://zakon4.rada.gov.ua/laws/show/2297-17
[21] http://zakon4.rada.gov.ua/laws/show/1058-15

– Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006р. №373[22];

– Нормативний документ системи технічного захисту інформації «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» НД ТЗІ 2.5-004-99, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22[23].

Окрім зазначених документів, слід наголосити на і на інших законодавчих актах, нормативних актах – державних стандартах та відомчих розпорядчих документах, які у тому або іншому ступені впливають на стан та перспективи розвитку систем електронної ідентифікації, процедур перевірки ідентичності, автентифікації тощо.

Суттєвим недоліком, перед яким стикаються розробники систем електронного урядування та інформаційних систем взагалі в Україні, є відсутність систематизованого нормативного визначення процесів електронної ідентифікації та автентифікації, а також підходів до вибору та забезпечення конкретного рівня гарантій автентифікації учасників електронної взаємодії, заснованого на оцінці ризиків хибної автентифікації.

Свідченням цього є приклади наведення терміну "ідентифікація" у нормативних актах різних рівнів. При цьому важливо зазначити, що актами по суті лише частково встановлено конкретну межу між термінами та відповідними до них процедурами, що стосуються встановлення (ідентифікації) особи за безпосередньою участю інших осіб або із використанням інформаційних систем, тобто автоматизованим способом.

Поняття «особа» взагалі, відповідно до законодавства України, має відношення до фізичних осіб та юридичних осіб. Згідно з Цивільним кодексом України, фізичною особою є людина як учасник цивільних відносин в той час, коли юридичною особою є організація, створена і зареєстрована у встановленому законом порядку.

Ідентифікація особи за безпосередньою участю інших осіб (як правило, фізичних осіб, що є посадовими особами) у законодавчих

[22] http://zakon4.rada.gov.ua/laws/show/373-2006-п
[23] http://www.dstszi.gov.ua/dstszi/doccatalog/document?id=106342

та підзаконних актах правового поля України передбачає встановлення тотожності фізичної або юридичної особи за сукупністю даних, що містяться у документах, виданими уповноваженими установами, які у певній мірі унеможливлюють виникнення сумнівів щодо цієї особи, яка звернувся за вчиненням тих або інших юридичних дій.

Так, наприклад, Законом України «Про нотаріат»[24] (Стаття 43) визначено, що «встановлення особи здійснюється за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи громадянина, який звернувся за вчиненням нотаріальної дії». При цьому надається перелік документів, використання яких робить можливим або унеможливлює ідентифікацію особи під час вчинення нотаріальних дій.

Іншим законами також встановлюються терміни “ідентифікація особи”:

“Ідентифікація особи” - встановлення на підставі документа, що посвідчує особу власника, та фіксація у письмовій формі прізвища та імені, дати народження та адреси особи, яка здійснює угоду, а також найменування, номера і дати видачі пред'явленого документа, найменування установи, що його видала (Закон України «Про банки і банківську діяльність»[25]);

“Ідентифікація особи” - встановлення тотожності особи за сукупністю інформації про неї за допомогою основних (обов'язкових) та додаткових (факультативних) біометричних даних, параметрів (Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[26]).

Окремо слід відзначити визначення терміну “персональні дані” відповідно до Закону України «Про захист персональних даних»[27], яким також опосередковано визначено поняття ідентифікації особи:

“Персональні дані” - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

---

[24] http://zakon4.rada.gov.ua/laws/show/3425-12
[25] http://zakon4.rada.gov.ua/laws/show/2121-14
[26] http://zakon4.rada.gov.ua/laws/show/5492-17
[27] http://zakon4.rada.gov.ua/laws/show/2297-17

Цей термін та його сутність має вагоме значення для висвітлення проблеми електронної ідентифікації в системах електронного урядування у подальшому.

В якості іншого прикладу, стосовно встановлення юридичних осіб та фізичних осіб - підприємців Законом України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців»[28] встановлено, що для їх ідентифікації під час провадження господарської діяльності та відкриття рахунку в банку використовується виписка з Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців - документ, що містить відомості про юридичну особу або її відокремлені підрозділи, або фізичну особу - підприємця, визначені цим Законом.

Більш неоднозначною є ситуація із визначення процесу ідентифікації осіб як користувачів інформаційних систем, тобто для випадків, коли процес відбувається в автоматичний спосіб.

Відмінними за правовим змістом від термінів “фізична особа” або “юридична особа”, які нормативно визначені для “нецифрового світу”, є поняття «користувач інформації в системі - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі» (Закон України «Про захист інформації інформаційно-телекомунікаційних системах»[29]), та «підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа» (Закон України «Про електронний цифровий підпис[30]»).

Так, на рівні Закону України «Про електронний цифровий підпис» встановлено, що електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

Тобто законом визначено механізм ідентифікації певної категорії громадян - користувачів інформаційних систем

[28] http://zakon4.rada.gov.ua/laws/show/755-15
[29] http://zakon4.rada.gov.ua/laws/show/80/94-вр
[30] http://zakon4.rada.gov.ua/laws/show/852-iv

(підписувачів). Проте, це стосується лише тих користувачів, які використовують електронний цифровий підпис для створення електронних документів.

В нормативно-правових актах інших рівнів їх автори також намагались визначити термін “ідентифікація” у контексті “цифрового світу”:

“Ідентифікація” - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. (Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006р. №373);

“Ідентифікація користувача” - процедура присвоєння користувачеві набору персональних електронних реквізитів (звичайно використовується пара логін - пароль) або надання йому спеціального електронного ключа, що перебуває в його ексклюзивному користуванні. (Наказ Міністерства економіки України "Про затвердження Порядку планування, формування, створення, функціонування, супроводження, систематизації електронних інформаційних ресурсів Міністерства економіки України та доступу до них" від 16.07.2010 N 854);

“Ідентифікація особи” - встановлення відповідності ідентифікаційних ознак людини, занесених у документи або базу даних, фактичним ознакам самої людини. (Наказ Державного комітету ядерного регулювання "Про затвердження Правил фізичного захисту ядерних установок та ядерних матеріалів" від 04.08.2006 N 116).

Отже, вважається за необхідне на нормативному рівні впорядкувати понятійний апарат сфери електронної ідентифікації, що є однією із основних умов створення інфраструктури електронної ідентифікації із забезпеченням її інтероперабельності (сумісності) не тільки на технологічному, але й на семантичному рівні та рівні політик.

Окремим питанням, яке має безпосередній вагомий вплив на впровадження та розвиток технологій електронної ідентифікації є питання унікальності ідентифікаційних даних та ідентифікаторів, котрі дозволять визначити (ідентифікувати) об’єкт (фізичну або

юридичну особу, інформаційну систему) серед інших об'єктів у визначеному контексті.

У нормативному полі України на рівні законодавчих актів визначено досить широкий перелік ідентифікаційних даних, які використовуються під час інформаційної взаємодії між суб'єктами надання тих або інших адміністративних послуг, виконання суб'єктами владних повноважень тощо.

Серед базових законодавчих актів, які слід вважати найбільш впливовими у соціальному та діловому контексті життя громадян України та які мають безпосереднє відношення до завдань Стратегії слід відзначити такі:

- Податковий кодекс України[31];
- Цивільний кодекс України[32];
- Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[33];
- Закон України «Про державну реєстрацію актів цивільного стану»[34];
- Закон України «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців»[35];
- Закон України «Про державний реєстр виборців»[36];
- Закон України «Про загальнообов'язкове державне пенсійне страхування»[37].

Цими законодавчими актами в різні роки були внесені до правового поля держави переліки даних, які дозволяють відрізнити фізичну або юридичну особу від інших суб'єктів для забезпечення виконання тих або інших функцій органами державної влади або недержавними установами під час реалізації прав громадян, надання адміністративних та соціальних послуг, здійснення державного нагляду тощо та використовувати ці дані під час автоматизованої обробки.

---

[31] http://zakon4.rada.gov.ua/laws/show/2755-17
[32] http://zakon4.rada.gov.ua/laws/show/435-15
[33] http://zakon4.rada.gov.ua/laws/show/5492-17
[34] http://zakon4.rada.gov.ua/laws/show/2398-17
[35] http://zakon4.rada.gov.ua/laws/show/755-15
[36] http://zakon4.rada.gov.ua/laws/show/698-16
[37] http://zakon4.rada.gov.ua/laws/show/1058-15

В результаті на теперішній час нормативно-правовими актами держави визначено такі основні та найбільш вживані ідентифікаційні дані фізичних осіб:

- прізвище;
- ім’я;
- по батькові;
- дата народження;
- дата смерті;
- стать;
- місце народження;
- місце проживання;
- громадянство;
- відцифрований зразок підпису особи;
- відцифрований образ обличчя особи;
- відцифровані відбитки пальців рук;
- серія та номер документу, що посвідчує особу, її цивільний стан або соціальний статус;
- реєстраційний номер облікової картки платника податків - фізичної особи;
- унікальний номер запису в Єдиному державному демографічному реєстрі.

Слід зазначити, що громадянам України відповідно до законодавства надано право вчиняти акти цивільного стану, які призводять до змін основних ідентифікаційних даних таких як прізвище, ім’я, по-батькові, дата та місце народження (зміна імені, усиновлення, шлюб).

Крім того, протягом життя людини об’єктивно може змінюватись також і місце проживання, а в окремих випадках - громадянство та стать.

Фізіологічні процеси також призводять до зміни образу обличчя та власноручного підпису людини.

Законом встановлено, що відцифровані відбитки пальців надаються за згодою особи. Також ймовірною є втрата відбитків пальців рук.

Ідентифікаційні дані, що відповідають акту смерті фізичної особи, можуть бути скасовані у випадках визнання особи померлою та появи фізичної особи, яка була оголошена померлою.

Важливо відзначити те, що серія та номер документів, що посвідчують особу, її цивільний стан або соціальний статус, є лише обліковими даними таких документів, які протягом життя людини з тих або інших причин не є постійними та змінюються у випадках втрати, заміни, видачі дублікатів тощо.

Отже, згадані вище ідентифікаційні дані фізичних осіб розглядаються як такі, що придатні для однозначної ідентифікації особи лише у конкретний момент часу. Водночас, у контексті електронної ідентифікації частина ідентифікаційних даних (ім'я, прізвище, по батькові) на різних етапах їх обробки, зокрема внесення до реєстрів або пред'явлення користувачем інформаційної системи під час реєстрації, мають значну залежність від помилкового введення та уявляють складність на етапах їх перевірки (верифікації).

Натомість, серед ідентифікаційних даних фізичних осіб, які на сьогодні відповідно до законодавства України мають носити незмінне значення, використовують більш адаптований до автоматизованої обробки формат, який передбачає, у тому числі, методи розрахунку контрольних цифр з метою запобігання помилкового введення та для забезпечення автоматичного їх формування, слід відзначити реєстраційний номер облікової картки платника податків - фізичної особи та унікальний номер запису в Єдиному державному демографічному реєстрі.

Важливо відзначити, що чинним законодавством України передбачено право фізичних осіб на відмову від прийняття реєстраційного номера облікової картки платника податків через свої релігійні переконання. За даними Державної фіскальної служби України, станом на початок 2015 року близько 200 тисяч громадян України скористались таким правом.

У даному випадку, ідентифікація фізичних осіб, у тому числі під час автоматизованої обробки даних щодо осіб в інформаційних системах органів державної влади, здійснюється з використанням серії та номера паспорта. Проблемність такої обробки на сьогодні полягає у непостійності цих значень з причин, про які було наголошено вище, а також у відсутності в країні централізованої

системи обробки даних щодо діючих, втрачених та визнаних недійсними паспортів.

З огляду на зазначене, використання унікального номера запису в Єдиному державному демографічному реєстрі, введеного в дію разом із набуттям чинності Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[38] 1 січня 2013 року, а фактично залученого до використання 1 січня 2015 року на початку видачі «біометричних» паспортів, розглядається як перспективне та таке, що має слугувати основою розбудови інфраструктури електронної ідентифікації України.

Водночас, використання реєстраційного номера облікової картки платника податків, серії та номера паспорта, місця реєстрації фізичної особи, найменування суб'єкта, що видав паспорт та дати видачі документа є в багатьох випадках обов'язковими під час укладення договорів та інших правочинів, подання звернень громадян до органів державної влади, звітності до органів нагляду тощо. Безумовно, впровадження систем електронної ідентифікації з метою автоматизації згаданих вище процесів та процедур, повинно враховувати глибоке проникнення використання цих ідентифікаційних даних, що вимагає зваженого підходу у випадках прийняття рішення щодо використання нових, можливо більш надійних та ефективних з точки зору автоматизованої обробки ідентифікаторів, та однозначного забезпечення їх зворотної сумісності із тими, що були у використанні раніше.

У цьому контексті варто зазначити на необхідності внесення змін до нормативної бази України для забезпечення використання унікального номера запису в Єдиному державному демографічному реєстрі у якості єдиного ідентифікатора фізичної особи в інших інформаційних системах.

Станом на початок 2015 року таке використання передбачено лише стосовно персоніфікованого обліку у системі загальнообов'язкового державного пенсійного страхування відповідно до Закону України «Про загальнообов'язкове державне пенсійне страхування»[39].

Таким чином, використання унікального номера запису в Єдиному державному демографічному реєстрі як унікального

[38] http://zakon4.rada.gov.ua/laws/show/5492-17

[39] http://zakon4.rada.gov.ua/laws/show/1058-15/page

ідентифікатора фізичних осіб вбачається перспективним за умов визначення нормативних та технологічних засад обміну ідентифікаційними даними між Єдиним державним демографічним реєстром та іншими базовими реєстрами, такими як Державний реєстр актів цивільного стану, Державний реєстр виборців, Державний реєстр фізичних осіб – платників податків, Державний реєстр застрахованих осіб, реєстрами майнових прав, базами даних, задіяних у сфері судочинства тощо.

Треба наголосити, що існуюча нормативна-правова база жодним чином не обмежує використання тих чи інших технологій ідентифікації та автентифікації користувачів інформації в інформаційних системах, проте встановлює лише загальні вимоги та надає рекомендації, необхідні для вибору таких технологій.

За базовий аспект визначення технології електронної ідентифікації нормативно-правові акти чинного законодавства використовують аспект захисту інформації в системах, де такі технології передбачаються до використання.

Так, вимогами Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», постанови Кабінету Міністрів України від 29 березня 2006 р. №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», іншими нормативно-правовими актами визначено необхідність та порядок побудови систем захисту інформації, що належить до різних категорій, у тому числі, до державних інформаційних ресурсів.

У Додатку В наведені основні вимоги, що висуваються до захисту інформації в національній нормативній базі.

2.2 Стан європейської нормативно-правової бази та стандартизації щодо електронної ідентифікації.

2.2.1 Аналіз вимог Регламенту ЄС №910/2014 «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЄС»

Серед нормативно-правових актів Європейського Союзу, які визначають основні засади законодавства у сфері електронної

ідентифікації, вперш за все слід зазначити Регламент ЄС №910/2014 Європейського Парламенту та Ради від 23 липня 2014 «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЄС» (далі – Регламент eIDAS)[40] .

Регламент eIDAS спрямований на підвищення рівня довіри до електронних транзакцій на внутрішньому ринку шляхом надання загальної основи для безпечної і цілісної електронної взаємодії між підприємствами, громадянами і державними органами, тим самим підвищуючи ефективність державних і приватних он-лайн послуг, електронного бізнесу та електронної торгівлі в ЄС.

Директива 1999/93/ЄС Європейського Парламенту та Ради[41], охоплювала в основному сферу електронних підписів, не надаючи всебічних крос-кордонних та крос-секторних основ для безпечних, надійних і простих електронних транзакцій. Регламент eIDAS удосконалює та розширює значення Директиви.

Цей документ робить вагомий внесок у побудову єдиного цифрового ринку шляхом створення умов для взаємного крос-кордонного визнання ключових компонентів, таких як електронна ідентифікація, електронні документи, електронні підписи та електронні послуги доставки, а також для сумісності послуг електронного урядування на території Європейського Союзу.

Поява Регламенту eIDAS на правовому полі Європейського Союзу продиктована тим, що у більшості випадків громадяни не можуть використати свою електронну ідентифікацію для автентифікації в іншій державі-члені, оскільки національні схеми електронної ідентифікації, прийняті в їх країні, не визнані і не приймаються в інших державах-членах. Цей електронний бар'єр не дозволяє провайдерам послуг володіти усіма перевагами внутрішнього ринку. Взаємно визнані і прийняті засоби електронної ідентифікації мають полегшити крос-кордонне надання електронних послуг на внутрішньому ринку і дозволять підприємствам та громадянам подолати умовні цифрові кордони, не стикаючись з перешкодами під час взаємодії з органами державної влади інших країн.

Регламент eIDAS висуває вимоги щодо відповідності принципам, що стосуються захисту персональних даних,

[40] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[41] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

передбачених Директивою 95/46/ЄС Європейського Парламенту і Ради. У цьому відношенні, коли справа доходить до принципу взаємного визнання, встановленому Регламентом, автентифікація для он-лайн послуги повинна стосуватися обробки тільки тих ідентифікаційних даних, які є адекватними і помірними для надання доступу до цієї он-лайн послуги. Крім того, вимоги, передбачені Директивою 95/46/ЄС щодо конфіденційності та безпеки обробки повинні виконуватись провайдерами послуг та наглядовими органами.

Також важливим правовим аспектом, визначеним Регламентом eIDAS є те, що держави-члени залишають за собою право використовувати та вводити у дію ти або інші засоби електронної ідентифікації для доступу до он-лайн послуг, примати рішення, чи слід залучати приватний сектор до надання таких засобів, мати вибір чи повідомити про всі, деякі або про жодну із схем електронної ідентифікації, що використовуються на національному рівні для доступу до громадських он-лайн послуг або особливих послуг.

Регламентом eIDAS визначено умови, з врахуванням яких повинні визнаватись засоби електронної ідентифікації та оголошуватись схеми електронної ідентифікації, що повинно допомогти державам-членам створити необхідний рівень довіри один до одного стосовно схем електронної ідентифікації та взаємно визнати і прийняти засоби електронної ідентифікації, що підпадають під оголошені державами схеми.

Також проголошується принцип взаємного визнання і прийняття, якщо держава-член, що оголошує (здійснює нотифікацію) схему електронної ідентифікації, відповідає умовам оголошення, а оголошення було опубліковано в Офіційному журналі Європейського Союзу. Проте, принцип взаємного визнання повинен стосуватись лише автентифікації під час отримання он-лайн послуг. Доступ до цих он-лайн послуг та їх кінцеве надання замовникові повинні бути тісно пов'язані з правом отримання таких послуг на умовах, встановлених національним законодавством.

До окремого значущого розділу вимог Регламенту eIDAS слід віднести визначення того, що рівні гарантій електронної ідентифікації повинні характеризувати ступінь довіри до засобу електронної ідентифікації під час встановлення ідентичності людини, забезпечуючи тим самим гарантію того, що особа, яка потребує ідентифікації, насправді є людиною, для якої було встановлено дану ідентичність. Встановлюється, що рівень гарантії

залежить від ступеню впевненості у тому, що засіб електронної ідентифікації забезпечує підтвердження заявленої ідентичності, або ствердження про ідентичність людини з урахуванням процесів (наприклад, підтвердження і перевірка справжності особи, автентифікація), діяльності з управління (наприклад, організацією, що надає засоби електронної ідентифікації, процедурами надання таких засобів), а також впровадженого технічного контролю.

Різні технічні визначення та опис рівнів гарантій існують як результат заснованих в Європі великомасштабних пілотних проектів, стандартизації та міжнародної діяльності. Так, великомасштабний пілотний проект STORK та стандарт ISO 29115, відсилають, зокрема, до рівнів 2, 3 і 4, які повинні бути взяті до уваги під час встановлення мінімальних технічних вимог, стандартів та процедур для рівнів гарантій «низький», «суттєвий» та «високий» у відповідності до положень Регламенту eIDAS, також при забезпеченні послідовного застосування положень Регламенту задля досягнення найвищого рівня гарантій, пов'язаного з гарантуванням ідентичності.

Низький, суттєвий або високий рівень гарантій має відповідати наступним критеріям:

(а) низький рівень гарантії повинен відноситись до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують обмежений ступінь довіри до ідентичності особи, про яку заявляється або стверджується, та які характеризуються відповідними технічними специфікаціями, стандартами та процедурами, пов’язаними з ними, у тому числі з технічними засобами контролю, метою яких є зниження ризику зловживання або підміни ідентичності;

(б) суттєвий рівень гарантії повинен відноситись до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують суттєвий ступінь довіри до ідентичності особи, про яку заявляється або стверджується, та які характеризуються відповідними технічними специфікаціями, стандартами та процедурами, пов’язаними з ними, у тому числі з технічними засобами контролю, метою яких є суттєве зниження ризику зловживання або підміни ідентичності;

(в) високий рівень гарантії повинен відноситись до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують вищий ступінь довіри до ідентичності особи, про яку заявляється або стверджується, ніж до засобів

електронної ідентифікації із суттєвим рівнем гарантій, та які характеризуються відповідними технічними специфікаціями, стандартами та процедурами, пов’язаними з ними, у тому числі з технічними засобами контролю, метою яких є недопущення зловживання або підміни ідентичності.

До 18 вересня 2015 року, з урахуванням відповідних міжнародних стандартів та при дотриманні положень Регламенту eIDAS, Єврокомісія шляхом прийняття виконавчих актів повинна встановити мінімальні технічні характеристики, стандарти та процедури стосовно низького, суттєвого та високого рівнів гарантії, які повинні застосовані для засобів електронної ідентифікації.

Передбачається, що ці мінімальні технічні характеристики, стандарти і процедури повинні бути встановлені з посиланням на надійність і якість щодо:

(а) процедур доведення та перевірки ідентичності фізичних або юридичних осіб, які застосовуються для видачі їм засобів електронної ідентифікації;

(б) порядку видачі запитуваних засобів електронної ідентифікації

(в) механізму автентифікації, в якому фізична або юридична особа використовує засіб електронної ідентифікації для підтвердження своєї ідентичності перед стороною, яка довіряє;

(г) суб'єктів, які видають засоби електронної ідентифікації;

(д) будь-якого іншого органу, який бере участь в обробці замовлення на видачу засобів електронної ідентифікації; і

(е) технічних характеристик та характеристик безпеки випущеного засобу електронної ідентифікації.

Окремо наголошується на тому, що встановлені вимоги повинні бути технологічно нейтральними, а досягнення необхідних вимог безпеки, повинно бути забезпечено за допомогою різних технологій.

Відповідно до Регламенту eIDAS, зобов'язання визнавати засоби електронної ідентифікації встановлюється тільки щодо тих засобів, рівень гарантії яких відповідає або вище рівня, необхідного для обслуговування в он-лайн режимі. Крім того, зобов'язання має виконуватись тільки коли відповідний орган державного сектора використовує істотний або високий рівень довіри по відношенню до он-лайн послуг. Водночас, Регламентом eIDAS визначено, що

держави-члени повинні залишатися вільними у питанні визнання засобів електронної ідентифікації більш низьких рівнів гарантій.

Документом проголошується, що держави-члени повинні заохочувати приватний сектор добровільно використовувати засоби електронної ідентифікації відповідно до оголошених схем з метою ідентифікації під час отримання он-лайн послуг або здійснення електронних транзакцій. Можливість використання таких засобів електронної ідентифікації має на меті дозволити приватному сектору покладатися на електронну ідентифікацію та автентифікацію, що вже широко використовується в багатьох державах-членах, принаймні в державних установах, для полегшення підприємствам та громадянам доступу до їхніх он-лайн послуг за кордоном. Для полегшення використання приватним сектором таких засобів електронної ідентифікації через кордони, можливість автентифікації, що надається будь-якою державою-членом, повинна бути доступною для сторін, які довіряють, приватного сектора, створених за межами території держави-члена на тих же умовах, що прийняті для сторін, які довіряють, приватного сектора всередині держави-члена.

Даний Регламент передбачає відповідальність держави-члена, яка оголосила схему електронної ідентифікації, суб'єкта, що випускає засоби електронної ідентифікації та суб'єкта, що проводить процедури автентифікації, за невиконання відповідних зобов'язань, визначених Регламентом. Тим не менш, це повинне застосовуватися у відповідності з національними правилами щодо відповідальності. Таким чином, Регламент eIDAS не впливає на ці правила, наприклад, з питань щодо визначення збитків або на прийняті процесуальні норми, у тому числі правила, що стосуються тягаря доведення.

Регламент eIDAS наголошує на тому, що безпека схем електронної ідентифікації є ключем до довіреного транскордонного взаємного визнання засобів електронної ідентифікації. У цьому контексті держави-члени повинні співпрацювати відносно безпеки та сумісності схем електронної ідентифікації на рівні Євросоюзу. Всякий раз, коли схеми електронної ідентифікації вимагають специфічного обладнання або програмного забезпечення, яке буде використовуватися сторонами, які довіряють, на національному рівні, крос-кордонна сумісність вимагає того, що держави-члени не повинні нав'язувати такі вимоги і пов'язані з ними витрати для сторін, які довіряють, за межами їх територій. У цьому випадку відповідні рішення повинні бути обговорені і розроблені в рамках інфраструктури інтероперабельності (сумісності). З іншого боку,

вплив технічних вимог, що випливають із національних специфікацій засобів електронної ідентифікації, на держателів таких електронних засобів (наприклад, смарт-карток) вбачаються неминучим.

Співробітництво держав-членів, як іще один із основних аспектів, визначених Регламентом eIDAS, повинно сприяти встановленню технічної сумісності схем електронної ідентифікації, які пройшли процедуру оголошення (нотифікації), таким чином, щоб створити високий рівень довіри і безпеки, відповідний ступеню ризику. Обмін інформацією та передовим досвідом між державами-членами повинен допомогти в цій співпраці з метою взаємного визнання схем електронної ідентифікації.

2.2.2 Стан європейської та міжнародної стандартизації в сфері електронної ідентифікації

На європейському та міжнародному рівнях стандартизації в сфери електронної ідентифікації проводиться дуже активна робота. Розроблені рекомендації, міжнародні стандарти та технічні специфікації становлять основу для побудови, впровадження та використання засобів, схем електронної ідентифікації та інфраструктури електронної ідентифікації на будь-якому, у тому числі, на національному рівні (Додаток Б).

Одним із найважливіших аспектів міжнародної та європейської нормативної бази сфери електронної ідентифікації слід відзначити підхід до визначення архітектури управління ідентичністю та надання послуг електронної ідентифікації, функціональні вимоги до обміну інформацією та захисту інформації в інфраструктурі електронної ідентифікації.

Окремо варто наголосити, що на рівні міжнародних стандартів та рекомендацій чітко визначено коло суб'єктів, залучених до інфраструктури електронної ідентифікації, описано їх діяльність та ролі.

Міжнародними стандартами ключовими суб'єктами в інфраструктурі електронної ідентифікації виділено користувача (User), постачальника (провайдера) послуг ідентифікації (Identity Service Provider) та сторони, що довіряє (Relying Party).

Стандартами передбачено можливість організаційної побудови

інфраструктури електронної ідентифікації таким чином, що до складу постачальника (провайдера) послуг ідентифікації можуть входити, або окремо функціонувати такі суб'єкти, як постачальники послуг автентифікації (Authentication Service Provider), органи реєстрації (Registration Authority), постачальники ідентичності (Identity Provider) та постачальники атрибутів (Attribute Provider), на котрих покладається виконання окремих ролей.

Зважаючи на відсутність опису суб'єкта постачальника (провайдера) послуг ідентифікації в нормативному полі України взагалі, особливу увагу слід звернути на необхідність адаптації законодавства та гармонізації стандартів країни до відповідних міжнародних та європейських актів.

Частково таку адаптацію та гармонізацію проведено завдяки створенню та розвитку системи електронного цифрового підпису України, що дозволяє розглядати суб'єктів надання послуг електронного цифрового підпису постачальниками послуг електронної ідентифікації.

Проте, такий розгляд можливий лише на основі опосередкованої відповідності функцій та завдань центрів сертифікації ключів функціям та завданням провайдерів електронної ідентифікації та лише у зрізі одного (найвищого) рівня гарантій електронної ідентифікації, визначених міжнародними стандартами.

Щодо вимог до постачальників (провайдерів) електронної ідентифікації, які забезпечують надання послуг з іншими рівнями гарантій, то варто говорити про відсутність адаптації законодавства та гармонізації стандартів країни до відповідних міжнародних та європейських актів.

2.3 Стан впровадження інфраструктури електронної ідентифікації в Європі

2.3.1 Схеми електронної ідентифікації

Аналіз загального стану впровадження інфраструктури електронної ідентифікації в державах-членах Європейського Союзу свідчить про неоднорідність прийнятих в країнах політик у цій сфері, використання різних технологій ідентифікації та автентифікації, які відповідають різним рівням гарантій електронної ідентифікації.

За даними досліджень незалежної компанії сфери глобальної безпеки UL LLC[42], слід відзначити три основних концептуальних підходи до цієї проблеми, які існують у Європі (рис. 2.1).

Частина держав-членів Європейського Союзу до введення в дію Регламенту eIDAS рухалась у напрямку максимального спрощення процедур, пов'язаних із електронною ідентифікацією для кінцевого користувача. У частині країн Європи до теперішнього часу найбільш вживаними механізмами ідентифікації та автентифікації в інформаційних системах є механізми використання пари «логін-пароль».

Друга категорія країн у системах надання он-лайн сервісів використовує більш надійні механізми автентифікації, які засновані на використанні одноразових паролів із варіаціями їх генерування за допомогою списків, надсилання коротких текстових повідомлень та спеціальних програмно-апаратних генераторів паролів (OTP-токенів).

Нарешті, третя категорія країн побудову систем надання он-лайн сервісів здійснює на основі використання криптографічних перетворень у процесах автентифікації. При цьому такі системи використовують різновиди програмної та апаратної реалізації засобів електронної ідентифікації. Апаратні засоби реалізовані у варіантах засобів кваліфікованого електронного підпису (hardware token) та старт-карток. Також використовуються засоби електронної ідентифікації на основі SIM карток у тих країнах, де впроваджено послуги мобільної ідентифікації (mobileID)

[42] http://ul.com

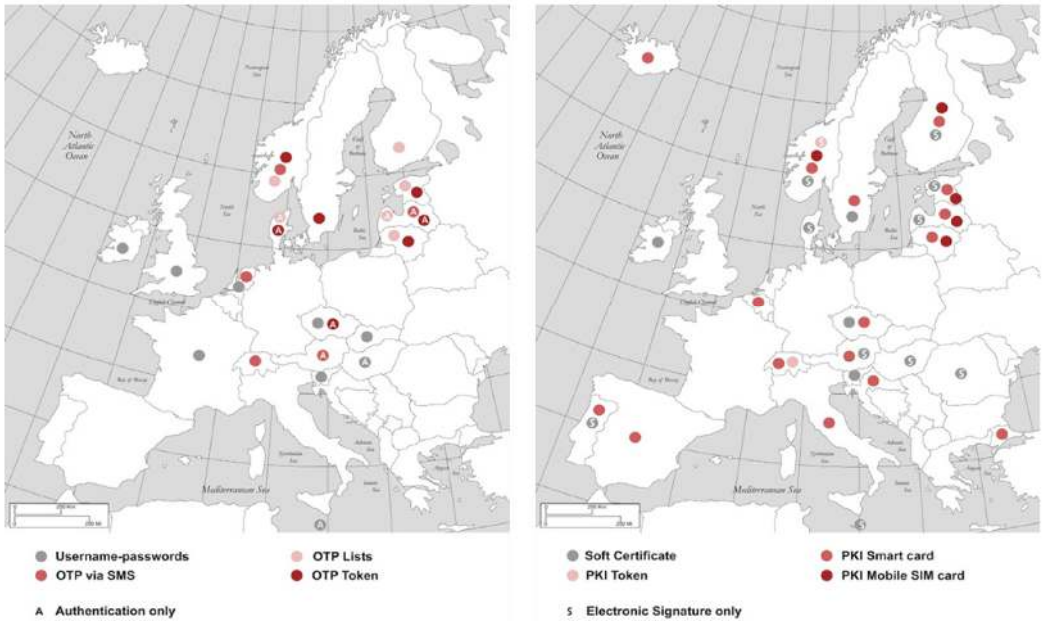


Рис. 2.1 - Схеми електронної ідентифікації, впроваджені у країнах Європи за даними UL LLC.

За результатами досліджень, проведених у 25 країнах було оцінено технології 63 побудованих схемах електронної ідентифікації.

За підсумками, відсоткове відношення використання тих чи інших технологій становить:

– схеми електронної ідентифікації, побудовані на основі механізмів використання пари «логін-пароль» - 9%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання одноразових паролів, заснованих на списках - 6%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання одноразових паролів, заснованих на коротких текстових повідомленнях - 5%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання спеціальних програмно-апаратних генераторів паролів (OTP-токенів) - 7%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання криптографічних перетворень у процесах автентифікації (програмні засоби) - 13%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання криптографічних перетворень у процесах автентифікації (апаратні засоби - hardware token) - 13%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання криптографічних перетворень у процесах автентифікації (апаратні засоби – смарт-картки) - 16%;

– схеми електронної ідентифікації, побудовані на основі механізмів використання криптографічних перетворень у процесах автентифікації (апаратні засоби – SIM-картки) - 5%.

Загальна тенденція, що відслідковується вказує на тяжіння політик електронної ідентифікації у бік надійних та безпечних реалізацій із суттєвим та високим рівнем гарантій електронної ідентифікації у загальному відсотковому відношенні 29% та 57% відповідно.

2.3.2 Електронна ідентифікація фізичних осіб

Окремої уваги заслуговують підходи країни Європи до визначення переліків ідентифікаційних даних, які використовуються у національних схемах електронної ідентифікації та визначення базових ідентифікаторів.

У ході досліджень, проведених під час роботи широкомасштабного пілотного проекту STORK (Secure idenTity acrOss boRders linKed)[43] серед учасників проекту – 18 країн Європи переважна більшість використовує унікальний національний ідентифікатор, який однозначно визначає фізичну особу у загальному контексті населення країн.

Окремі держави-члени Європейського Союзу (Австрія, Германія, Італія, Франція) використовують для електронної ідентифікації секторальні ідентифікатори, або специфічні атрибути як серійний номер сертифіката електронного підпису (Греція).

Таблиця 2.1 Використання ідентифікаційних даних фізичних осіб для їх електронної ідентифікації в державах Європи.

[43] https://www.eid-stork.eu/index.php

Держава	Ідентифікатор	Прізвище	Ім`я	Дівоче прізвище	Дата народження
Austria	Unique ID	+	+		+
Belgium	National ID number	+	+		+
Estonia	National ID number	+	+		+
Finland	National ID number	+	+		+
France	Sectoral ID	+	+		+
Germany	Sectorral and card specific ID number	+	+	+	+
Greece	Certificate Identification number	+	+		+
Iceland	National ID number	+			+
Italy	Fiscal Code	+	+		+
Lithuania	National ID number	+	+		+
Luxemburg	National ID number	+	+		+
Netherlands	National ID number (Citizen Service Number (BSN))	+	+		+
Portugal	National ID number	+	+		+
Slovakia	National ID number	+	+		+
Slovenia	Tax number and Personal registration Number	+	+		+
Spain	National ID number	+	+		+
Sweden	Personal Serial number	+	+		+
United Kingdom	Personal ID Number	+	+		+

Таблиця 2.1 (продовження) Використання ідентифікаційних даних фізичних осіб для їх електронної ідентифікації в державах

Європи.

Держава	Місце народження	Адреса проживання	Стать	Національ-ність	Сімейний стан	Релігійне ім`я або псевдонім
Austria						
Belgium	+	+	+	+		
Estonia			+			
Finland	+	+	+	+		
France	+	+	+			
Germany	+	+				+
Greece		+	+			
Iceland	+	+	+	+		
Italy	+	+	+			
Lithuania	+	+	+	+	+	
Luxemburg				+		
Netherlands	+	+	+	+		
Portugal						
Slovakia		+	+	+		
Slovenia	+		+	+	+	
Spain		+	+	+		
Sweden			+			
United Kingdom	+		+		+	

Використання унікального національного ідентифікатора, вважається за основу ефективного впровадження інфраструктури електронної ідентифікації.

Досвід, наприклад Естонії, свідчить, що впровадження інфраструктури електронної ідентифікації на основі унікального національного ідентифікатора у сукупності із забезпеченням ефективної електронної взаємодії із базовими реєстрами дозволяє

побудувати систему електронного урядування із глибоким проникненням сервісів до суспільного життя населення та бізнес-середовища, а також здобуття високих показників у світових рейтингах оцінки стану розвитку електронного урядування.

Варто відзначити широке *використання у якості засобів електронної ідентифікації документів*, які посвідчують особу у форматі ідентифікаційних карток.

Станом на початок 2015 року державами-членами Європейського Союзу проваджується п'ять напрямків національної політики щодо документів, які посвідчують особу у форматі ідентифікаційних карток:

1) Держави-члени, які не впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток (наприклад: Великобританія, починаючи з 1951 року);

2) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток для візуальної ідентифікації власника, на добровільних засадах (наприклад: Франція);

3) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток для візуальної ідентифікації власника, на обов'язкових засадах (наприклад: Італія);

4) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток для електронної ідентифікації власника, на добровільних засадах (наприклад: Швеція);

5) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток для електронної ідентифікації власника, на обов'язкових засадах (наприклад: Естонія).

Висновок: держави-члени Європейського Союзу мають широкий спектр заходів політики щодо документів, що посвідчують особу у форматі ідентифікаційних карток. Такі документи є обов'язковими у 8 державах-членах Європейського Союзу.

Також в різних державах-членах Європейського Союзу діють різні політики щодо *мінімального віку, від якого громадяни, відповідно до законодавства, повинні отримувати документів*, що посвідчують особу у форматі ідентифікаційних карток. Як приклад: Германія – 16 років, Бельгія – 14 років, Австрія – 12 років.

Більшість держав, які випускають документи, що посвідчують особу у форматі ідентифікаційних карток, провадять політику *візуальної ідентифікації власника документа за допомогою фото*. Італія та Австрія є єдиними державами-членами Європейського Союзу, які не дотримуються такої політики.

Щодо *використання документів, що посвідчують особу у форматі ідентифікаційних карток, з функціями документів для перетину кордону*, у державах-членах Європейського Союзу прийнято три напрямки політики, а саме:

1) Обіг документів, що посвідчують особу у форматі ідентифікаційних карток, які не містять зони для машинного читання даних (MRZ) та не містять біометричних даних власника документу відповідно до вимог Міжнародної організації цивільної авіації (ICAO) (наприклад: Італія, з 2006 року);

2) Обіг документів, що посвідчують особу у форматі ідентифікаційних карток, які містять зону для машинного читання даних (MRZ) та не містять біометричних даних власника документу відповідно до вимог Міжнародної організації цивільної авіації (ICAO) (наприклад: Португалія, з 2007 року);

3) Обіг документів, що посвідчують особу у форматі ідентифікаційних карток, які містять зону для машинного читання даних (MRZ) та містять біометричні дані власника документу відповідно до вимог Міжнародної організації цивільної авіації (ICAO) (наприклад: Швеція, з 2005 року);

Таким чином, держави-члени Європейського Союзу дотримуються різних стратегій щодо функцій документів, що посвідчують особу, як документів для перетину кордонів. Водночас, існує тенденція щодо використання ICAO-сумісних документів, що посвідчують особу.

Стосовно *термінів використання* документів, що посвідчують особу у форматі ідентифікаційних карток у державах-членах Європейського Союзу прийнято такі політики:

1) Термін чинності документів становить 10 років (Приклади: Германія, Іспанія, Португалія, Швеція, Нідерланди, Естонія);

2) Термін чинності документів становить 5 років (Приклад: Бельгія).

Загальна тенденція до використання документів, що посвідчують особу у форматі ідентифікаційних карток має напрямок до терміну, що становить 10 років. Інші види документів, що мають паперовий формат, використовуються більше ніж 10 років.

Держави-члени Європейського Союзу встановлюють власну *цінову політику* щодо оплати документів, що посвідчують особу у форматі ідентифікаційних карток. Так, у Польщі такі документи видаються безкоштовно. Водночас така країна, як Германія впровадила досить суттєву вартість отримання таких документів: 28 Євро, а у Фінляндії вартість документу коливається від безкоштовної до 29 Євро.

У контексті Стратегії важливим є аналіз використання документів, що посвідчують особу у форматі ідентифікаційної картки, у якості засобів електронної ідентифікації для отримання он-лайн сервісів від держави.

На початок 2015 року налічуються 4 основні напрями політики такого використання:

1) Держави-члени, які не впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток, для двох-факторної автентифікації у системах електронного урядування та інших системах (Приклад: Великобританія);

2) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток, для двох-факторної автентифікації у системах електронного урядування в окремих доменах (Приклад: Португалія, з 2007 року);

3) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток, для двох-факторної автентифікації в усіх системах електронного урядування та у жодному недержавному домені (Приклад: Бельгія, з 2004 року);

4) Держави-члени, які впроваджують документи, що посвідчують особу у форматі ідентифікаційних карток, для двох-факторної автентифікації в усіх системах електронного урядування та в усіх недержавних доменах (Приклад: Германія, з 2010 року).

Стосовно використання функції електронного цифрового підпису як додаткової для документів, що посвідчують особу у форматі ідентифікаційних карток для електронної ідентифікації власника, спостерігається два різновиди політик:

1) Документи, що посвідчують особу у форматі ідентифікаційних карток для електронної ідентифікації власника, використовуються для підтримки сервісів електронного цифрового підпису на добровільних засадах за окрему оплату (Приклад: Фінляндія, з 1998 року);

2) Документи, що посвідчують особу у форматі ідентифікаційних карток для електронної ідентифікації власника, використовуються для підтримки сервісів електронного цифрового підпису на обов'язкових засадах за окрему оплату (Приклад: Естонія, з 2002 року).

Загальна тенденція щодо політик використання функції електронного цифрового підпису як додаткової для документів, що посвідчують особу у форматі ідентифікаційних карток для електронної ідентифікації власника, спрямована у бік надання можливості вибору такого використання для громадян.

Варто навести дані також стосовно загальносвітових тенденцій щодо впровадження документів, що посвідчують особу для електронної ідентифікації власника. За оцінками Acuity Market Intelligence[44], на теперішній час кількість країн, які використовують документи, що посвідчують особу для електронної ідентифікації власника у два рази перевищує кількість країн, які не використовують такі документи.

Передбачається, що до 2018 року відношення кількості країн, які перейшли до впровадження документів, що посвідчують особу для електронної ідентифікації власника, до інших, які не використовують такі документи, становитиме 5 до 1. Загальний відсоток країн, які перейшли до впровадження документів, що посвідчують особу для електронної ідентифікації власника, становитиме 82%, а кількість випущених в обіг документів перевищить половину населення земної кулі та становитиме 3,5 мільярди.

Відповідні діаграми наведено нижче:

[44] http://www.acuity-mi.com/GNeID_Report.php

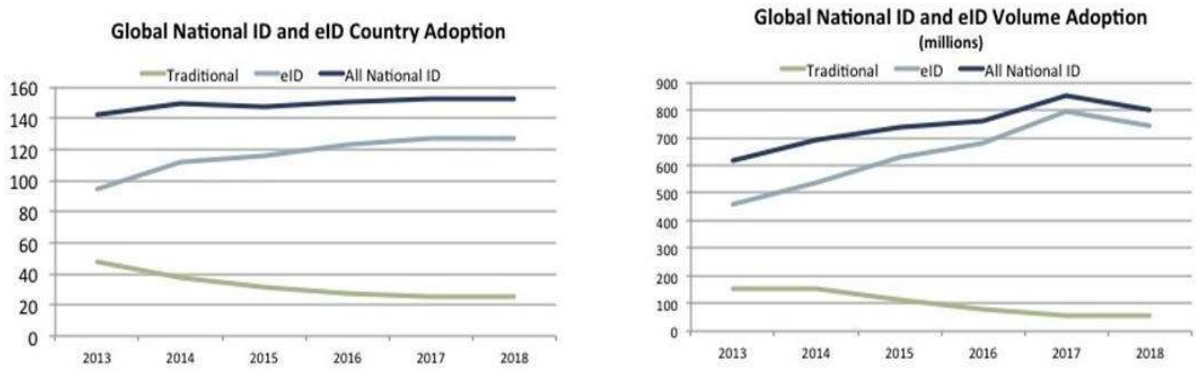


Рис.2.2 Світові тенденції використання форматів документів, що посвідчують особу за даними Acuity Market Intelligence

2.3.3 Електронна ідентифікація юридичних осіб

Окремим напрямком є рішення питань електронної ідентифікації юридичних осіб. Більшість держав-членів Європейського Союзу вимагають від юридичних осіб реєструються в так званому Комерційному регістрі (аналог українського Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців), хоча точна назва та характер сервісу змінюється в кожній державі-члені. Під час реєстрації кожна компанія отримує номер, який однозначно її ідентифікує. Деякі з цих номерів є простими послідовними, інші – номери складені, які не тільки ідентифікують компанію, а й також філій компанії.

У семи з дев'ятнадцяти країн-членів номер комерційної реєстрації представляє собою число, яке може бути використане ідентифікації компанії. Також для ідентифікації юридичної особи можуть бути використаний номер платника НДС (VAT). Крім того, для ідентифікації використовують комерційний номер або номер асоціації (Австрія, association number or commercial number), номер фонду страхування (Греція, Insurance Fund), фіскальний номер (Італія, Словаччина, Fiscal Number)

Таблиця 2.2 Кількість і тип ідентифікаторів компаній у державах Європи

Держава	Кількість ідентифікаторів	Назва ідентифікаторів

	1	2	3	
Austria			+	Commercial and associated numbers, VAT
Belgium	+			
Czech Rerublic		+		Commercial and fiscal register numbers
Estonia		+		Commercial register number and VAT
France	+			
Greece			+	Commercial register and insurance fund numbers, and VAT
Iceland	+			
Italia			+	Commercial register and fiscal numbers, and VAT
Lithuania		+		Commercial Register Number and VAT
Luxemburg	+			
Portugal	+			
Slovakia			+	Commercial and Fiscal Register Numbers, and VAT
Slovenia				Commercial register and fiscal numbers
Spain		+		Commercial register and fiscal numbers
Sweden	+			
Switzerland	+			
Netherland		+		Commercial register and fiscal numbers
Turkey		+		Commercial register and fiscal numbers
Great Britain		+		Commercial Register Number and VAT

Крім цих ідентифікаторів допускається використання і інших ідентифікаційних даних для ідентифікації юридичної особи (Таблиця 2.3).

Таблиця 2.3 Допустимі ідентифікаційні дані юридичних осіб в державах Європи

Держава	Офіційна назва	Загальна назва	Колишнє найменування	Адреса (або її частина)
Austria	Так	Ні	Ні	Ні
Belgium	Так	Ні	Ні	Так
Czech Rerublic	Так	Ні	Ні	Ні
Estonia	Так	Так	Ні	Так
France	Так	Ні	Ні	Так
Greece	Так	Так	Ні	Так
Iceland	Так	Ні	Так	Так
Italia	Так	Ні	Ні	Ні
Lithuania	Так	Ні	Ні	Ні
Luxemburg	Так	Ні	Ні	Ні
Portugal	Так	Ні	Ні	Ні
Slovakia	Так	Ні	Ні	Так
Slovenia	Так	Так	Ні	Так
Spain	Так	Так	Ні	Так
Sweden	Так	Ні	Ні	Так
Switzerland	Так	Ні	Ні	Так
Netherland	Ні	Ні	Ні	Ні
Turkey	Так	Так	Ні	Так
Great Britain	Так	Ні	Ні	Так

У більшості держав Європи дозволяється використовувати обидва ідентифікатора для бізнес-установ (Таблиця 2.2 та Таблиця 2.3). Для ідентифікації некомерційних організацій, державних установ, міністерств, тощо існують свої особливості. (Таблиця 2.4).

Таблиця 2.4 Ідентифікатори та описи державних органів у порівнянні з ідентифікаційними даними бізнес-установ

Держава	Ідентифікатори	Примітка
Austria	Різні	
Belgium	Однакові	Державні органи не є незалежними юридичними особами
Czech Rerublic	Майже	Державні органи зареєстровані в окремому реєстрі
Estonia	Однакові	
France	Однакові	
Greece	Однакові	
Iceland	Однакові	
Italia	Майже однакові	Державні органи не мають номеру VAT
Lithuania	Однакові	
Luxemburg	Однакові	
Portugal	Різні	Державні органи визначені правовим актом, який створює їх
Slovakia	Однакові	
Slovenia	Однакові	
Spain	Різні	Державні органи не зареєстровані в Комерційному реєстрі
Sweden	Однакові	
Switzerland	Однакові	
Netherland	Іноді однакові	
Turkey	Однакові	
Great Britain	Схожі або однакові	

На відміну від громадян, компанії не діють самі по собі, вони представлені посадовими особами. Тим не менше, більшість держав-членів Євросоюзу використовують засоби електронної ідентифікації для автентифікації, специфічні для бізнес-установ (Таблиця 2.5). Більшість з цих засобів є апаратними ключами, які містять

кваліфікований сертифікат для електронного підпису. Ці засоби електронної ідентифікації можуть бути використані не тільки для автентифікації, а й для підписання документів від імені компанії. Слід зауважити, що, хоча ці засоби електронної ідентифікації можуть використовуються виключно для представлення компанії, вони номінативні, тобто вони містять ідентифікаційні дані представників. Більшість з цих засобів є специфічними в конкретних секторах (фінансові, адміністративні, правові, щодо банківської справи, охорони здоров'я, тощо), а засоби для використання у різних секторах не є взаємозамінними.

У деяких державах-членах єдиний спосіб діяти від імені компанії є використання електронної ідентифікації громадянина в поєднанні з певним мандатом (Австрія, Греція, Швейцарія і Нідерланди) (Таблиця 2.5). В інших, як Бельгія, хоча є певні засоби електронної ідентифікації для компаній, вони не можуть бути використані для електронного підпису. Електронний підпис в назві компанії може бути накладено тільки за допомогою засобу електронної автентифікації разом з мандатом.

Таблиця 2.5 Держави Європи, в яких впроваджено засоби електронної ідентифікації для автентифікації бізнес-установ

Держава	Специфічний засіб електронної ідентифікації	Специфічний сектор	Підписи дозволені
Austria			
Belgium	Так		
Czech Rerublic	Так	Так	Так
Estonia	Рідко	Ні	Так
France			
Greece			
Iceland	Так		Так
Italia	Так		Так
Lithuania	Так		Так

Luxemburg	Так		Так
Portugal	Так		Так
Slovakia	Так	Так	
Slovenia	Так	Так	Так
Spain	Так		Так
Sweden	Так	Так	Так
Switzerland			
Netherland			
Turkey			
Great Britain	Так		Так

У багатьох державах, крім засобів з кваліфікованими сертифікатами, які представляють компанії, є також інші типи засобів електронної ідентифікації, які можуть бути використані для представлення компанії (Таблиця 2.6), та використовують різні схеми електронної ідентифікації.

Таблиця 2.6. Типи засобів електронної ідентифікації, що використовується для представлення бізнес-установ в державах Європи

Держава	Пароль	Пароль + ім'я	Програмний сертифікат	Кваліфікований сертифікат
Austria				
Belgium	Так			
Czech Rerublic				Так
Estonia				Так
France				
Greece				
Iceland	Так		Так	Так

Italia				Так
Lithuania				Так
Luxemburg				Так
Portugal				Так
Slovakia	Так	Так	Так	Так
Slovenia			Так	Так
Spain			Так	Так
Sweden			Так	
Switzerland				
Netherland				
Turkey				
Great Britain	Так	Так	Так	Так

Прийняття Регламенту eIDAS слугує поштовхом для провайдерів електронних послуг та провайдерів послуг електронної ідентифікації в Європейському Союзі до використання електронної печатки та кваліфікованої електронної печатки як засобів електронної ідентифікації юридичних осіб та різновиду електронного підпису під час здійснення он-лайн транзакцій.

Як нормативна новація концепція використання кваліфікованої електронної печатки дозволить вирішити питання електронної ідентифікації юридичних осіб із високим рівнем гарантій за умов впровадження інфраструктури відкритих ключів та застосування сертифікованих засобів створення кваліфікованого електронного підпису. За такою схемою, кваліфікований провайдер довірчих послуг виступає в ролі провайдера послуг електронної ідентифікації.

Варто зазначити, що в Україні концепцію використання електронної печатки як спеціального виду електронного цифрового підпису, впроваджено з початку розбудови системи електронного цифрового підпису ще у 2004 році.

2.3.1 Вплив стану розвитку систем електронної

ідентифікації на загальні рейтинги розвитку електронного урядування

Стосовно світових рейтингів розвитку електронного урядування (за щорічними оцінками Організації Об'єднаних Націй[45] та Європейської Комісії[46]) та їх залежності від рівня впровадження сервісів електронної ідентифікації, слід зазначити, що країни, які впровадили документи, що посвідчують особу для електронної ідентифікації власника, набули високих рейтингів як у розрізі рівнів розвитку інфраструктури електронної ідентифікації, так і рівнів розвитку електронного урядування взагалі.

Таблиця 2.7 Рейтинг розвитку систем електронного урядування країн Європейського Союзу, в яких впроваджено документи, що посвідчують особу для електронної ідентифікації власника

Держава	2014 UN eGov Total Rank	2014 UN eGov Development Index	2014 UN eGov Online Service Component	2014 UN Gov Telecomm. Infra structure Component	2014 UN eGov Human Capital Component	2014 EU28 eID Rating
Finland	10	0,8449	0,7717	0,8594	0,9037	0,84
Spain	12	0,841	0,9449	0,6629	0,9152	0,98
Sweden	14	0,8225	0,7008	0,8866	0,8802	0,67
Estonia	15	0,818	0,7717	0,7934	0,8889	0,86
Austria	20	0,7912	0,748	0,7597	0,866	0,89
Italy	23	0,7593	0,748	0,6747	0,8552	0,76
Belgium	25	0,7564	0,6772	0,6988	0,8932	0,71
Lithuania	29	0,7271	0,7559	0,5697	0,8557	0,79
Latvia	31	0,7178	0,7008	0,6237	0,8288	0,67
Portugal	37	0,69	0,6378	0,6094	0,8227	0,83

[45] http://unpan3.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf
[46] https://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-country-factsheets-e-government

Czech Republic	53	0,607	0,3701	0,5753	0,8755	0,39

Проте, слід зазначити, що впровадження документів, що посвідчують особу для електронної ідентифікації власника, не завжди є на 100% визначальним чинником для рейтингу розвитку інфраструктури електронної ідентифікації та електронного урядування в цілому.

Так, такі держави-члени Європейського Союзу, як Велика Британія, Франція та Данія використовують альтернативні по відношенню до документів, що посвідчують особу для електронної ідентифікації власника, засоби електронної ідентифікації та досягли найвищих показників як у європейському так і загальносвітовому рейтингу розвитку електронного урядування.

Таблиця 2.8 Рейтинг розвитку систем електронного урядування країн Європейського Союзу, в яких не впроваджено або впроваджується на етапі пілотного проектування документи, що посвідчують особу для електронної ідентифікації власника

Country	2014 UN eGov Total Rank	2014 UN eGov Development Index	2014 UN eGov Online Service Component	2014 UN eGov Telecomm. Infrastructure Component	2014 UN eGov Human Capital Component	2014 EU28 eID Rating
France	4	0,8938	1,000	0,8003	0,8812	0,62
United Kingdom	8	0,8695	0,8976	0,8534	0,8574	0,47
Denmark	16	0,8162	0,6614	0,874	0,9132	1,00
Greece	34	0,7118	0,6063	0,6549	0,8741	0,26
Hungary	39	0,6637	0,5591	0,5654	0,8668	0,38
Slovenia	41	0,6505	0,4252	0,6193	0,9072	0,71
Poland	42	0,6482	0,5433	0,5618	0,8396	0,79
Croatia	47	0,6282	0,4646	0,6271	0,7928	0,12
Slovakia	51	0,6148	0,4882	0,5296	0,8265	0,08

Cyprus	58	0,5958	0,4724	0,532	0,7828	0,42
Romania	64	0,5632	0,4409	0,4385	0,81	0,48
Bulgaria	73	0,5421	0,2362	0,5941	0,796	0,43

Наведені дані свідчать про те, що досягнення високих показників розвитку тієї або іншої сфери електронного урядування не залежить напряму від однієї конкретної технології. Показовим прикладом у цьому сенсі є Швеція, де незважаючи на те, що країна впровадила документи, що посвідчують особу для електронної ідентифікації власника, найбільшого попиту та рівня проникнення послуг набули послуги «банківської ідентифікації» (BankID). Така система, використовуючи базові принципи інфраструктури відкритих ключів, стала достойною альтернативою і нас сьогодні забезпечує надання послуг електронної ідентифікації більш ніж 90% користувачів системи електронного урядування.

Також дуже важливим є впровадження альтернативних засобів електронної ідентифікації таких як засоби мобільної ідентифікації (mobileID), що дозволяє надавати користувачам можливість вибору між засобами, робить інфраструктуру електронної ідентифікації більш гнучкою та привабливою з точки зору кінцевого користувача.

За даними GSM - Асоціації [47] у світі розгорнуто близько 20 мереж мобільного зв'язку із наданням послуг електронної ідентифікації (див. Рисунок), більшу частину з яких становлять мережі на території країни Європейського Союзу:

[47] http://www.gsma.com/

10.03.2015 0:39:51

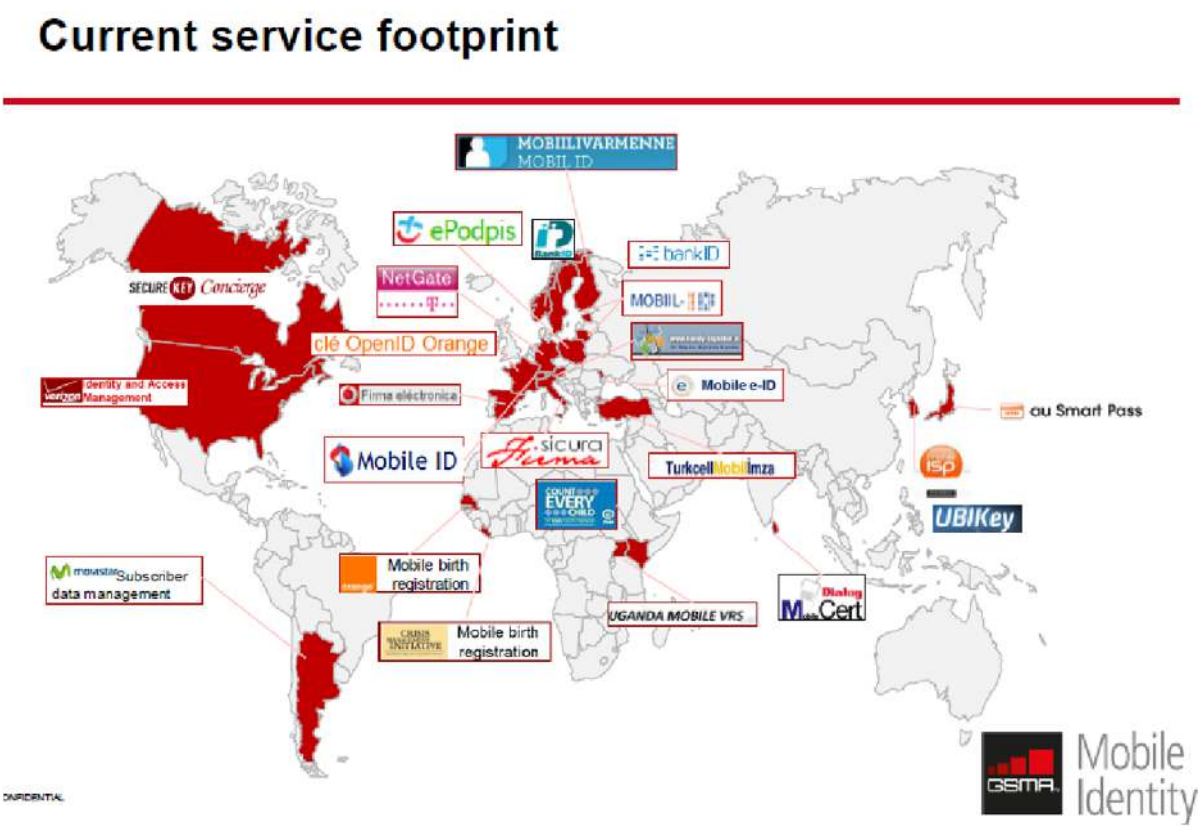


Рис.2.3 Географія мереж мобільного зв'язку, в яких надаються послуги мобільної електронної ідентифікації (moblieID).

Впровадження альтернативних засобів електронної ідентифікації розглядається як один із стимулів підвищення відсотку проникнення електронних послуг в життя населення та бізнесу. Окрім послуг банківської ідентифікації та мобільної ідентифікації в окремих країнах, наприклад, Польща, впроваджено механізми реєстрації на порталі електронних адміністративних послуг, альтернативних із кваліфікованим електронним підписом[48] .

Такий підхід впроваджено перш за все для розширення пунктів реєстрації користувачів порталу. Відповідно до прийнятого рішення, користувач має можливість створити обліковий запис на порталі, а згодом, для підтвердження свого профілю він повинен відвідати один із пунктів підтвердження профілю (розгорнуто у декількох сотнях представництвах служб соціального захисту та муніципалітетах). Як альтернатива до цього рішення діє варіант використання отриманого раніше кваліфікованого електронного підпису, завдяки чому

[48] http://epuap.gov.pl/wps/portal/E2_ZalozProfil

користувачеві можна підтвердити профіль не покидаючи робочого місця.

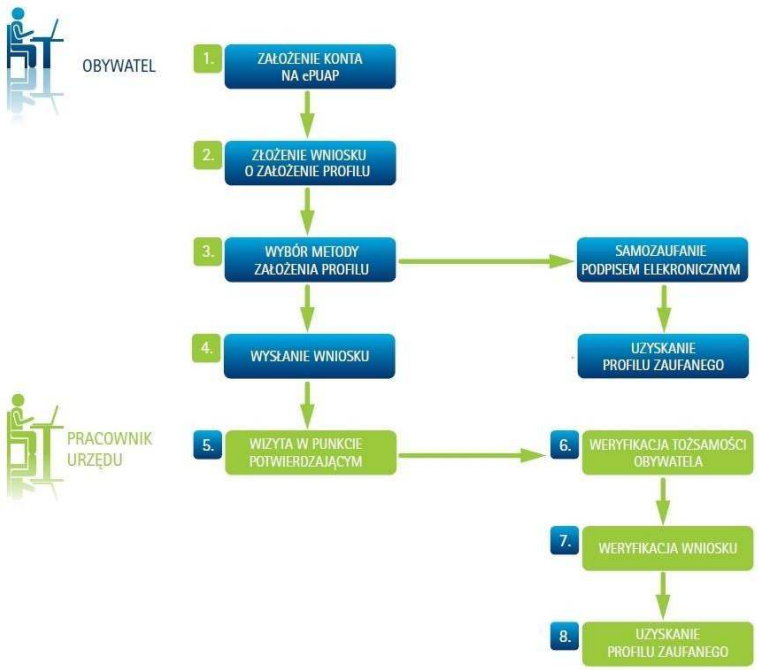


Рис.2.4 Приклад впровадження альтернативних схем електронної ідентифікації на порталі електронних адміністративних послуг у Польщі

З огляду на зазначене, під час впровадження інфраструктури електронної ідентифікації України вбачається за необхідне прийняття рішення щодо надання можливості громадянам та бізнесу вибирати схему електронної ідентифікації та мати широкий вибір місця підтвердження ідентичності. За попередніми оцінками, впровадження альтернативних механізмів електронної ідентифікації в Україні може збільшити кількість пунктів реєстрації (підтвердження ідентичності) із кількасот (пункти реєстрації споживачів послуг електронного цифрового підпису в центрах сертифікації ключів) до десятків тисяч за умов покладання функцій підтвердження ідентичності на центри надання адміністративних послуг, нотаріусів, відділення банківських установ, підрозділи служб соціального захисту населення, пенсійних установ, поштових відділень тощо.

3. Базові принципи Стратегії

Базові принципи формують основу для реалізації Стратегії, формування та досягнення цілей та задач держави у сфері електронної ідентифікації на найближчій період.

3.1 Безпечність та гнучкість технічних рішень електронної ідентифікації

Забезпечення безпеки у широкому сенсі електронної ідентифікації є дуже важливим. Використання шифрування, використання відкритих та добре перевірених стандартів безпеки, контроль процесів забезпечення безпеки спрямовані на забезпечення надійності та безпечності технічних рішень електронної ідентифікації. Засоби електронної ідентифікації повинні мати вбудовані засоби захисту, які спроможні виявляти та запобігати зловмисному вторгненню, корупції та іншим порушенням з максимальної ймовірністю.

Інфраструктура електронної ідентифікації має бути стійкою, мати можливість відновлюватися після збоїв та атак, адаптуватися до нових умов використання, та змін технологій. Важливим фактором має бути стійкість до втрати даних, навмисних атак та можливість надавати послуги після відновлення. Інфраструктура електронної ідентифікації має запобігати неавторизованим транзакціям особами та організаціями.

3.2 Інтероперабельність (сумісність)

Інтероперабельність технічних рішень повинна стати важливим стимулом постачальникам (провайдерам) електронних послуг приймати ідентифікаційні дані з різних джерел, пов’язаних між собою єдиним ідентифікатором (за аналогією приймання банком різних карт від різних емітентів). Інтероперабельність повинна забезпечити мобільність та портативність засобів електронної ідентифікації та дозволить громадянам використовувати різні засоби електронної ідентифікації та надавати їх постачальником електронних послуг.

Принцип інтероперабельності базується на виконання таких умов:

– засоби та схеми електронної ідентифікації мають відповідати відкритим стандартам;

– якщо фізична або юридична особа, програмній або апаратний засіб надає чинні та підтверджені ідентифікаційні дані, будь яка сторона, що довіряє, має прийняти ці дані у якості засобів авторизації та підтвердження особи.

У рамках інфраструктури електронної ідентифікації громадяни повинні мати можливість проводити он-лайн транзакції через різних провайдерів електронних послуг. Крім того, інтероперабельність має забезпечити у перспективі і транскордонність електронної ідентифікації.

Існує три типи вимог до забезпечення інтероперабельності:

– технічна інтероперабельність (функціональна сумісність) – можливість взаємодії та обміну даними між різними технологіями, що заснована на добре визначених та широко розповсюджених стандартах, форматах, протоколах та інтерфейсах;

– семантична інтероперабельність – спроможність кожної сторони до передачі даних та розуміння стороною, що приймає дані, сутності та сенсу отриманого повідомлення;

– інтероперабельність політик – сумісність загальних ділових правил та процесів, що пов’язані з передачею, отриманням та прийняттям даних між системами, що підтримуються відповідною нормативною базою.

Держава повинна заохочувати використання відкритих стандартів для забезпечення інтероперабельності. Рішення електронної ідентифікації мають бути модульними, що дозволить постачальникам послуг створювати складні системи ідентифікації. Це забезпечить гнучкість, надійність та можливість повторного використання таких систем, забезпечує простоту та ефективність в управління змінами.

3.3. Забезпечення конфіденційності особистої інформації та персональних даних

Суть принципу забезпечення конфіденційності особистої інформації та персональних даних міститься у тому, що під час здійснення он-лайн транзакцій або отримання електронних послуг

має бути забезпечено можливість надання тільки тих даних, які потрібні для отримання такої послуги або здійснення транзакції. Наприклад, для купівлі білету до кінотеатру необхідно надати докази лише того, що людина досягнула 18 річного віку, але не важливе її місце проживання, статус або інші данні. Подібні аспекти, які порушують конфіденційність персональних даних, мають бути максимально усунені під час надання електронних послуг та здійснення он-лайн транзакцій.

Діяльність постачальників (провайдерів) послуг електронної ідентифікації та електронних послуг має будуватися на основі таких принципів забезпечення конфіденційності особистої інформації та персональних даних:

- прозорість: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг мають бути прозорими в контексті своєї діяльності та інформувати осіб щодо збору, використання, розповсюдження та технічної обробки їх персональних даних;
- особиста участь: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг мають відкрито та безперешкодно залучати конкретних осіб у процес використання їх персональних даних та узгоджувати з ними збір, використання, розповсюдження та технічну обробку персональних даних. Також ці суб'єкти повинні надавати механізми забезпечення доступу, корегування та відновлення персональних даних;
- уточнення мети: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, мають вказати орган, який уповноважив їх збирати персональні дані, а також мету збору, використання та обробки персональних даних.
- мінімізація даних: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, мають використовувати тільки ті дані, які мають безпосереднє відношення та необхідні для вказаної мети та зберігати персональні дані тільки протягом часу, який необхідний для виконання вказаної задачі;
- обмежене використання: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, мають використовувати персональної дані виключно з метою,

що вказана у повідомленні про мету обробки. Обмін персональними даними має здійснюватися виключно в межах цілей, для яких були надані персональні дані;

- якість та повнота даних: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, шляхом проведення процедур верифікації мають переконатися в тому, що ідентифікаційні дані є точними, актуальними, своєчасними та повними;

- безпека: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, мають впроваджувати комплекс організаційних та технічних заходів для захисту персональних даних (на будь яких носіях та середовищі) та надавати відповідні рівень гарантій безпеки відносно ризиків втрати, несанкціонованого доступу або зловживання, знищення, зміни, ненавмисного або навмисного розголошення персональних даних;

- підзвітність та аудит: суб'єкти, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, мають нести відповідальність за додержання наведених умов, забезпечувати підготовку всіх своїх співробітників та контрагентів, що використовують персональні дані, контролювати фактичне використання персональних даних та демонструвати виконання принципів та вимог забезпечення конфіденційності персональних даних.

Впровадження цих принципів у практику діяльності постачальників (провайдерів) послуг електронної ідентифікації та електронних послуг є основою свідомого вибору громадянами щодо використання особистої інформації у кіберпросторі. Прийняття цих принципів також гарантує:

- обмеження збору персональних даних організаціями, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг;

- використання та розповсюдження лише тієї особистої інформації, яка дійсно необхідна для надання конкретної електронної послуги або здійснення он-лайн транзакції;

- потрібний рівень захисту особистої інформації та рівень гарантій безпеки;

– відповідальність та підзвітність суб'єктів, що є постачальниками (провайдерами) послуг електронної ідентифікації та електронних послуг, перед власниками особистої інформації.

Повна реалізація наведених вище принципів є основою побудови довірчої інфраструктури електронної ідентифікації у кіберпросторі України та забезпечити відповідних рівень гарантій безпеки персональних даних.

3.4. Добровільність використання спеціальних (захищених) засобів електронної ідентифікації

Усвідомлюючи важливість проблеми забезпечення захисту персональних даних та особистої інформації, використання спеціальних більш захищених рішень з електронної ідентифікації має бути добровільним як для юридичних, так і для фізичних осіб. Держава на має зобов'язувати організації впроваджувати спеціальні ідентифікаційні рішення для надання он-лайн послуг, а також змушувати громадян отримувати захищені засоби електронної ідентифікації, якщо вони не бажають приймати участь у он-лайн операціях підвищеного ризику, що надають державні органи або приватні підприємства. Інфраструктура електронної ідентифікації має охоплювати увесь спектр можливих операцій, від анонімних, до тих, що передбачають високий рівень захищеності та гарантій безпеки.

3.5. Економічність та простота технічних рішень

Створення інфраструктури електронної ідентифікації має усунути проблему, що пов'язана з використанням та управлінням фізичною особою великою кількістю облікових записів та паролів для виконання он-лайн транзакцій та отримання електронних послуг. Такий стан справ підвищує ризик втрати реєстраційного запису (аккаунту) та розкриття (втрати) паролів.

В рамках інфраструктури електронної ідентифікації держава повинна буди розповсюджувати (або підтримувати таке розповсюдження) засоби електронної ідентифікації, сприяти скороченню різноманітних електронних баз та реєстрів, які потребують різних способів та типів ідентифікації.

Фізичні та юридичні особи будуть мати свою вигоду, яка полягає у скороченні кількості облікових даних, яки можуть бути використання для взаємодії з різними постачальниками електронних послуг. Державні установи та приватні підприємства також будуть мати вигоду, яка полягає у скороченні випуску різних ідентифікаційних даних, що потребують локального управління та розробки (закупівлі) спеціального програмного та апаратного забезпечення, технічного обслуговування тощо. Рішення електронної ідентифікації мають будуть вигідними для всіх зацікавлених сторін, тому що спрямовані на зниження ризиків шахрайства с ідентифікаційними даними, зниження витрат на підтримку процесів, що вимагають паперового документообігу, більш оптимальне використання існуючих інфраструктур та систем (системи електронного цифрового підпису, систем ідентифікації клієнтів великих банків, системи ідентифікації клієнтів компаній мобільного зв'язку тощо). Цю сприятиме зниженню вартості впровадження засобів та схем електронної ідентифікації, збільшення доходів від інвестицій у ринок електронних послуг.

Схеми та засоби електронної ідентифікації мають бути інтуїтивно зрозуміли, прості використанні та спиратися на технології, що вимагають мінімальної підготовки з боку потенційних користувачів. Постачальники (провайдери) послуг електронної ідентифікації мають проводити дослідження щодо оцінки привабливості для користувачів (usability). Для досягнення легкості та швидкості впровадження засобів електронної ідентифікації необхідно використовувати існуючи компоненті різних систем (мобільні телефони, банківські картки, персональні комп'ютері, планшети тощо). Бажано, щоб створювані рішення електронної ідентифікації були інтегровані із існуючими схемами електронної ідентифікації.

4. Основні цілі та завдання реалізації Стратегії

Стратегія спрямована на досягнення таких цілей.

1. Побудова інфраструктури електронної ідентифікації в Україні.

2. Забезпечення інтероперабельності (сумісності) інфраструктури електронної ідентифікації.

3. Створення довірчого середовища у кіберпросторі України та мотивування громадян до використання електронних послуг.

4. Забезпечення сталого розвитку національної інфраструктури електронної ідентифікації та пов'язаних з нею інших електронних послуг.

Перші дві цілі спрямовані на проектування та створення національної інфраструктури електронної ідентифікації та управління нею для надання громадянам, приватному та державному сектору національної економіки електронних послуг.

Третя мета спрямована на забезпечення конфіденційності, цілісності, доступності ті інших властивостей, що пов'язані із безпекою інформації у кіберпросторі держави та захисту конституційних прав громадян під час використання електронних послуг, а також на широку освіту громадян, для успішного впровадження інноваційних технологій електронної ідентифікації та електронних послуг.

Четверта мета спрямована на визначення державних пріоритетів щодо сталого розвитку та удосконалення інфраструктури електронної ідентифікації, пов'язаних з нею інших систем (наприклад, системи електронного цифрового підпису) та удосконалення безпеки електронної ідентифікації.

4.1 Побудова інфраструктури електронної ідентифікації

Побудова інфраструктури електронної ідентифікації має забезпечити гарантії ідентичності учасників он-лайн транзакцій та споживачів електронних послуг в Україні. Створення інфраструктури електронної ідентифікації спрямоване на:

– мотивування провайдерів електронних послуг будувати процеси автентифікації перш за все на основі розуміння ризиків, що пов'язанні з он-лайн транзакціями у кіберпросторі, а не на основі власних бізнес-потреб;

– забезпечення загальної правової, організаційної та технологічної основи створення довірчої ідентифікації серед учасників он-лайн транзакцій та споживачів електронних послуг;

– впровадження в Україні національних, європейських та міжнародних стандартів, що забезпечують достатній рівень взаємодії (технологічної, семантичної, організаційної тощо) між провайдерами електронних послуг;

– усунення невизначеності стосовно відповідальності за випуск засобів електронної ідентифікації, атрибутів, ідентифікаційних даних тощо.

Для досягнення першої мети необхідно вирішити таки завдання.

Розробка та прийняття стандартів електронної ідентифікації та автентифікації, що засновані на моделях ризику. Розробка та застосування національних стандартів електронної ідентифікації та автентифікації є дуже важливим для забезпечення стабільності, надійності та безпеки інтернет-середовища. Модель ризиків необхідна для оцінки та адаптації рівня безпеки у залежності від ризиків електронної ідентифікації та електронних послуг. Також модель ризиків необхідна для розуміння потрібного рівня захищеності електронних послуг, на основі моделі (типів) загроз та потенційного рівня наслідків (втрат) під час проведення електронних транзакцій. Національні стандарти мають бути гармонізовані з міжнародними та європейськими стандартами та визначати організаційні заходи та механізми електронної ідентифікації користувачів, інформаційних систем та засобів через відкриті мережі, їх автентифікації, забезпечувати необхідний рівень інтероперабельності та безпеки, зберігаючи при цьому спроможність до адаптування до нових загроз безпеки та нових технологій.

Визначити та нормативне закріпити відповідальності постачальників (провайдерів) послуг електронної ідентифікації та встановлення механізмів підзвітності. Норми національного законодавства повинні визначити права та обов'язки всіх учасників інфраструктури електронної ідентифікації та створити правові, організаційні та технічні механізми спонукання до їх дотримання.

Уряд має вирішити питання відповідальності в рамках інфраструктури електронної ідентифікації центральних та місцевих органів влади, провайдерів електронних послуг, громадян, а також встановити механізми підзвітності стосовно надання та споживання послуг електронної ідентифікації. Нові нормативно-правові акти повинні зберігати гнучкий підхід щодо забезпечення безпеки інформації, що є власністю держави, та інформації, що не є власністю держави.

4.2 Забезпечення інтероперабельності (сумісності) інфраструктури електронної ідентифікації

Підтримка інтероперабельності є важливим елементом створення довірчої ідентифікації між учасниками інфраструктури електронної ідентифікації. Вирішення проблем інтероперабельності спрямовано на:

- забезпечення високих темпів впровадження рішень електронної ідентифікації для забезпечення безпечного та спрощеного доступу до он-лайн послуг;
- розробку та впровадження широкого спектру рішень на основі електронної ідентифікації, які придатні для сумісного функціонування;
- розробку та впровадження безпечних, зручних, орієнтованих на користувача варіантів ідентифікації та автентифікації користувача;
- зниження вартості реалізації рішень, що буде сприяти швидкому зростанню ринку послуг електронної ідентифікації та електронних послуг в Україні.

Для досягнення другої мети необхідно вирішити таки завдання.

Продовжувати Урядом керівні дії та прийняття Стратегії. Держава та Уряд України повинні стати найбільшими постачальниками та споживачами електронних послуг. Тому центральні та місцеві органи влади мають виступати основними «драйверами» впровадження послуг електронної ідентифікації та електронних послуг, виступати лідерами у галузі рішень щодо електронної ідентифікації та надання електронних послуг. Таки дії влади будуть сприяти зростанню споживчих сподівань та запиту на нові електронні послуги. Держава також має виступати у якості

важливого споживача електронних послуг приватного сектору, з метою покращення бізнес-пропозицій та ринку таких рішень.

Сприяти прискореному розгортанню eID-інфраструктури, впровадженню технічних рішень та реалізації Стратегії. Уряд має заохочувати та стимулювати швидку реалізацію рішень, що підтримують електрону ідентифікацію та електронні послуги. Зусилля у цій області будуть сприяти впровадженню інновацій на ринку та прискорять темпи впровадження процесів та засобів електронної ідентифікації, сприятимуть впровадженню нових електронних послуг та формуванню електронного ринку України. Уряд має взаємодіяти з промисловістю, банківським та ІТ-сектором з метою організації, координації та фінансування експериментальних програм та розробок, яки можуть сприяти швидкому зростанню ринку інтероперабельних електронних послуг, яки будуть надаватися з боку багатьох спільнот та приватного сектору.

Сприяти широкої доступності рішень для укріплення довірі між учасниками eID-інфраструктури. Необхідно ще на етапі проектування та пілотного використання забезпечити інтероперабельність між постачальниками електронних послуг. Основним критерієм для впровадження схем та засобів електронної ідентифікації має бути зручність для користувача (usability). Уряд має прийняти заходи щодо стимулювання всіх рівнів взаємодії між учасниками інфраструктури електронної ідентифікації, сприяти її широкому використанню всіма громадянами України.

4.3. Створення довірчого середовища у кіберпросторі України та мотивування громадян до використання електронних послуг

Необхідно формувати середовище довіри у кіберпросторі держави шляхом запровадження механізмів забезпечення конфіденційності, цілісності та доступності даних, що пов’язані з ідентифікацію та автентифікацією громадян, а також використанням електронних послуг. Під час проведення просвітницьких заходів серед населення, впровадження програм з обізнаності суспільства про переваги використання електронної ідентифікації, необхідно врахувати інтереси громадян, приватного сектору та держави. Створення довірчого середовища спрямоване на:

- забезпечення конфіденційності персональних даних та іншої інформації, запобігання несанкціонованого збору, накопичення, використання та розповсюдження ідентифікаційних даних громадян;
- забезпечення захисту інтелектуальної власності;
- підвищення інформованості широкого кола користувачів про електрону ідентифікацію та електронні посвідчення громадянина.

Для досягнення цієї мети необхідно вирішити таки завдання.

Забезпечити конфіденційність та безпеку он-лайн транзакцій. Реалізація Стратегії має забезпечити конфіденційність та безпеку особистої інформації громадян та впровадити чіткі правила та керівні принципи щодо обміну постачальниками послуг та сторонами, що довіряють, особистою та іншою інформацією, а також визначення того, якою інформацією вони можуть обмінюватися. Ці заходи підтримують гарантії держави щодо захисту користувачів від зловживань та несанкціонованого розкриття їх особистої інформації, а також упевненості приватних осіб в їх захищеності під час виконання електронних транзакцій. Це сприятиме більш широкому використанню технологій електронної ідентифікації.

Забезпечити обізнаність та відповідний рівень освіти (компетентності) користувачів (громадян) для свідомого застосування електронної ідентифікації. Необхідно докладати зусиль щодо інформованості та навчання користувачів використовувати механізмі електронної ідентифікації. Уряд у співробітництві із приватним сектором має адаптувати зусилля щодо просвітницької діяльності та підвищенню обізнаності населення щодо електронної ідентифікації враховуючі демографічні особливості. Необхідно впроваджувати просвітницькі програми, які забезпечать обізнаність користувачів про переваги та ризики використання електронної ідентифікації, методи захисту користувачів, та іншу інформацію. Необхідно проводити відповідну роботу серед провайдерів електронних послуг, особливо стосовно забезпечення конфіденційності, цілісності та доступності інформації. Уряд, державні та приватні навчальні заклади, приватний сектор мають розвивати освітні ресурси для малого та середнього бізнесу з метою забезпечення стабільності функціонування інфраструктури електронної ідентифікації. Провайдери послуг мають розуміти свою

відповідальність щодо укріплення довіри до інфраструктури. Просвітницька та освітня програми мають бути спрямовані на широке коло користувачів, усувати відповідні ризики, забезпечувати готовність користувачів використовувати новітні технології та адаптуватися до розвитку технологій електронної ідентифікації та електронних послуг.

4.4 Забезпечення сталого розвитку національної інфраструктури електронної ідентифікації та пов'язаних з нею інших електронних послуг

Враховуючі глобальний характер економічних відносин, правові, організаційні та технічні рішення, ще є підґрунтям розвитку національної інфраструктури електронної ідентифікації виходять за національні рамки. Для створення інфраструктури електронної ідентифікації необхідно реалізовувати рішення на національному та міжнародному рівнях, у тому числі розробляти та гармонізувати національні стандарти, проводити дослідження та розробки, координувати державні та комерційні програми. Уряд України має прийняти на себе керівництво, координацію зусиль та співробітництво в області розробки, впровадження та використання засобів електронної ідентифікації з метою впровадження процесів електронної ідентифікації, а також реалізовувати цільові державні програми для впровадження таких рішень. Досягнення цієї мети спрямовано на:

- планування та надання достатніх ресурсів для розробки національних стандартів та участі у розробці міжнародних стандартів в сфері електронної ідентифікації, електронного цифрового підпису та електронних довірчих послуг;
- надання достатніх ресурсів для проведення наукових досліджень та розробок щодо створення інноваційних технологій електронної ідентифікації;
- удосконалення координації між державними та недержавними програмами та заходами, що пов'язані з впровадженням засобів та схем електронної ідентифікації.

Для досягнення цієї мети необхідно вирішити таки завдання.

Здійснювати координацію заходів Уряду щодо впровадження засобів електронної ідентифікації та

електронних посвідчень на національному та міжнародному рівнях. Уряд України має докладати зусилля щодо створення безпечного кіберпростору держави. Необхідно координувати зусилля на місцевому та центральному рівнях щодо протидії кіберзлочинності та кібертероризму. Випуск засобів електронної ідентифікації, впровадження схем електронної ідентифікації мають спиратися та враховувати відповідні заходи щодо забезпечення кібербезпеки. Крім того, Уряд має координувати свою діяльність щодо забезпечення кібербезпеки з відповідними міжнародними програмами та політиками. Шляхом управління та координації національних зусиль, а також участю у міжнародних заходах, Уряд має впроваджувати єдиний підхід у галузі довіреної електронної ідентифікації.

Розширювати співробітництво в галузі розробки технічних стандартів на національному, регіональному та міжнародному рівнях. Подальший прогрес та інновації у галузі впровадження засобів електронної ідентифікації та електронних послуг залежить від участі України у розвитку національних стандартів, гармонізації європейських та міжнародних стандартів у галузі інформаційних технологій. Це забезпечить інтероперабельність рішень та транскордонність електронної ідентифікації, прискорить інтеграцію національної інфраструктури електронної ідентифікації у європейську та міжнародну, а також інтеграції національного цифрового ринку у європейський. Національна інфраструктура електронної ідентифікації має бути функціонально сумісна з європейською, спрямована на адаптацію із законами та політиками Європейського Союзу. Зусилля у цьому напрямку мають сприяти розвитку технічних стандартів для ідентифікації та автентифікації організацій, засобів, програмного забезпечення, даних та користувачів.

Стимулювати інновації шляхом активних наукових досліджень. Уряд має узгоджувати існуючі та перспективні цільової програми з дослідження та розвитку технологій електронної ідентифікації, автентифікації та електронних послуг. Результати досліджень, що будуть отримані у рамках державних програм, мають активно впроваджувати у тому числі і через приватний сектор. Заходи щодо досліджень мають бути широкими, об’єднувати зусилля наукової спільноти, виробництва у державному та приватному секторі з метою швидкої розробки та впровадження нових інноваційних технологій.

10.03.2015 0:39:51

5. Переваги, що надає реалізація Стратегії

Значущість технологій електронної ідентифікації для громадян, приватного сектору та держави є тісно взаємопов'язаною. Широке розповсюдження електронних послуг та електронної ідентифікації надасть переваги всім сторонам, що є учасниками системи. На національному рівні, враховуючи все більшу залежність економіки та критичної інфраструктури від Інтернет-технологій, будь які ініціативи, які спрямовані на підвищення безпеки інформаційного та кіберпростору держави мають позитивний вплив на рівень національної безпеки та стабільність економічного розвитку держави.

Переваги, що надає побудова та впровадження системи електронної ідентифікації розглядаються на рівні фізичної особи (громадянина), приватного сектору та держави (уряду).

5.1 Переваги для фізичних осіб

Громадяни використовують Інтернет з різними цілями та володіють різним рівнем технічних навичок. Громадяни очікують безпечного та простого у використанні Інтернет-середовища. Це передбачає перш за все конфіденційність даних та безпеку, а також те, що електронна ідентифікація не створює надзвичайних складнощів та незручностей для фізичних осіб. Таким чином концентрація уваги на прикладному рівні технології електронної ідентифікації є ключовим фактором успіху реалізації Стратегії. Переваги для фізичних осіб полягають у наступному.

З точки зору безпеки. Постачальники ідентифікації та електронних послуг з використанням вбудованих технологій захищають персональні та особисті данні фізичних та юридичних осіб. Технології захисту є стандартизованими, перевіреними та використовуються для захисту інтересів громадян. Безпека забезпечуються шляхом використання надійної ідентифікації та автентифікації всіх сторін (фізичних та юридичних), що приймають участь у електронної транзакції.

З точки зору ефективності діяльності. Фізичні особи отримують доступ до більшої кількості послуг з більш широким спектром операцій. При цьому зменшуються часові витрати та зростає продуктивність.

З точки зору надійності (гарантій безпеки). Удосконалені ідентифікаційні рішення знижують психологічний ефект страху перед шахрайством, що пов'язаний з крадіжкою особистих даних або іншими зловживаннями. Користувачі відчувають комфорт під час здійснення ділових електронних операцій та добровільно приймають участь в он-лайн транзакціях.

З точку зору конфіденційності. Без необхідності постачальники ідентифікації, електронних послуг не збирають, не використовують та не передають особисту інформацію громадян. Вони приймають заходи щодо захисту або несанкціонованого розкриття особистих даних фізичних осіб. Крім того, на особисті дані не залишається ніяких посилань у постачальника послуг, кріс тих випадків, коли це необхідно.

З точку зору свободи вибору. Фізичні особи мають свободу вільного вибору варіанту електронної ідентифікації та постачальника ідентифікації (електронна картка, мобільна ідентифікація тощо). Фізичні особи також мають право вільного вибору способу ідентифікації – анонімно або з підтвердженням своєї особи.

5.2 Переваги для юридичних осіб приватного сектору

Приватний сектор включає підприємства, некомерційні, неурядові організації, правозахисні групи та асоціації. Реалізація Стратегії розширює можливості цих організацій бути гнучкими, інноваційними та ефективно реагувати на зміну ринкового середовища. Стратегія спрямована на підтримку зусиль приватного сектору у сфері підвищення досвіду громадян у використання електронних послуг та операцій у різних секторах економіки (торгівля, фінансові послуги, побутові послуги тощо). Система електронної ідентифікації забезпечує приватному сектору гнучкі механізми управління облікових даних та атрибутів, що необхідна для їх клієнтів. Переваги для приватного сектору будуть змінюватися у залежності від ролі тієї або іншої організації в системі електронної ідентифікації (наприклад, буди постачальником ідентифікації або постачальником електронних послуг).

Переваги для приватного сектору полягають у наступному.

У сфері безпеки. Надійні ідентифікаційні рішення зменшать втрати, що пов'язанні з шахрайством, забезпечують більш високий рівень інтелектуальної власності та конфіденційність інформації, що передається між учасниками електронних послуг.

З точки зору ефективності діяльності. Використання електронних ідентифікаторів та визначених процесів ідентифікації та автентифікації підвищують продуктивність за рахунок скорочення паперових процесів та витрат на управляння обліковими даними та паролями. Оптимізація діяльності та підвищення її ефективності мають позитивний вплив на акціонерну вартість компанії, конкурентоспроможність та привабливість на ринку.

З точки зору надійності (гарантій безпеки). Впровадження технічних рішень електронної ідентифікації знижує ризик порушень безпеки та підвищує рівень довіри приватного сектору та його клієнтів до електронних операцій. Клієнти та приватні компанії розуміють ризики, розділяють їх та приймають більш оптимальні та раціональні рішення.

З точки зору конфіденційності даних. Впровадження технічних рішень електронної ідентифікації знижую складність управління та обслуговування персональних даних клієнтів та персоналу компанії. Це, в свою чергу, знижує ризик порушень конфіденційності даних.

З точки зору інновацій. Впровадження системи електронної ідентифікації створює нові ринкові можливості для приватних компаній у вигляді надання нових інноваційних високотехнологічних послуг. Компанії які перші впроваджують нові послуги з використанням системи електронної ідентифікації отримують ринкові переваги.

5.3 Переваги для державних органів

Всі органі влади – центральні, регіональні, місцеві – мають можливість виступати лідерами у впровадженні електронних послуг та реалізації технічних рішень електронної ідентифікації.

Безпека електронних послуг та електронних операцій є складовою національної безпеки, тому уряд в межах повноважень має безпосередньо впливати на забезпечення безпеки електронної ідентифікації та електронних послуг.

Переваги для уряду полягають у наступному.

З точки зору безпеки. За рахунок підвищення надійності ідентифікації та автентифікації всіх учасників електронних операцій, фізичних так і юридичних, підвищується загальний рівень безпеки у кіберпросторі держави.

З точки зору надійності (гарантій безпеки). Надійні технічні рішення електронної ідентифікації зменшують кількість кіберзлочинів в Інтернет середовищі, підвищують стійкість та цілісність систем та мереж та підвищують загальний рівень безпеки споживачів. Система електронної ідентифікації забезпечує юридичні механізми розслідування кіберзлочинів, шахрайства у результаті незаконного або неправильного використання системи електронної ідентифікації.

З точки зору ефективності діяльності державних органів влади. Система електронної ідентифікації надає можливість центральним та місцевим органам влади надавати більш якісні адміністративні послуги громадянам, виконувати відповідні державні та адміністративні функції, скорочувати та підвищувати відповідні процеси державного та місцевого управління.

*З токи зору іннов*ацій. Зобов'язання держави впроваджувати пілотні проекти надання електронних адміністративних послуг на базі системи електронної ідентифікації, сприяти впровадженню

електронних послуг у повсякденну практику, підтримувати наукові дослідження та інноваційних розробок приводить до інноваційного розвитку ринку електронних послуг та до позитивного впливу на рівень кібербезпеки держави та суспільства у довготривалої перспективі. Крім того впровадження таких технологій в систему освіти, охорони здоров'я та навколишнього середовища мають позитивний соціальний ефект та приводять до інноваційного розвитку соціально значущих сфер життєдіяльності суспільства.

6. Ключові фактори успіху впровадження рішень з електронної ідентифікації

Ефективна реалізація технічних рішень з електронної ідентифікації залежить від багатьох факторів. Конкретні рішення з електронної ідентифікації можуть виступати як в ролі каталізаторів активного провадження електронної ідентифікації та послуг, так і перешкодою. Серед таких факторів можна виділити кількість послуг, що будуються на базі електронної ідентифікації, простота використання механізмів електронної ідентифікації та сприйняття населення корисності такої послуги, доступність різних варіантів технічних рішень електронної ідентифікації, суб'єктивне сприймання загроз безпеці та конфіденційності.

До основних факторів успіху впровадження системи електронної ідентифікації відносяться.

Доступність послуг.

Доступність послуг, які будуть спиратися на рішення електронної ідентифікації є фактором позитивного впливу на поширення засобів електронної ідентифікації серед населення. Збільшення кількості послуг, доступних до користувачів через механізми електронної ідентифікації є результатом партнерства держави з приватним бізнесом. Прикладами ефективної співпраці держав та приватного бізнесу є Бельгія, Естонія, Німеччина, Литва де емітент ідентифікації тобто держава, дозволяє пропонувати приватному бізнесу свої послуги використовуючи інфраструктури електронної ідентифікації. Так у Бельгії за допомогою державної картки електронної ідентифікації надається понад 600 електронних послуг з боку приватних підприємств.

У деяких країнах емітентом електронної ідентифікації може виступати не тільки держава, а і приватні установи (наприклад BankID – ініціатива банківських установ, PKI MobileID – сумісна ініціатива операторів зв'язку, банків та центрів сертифікації ключів). Це також позитивно впливає на прийняття населенням електронної ідентифікації, тому що громадяни можуть підключатися до порталу адміністративних (державних) послуг використовуючи вже існуючі комунікаційні канали, які обладнані банківськими установами або операторам мобільного зв'язку. Такий підхід є успішним не тільки із-за того, що він заощаджує час та гроші, але й тому, що він впливає на більш широке застосування електронної ідентифікації серед

населення. Крім того, використовуючи одні і ті ж самі засоби (банківська картка, картка мобільного зв'язку тощо) для отримання великої кількості електронних послуг, допомагає користувачам зрозуміти переваги використання електронної ідентифікації, формує навички використання електронних послуг.

Легкість та простота використання рішень з електронної ідентифікації.

Засоби електронної ідентифікації мають бути простими у використанні. Встановлення та підтримка в актуальному стані програмного забезпечення, драйверів пристроїв для зчитування старт-карток, сертифікатів на свій комп'ютер сприймається користувачем як громіздке рішення. Необхідно прагнути реалізовувати як можливо простіші та легкі у використання рішення. З цієї точки зору схеми типу «логін-пароль» або одноразовий пароль (OTP) схеми ідентифікації є досить зручними, але менш безпечними у порівнянні зі схемами, що засновані на інфраструктурі відкритих ключів (PKI) або на сертифікатах атрибутів.

Враховуючі вимоги зручності для користувачів (usability) у Швейцарії, наприклад, впроваджені два типа засобів електронної ідентифікації на основі PKI – міні смарт-картки, яка може використовуватися за допомогою пристрою для зчитування з USB портом, та Plug&Play USB-токен, для цифрового підпису.

Мобільні рішення поліпшують сприйняття засобів електронної ідентифікації, що засновані на PKI, оскільки користувач не залежить від комп'ютера або пристрою для зчитування смарт-карт для здійснення он-лайн транзакції. Оскільки в Україні вже існує система ЕЦП, то можуть бути запропоновані протоколи автентифікації «на лету». Якщо у майбутньому можна буде за допомогою мобільних рішень здійснювати і цифровий підпис, то це тільки розширить спектр електронних послуг, що будуть надаватися провайдерами.

Сприйняття корисності.

Важливо, щоб рішення електронної ідентифікації мали явні переваги, які добре сприймаються громадянами. З точки зору громадянина рішення електронної ідентифікації мають сприйматися як корисні, які дозволяють громадянину економити час або гроші (наприклад, шляхом отримання послуги в електронному вигляді, замість того, щоб йти в державну установу або службу).

Необхідно враховувати, що з початку он-лайн автентифікація цінується користувачем у зв'язку з послугами, які надають емітенти

карт. Але чим більше електронних послуг (державних та приватних) буде доступно користувачеві, тим вище буде рівень сприйняття корисності.

Для підвищення мотивації використання засобів електронної ідентифікації реалізують різні підходи. Наприклад в Португалії національна карта електронної ідентифікації об'єднує п'ять попередніх карт (ID карту, податкову картку, картку соціального страхування, картку для голосування і картку соціальних послуг).

У Росії майбутня «універсальна картка" буде об'єднувати декілька функціональних карт: посвідчення особи, водійські права, картку медичного страхування, банківську картку, транспортну картку, податкову картку і медичну карку для використання в аптеках. Схожі підходи, у той або інший обсяг, існують або плануються в ряді інших європейських країн: Бельгія (транспортні карки), Естонія (проїзний квиток, картка для голосування, водійське посвідчення), картки медичного страхування (Фінляндія).

Наявність різних способів електронної ідентифікації .

Архітектура інфраструктури електронної ідентифікації має передбачати можливість використання декілька варіантів (способів) електронної ідентифікації. Це буди сприяти поширенню послуг на базі електронної ідентифікації серед громадян. У багатьох європейських країнах, паралельно доступно декілька типів засобів електронної ідентифікації.

Витрати переходу на інші способи електронної ідентифікації .

Витрати переходу, що пов'язані з новим рішенням електронної ідентифікації включають в себе вартість нового засобу та іншого устаткування та час, який необхідно витрати для навчання використовувати нову технологію.

Час, витрачається на навчання та перехід на використання іншого засобу або технології, впливає на прийняття рішення з боку користувача на використання нового засобу, особливо коли є значний технологічний розрив між рішенням, що використовувалось раніше і новим рішенням. Якщо рішення з точку споживчих якостей та зручності схожі, то перехід пройде скоріше та безболісно. Наприклад, впровадження електронної ідентифікації у вигляді BankID у деяких країнах було дуже успішним завдяки використанню банківських кратк та технологій для здійснення он-лайн платежів як звичних для населення. Іншим вдалим прикладом е використання технологій PKI, яка використовуються у фіскальних органах.

Сприйняття загроз безпеці та конфіденційності.

Важливим фактором успішного впровадження рішень електронної ідентифікації є рівень сприйняття громадянами загроз безпеці та конфіденційності. Від розуміння населенням існуючих загроз безпеці інформації у кіберсередовищі залежить його тяготіння до використання надійних та безпечних засобів електронної ідентифікації. Необхідно сформувати довірче середовище та інформувати громадян про безпеку використання нових рішень і електронних послуг.

7. Концепція інфраструктури електронної ідентифікації України

7.1 Базова модель електронної ідентифікації

На сьогодні визначено три базові моделі електронної ідентифікації за ознакою відповідальності за збереження ідентифікаційних даних[49].

Модель, орієнтована на користувача (Рис 7.1). В цій моделі саме користувач бере на себе відповідальність за генерацію та підтримку ідентифікаційних даних перед постачальниками послуг електронної ідентифікації та постачальниками електронних послуг. Ідентифікаційні дані надаються виключно за запитом постачальника послуг та якщо користувач у явному виді дає на це згоду. Користувач завжди є власником свої ідентифікаційних даних.

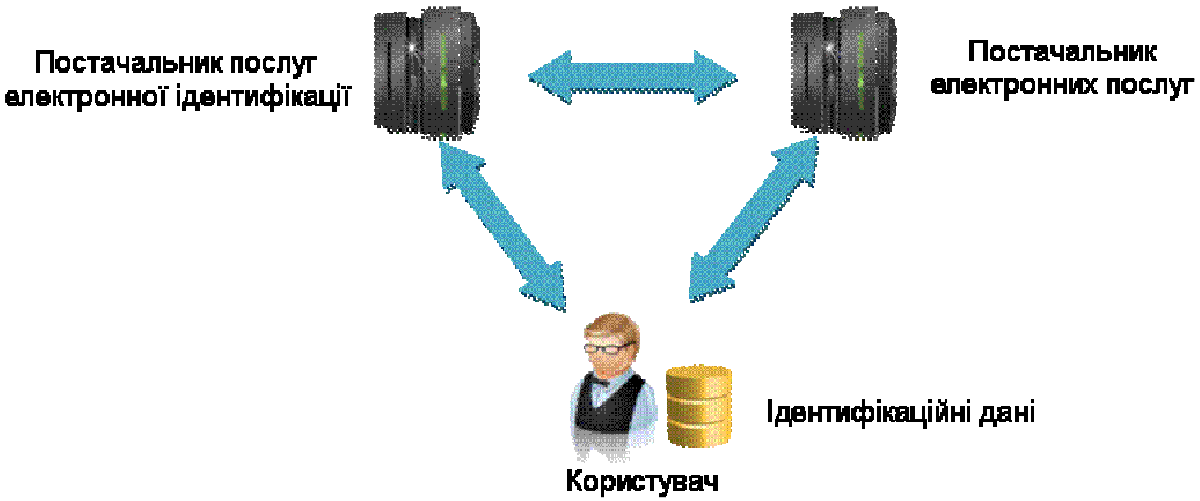


Рис 7.1. *Модель, орієнтована на користувача*

Централізована модель (Рис 7.2). Така модель є найбільш поширеною на практиці. В цій моделі, якщо користувачі бажають отримати доступ до електронних послуг, вони с початку мають надати ідентифікаційну інформацію у спеціальний орган реєстрації. Ідентифікаційні дані зберігається централізовано у реєстрі під

[49] Palfrey J., Gasser U.: Digital Identity Interoperability and eInnovation, Case Study, November 2007, Berkman Publication Series

управлінням постачальника послуг електронної ідентифікації. Під час запиту електронної послуги, користувач дає згоду на те, що постачальник послуг електронної ідентифікації надає відповідну інформації автентифікації постачальнику електронних послуг. У цій моделі користувач не має контролю за своєю ідентифікаційною інформацією. За її збереження та використання несе повну відповідальність постачальник послуг електронної ідентифікації.

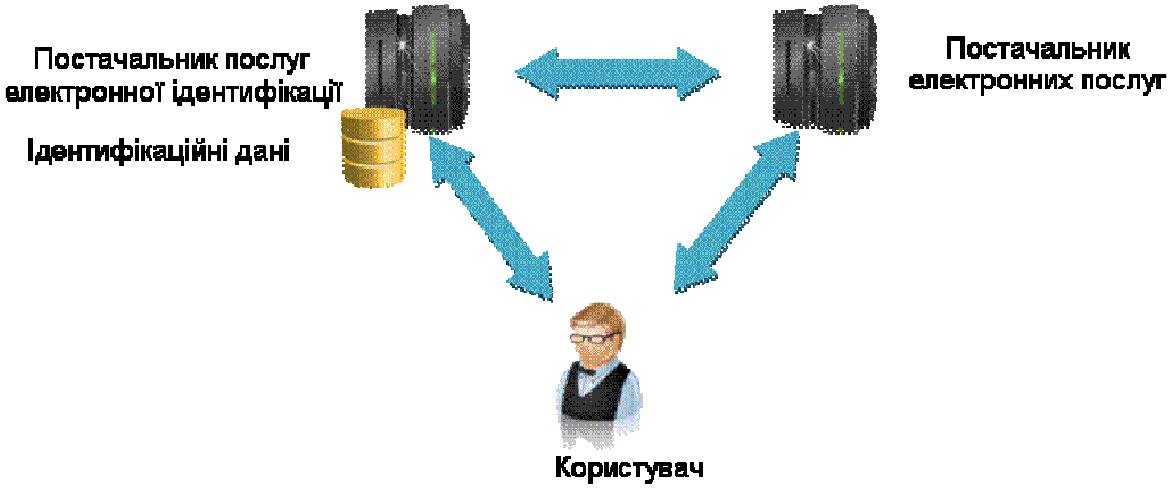


Рис 7.2. *Централізована модель*

Децентралізована модель (рис 7.3). В цій моделі ідентифікаційні дані користувача зберігаються у різних постачальників послуг електронної ідентифікації. Але постачальники послуг електронної ідентифікації можуть легко обмінюватись ідентифікаційними даними за допомогою відповідних репозиторіїв. Довіра у цій моделі досягається за рахунок встановлення відношень між різними постачальниками послуг електронної ідентифікації та на основі узгодження політик використання ідентифікаторів.

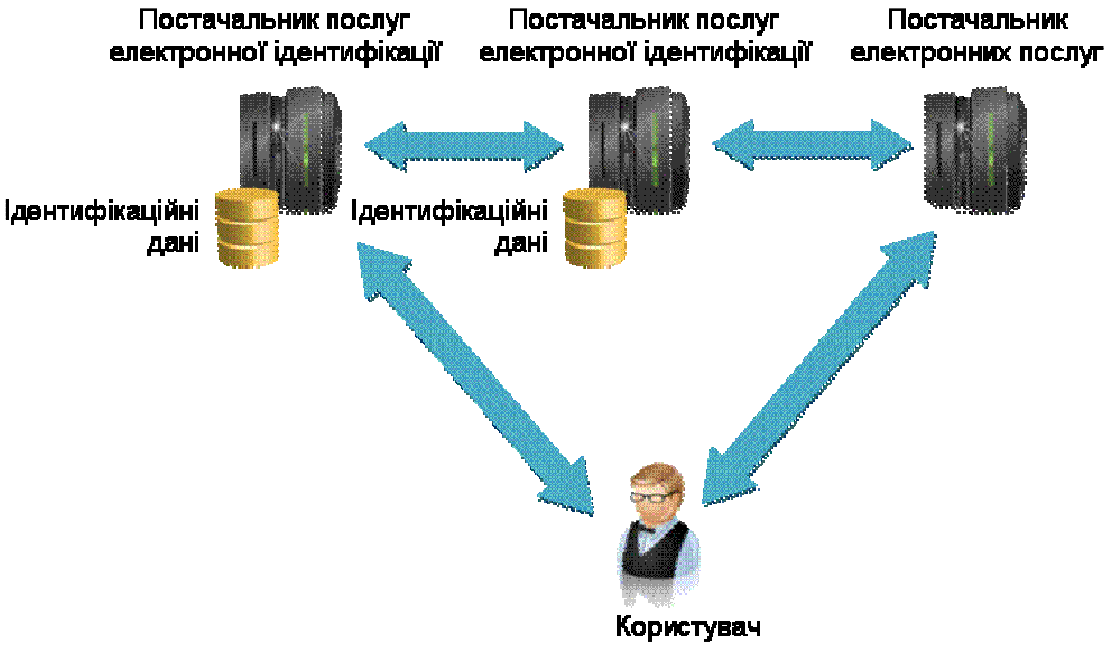


Рис 7.3. *Децентралізована модель*

Враховуючі державний та адміністративний устрій України, а також досвід впровадження систем електронної ідентифікації в інших країнах, в якості базової моделі електронної ідентифікації має бути обрана децентралізована модель. Модель реалізує таки основні принципи:

1. Інфраструктура електронної ідентифікації будується на основі унікального ідентифікатора громадянина, який має присвоюватися кожному громадянину та резиденту України.

2. Формування та підтримка унікального ідентифікатора громадянина повинна здійснюватися визначеним державним органом шляхом централізованої підтримки відповідного єдиного реєстру.

3. Порядок формування та формат унікального ідентифікатора громадянина повинен бути визначений державним нормативним актом. Унікальний ідентифікатор громадянина надається особі в порядку, визначеним законодавством з обов'язковою реєстрацією громадянина у єдиному реєстрі.

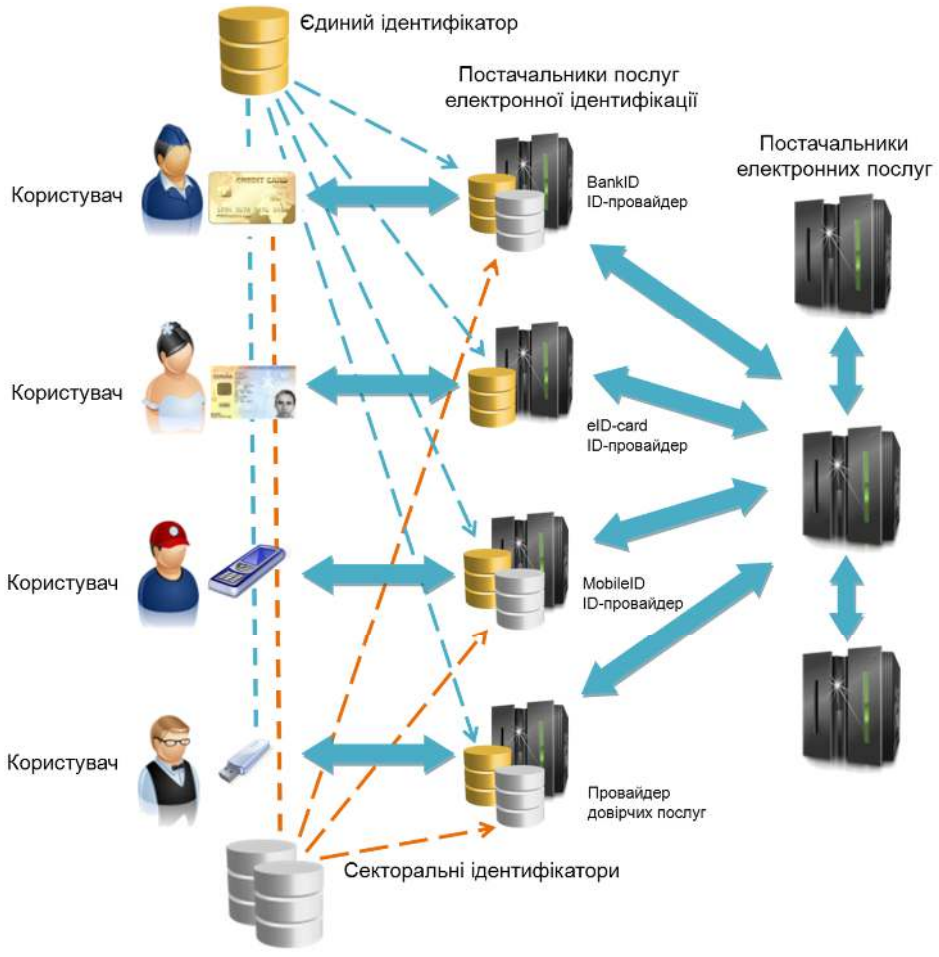
4. Унікальний ідентифікатор громадянина повинен бути однозначно зв'язаним із особою та діяти протягом всього життя особи (принцип одна особа = один ідентифікатор).

5. Інші ідентифікатори, які можуть використовуватись у конкретних сферах цивільних стосунків та соціальних відносин (секторальні ідентифікатори), повинні бути пов'язані із унікальним ідентифікатором громадянина.

6. Політика управляння унікальним ідентифікатором громадянина має бути пов'язаною з політикою управління документів, які посвідчують особу громадянина.

7. Держава має монополію на надання та управління унікальним ідентифікатором громадянина.

Спираючись на вище наведене у якості базової моделі електронної ідентифікації в Україні пропонується модель, що надана на рисунку 7.4. В загальній архітектурі електронного урядування та надання адміністративних електронних довірчих послуг місце базової моделі пояснюється на рисунку 7.5.



10.03.2015 0:39:51

Рис 7.4. *Базова модель електронної ідентифікації України*

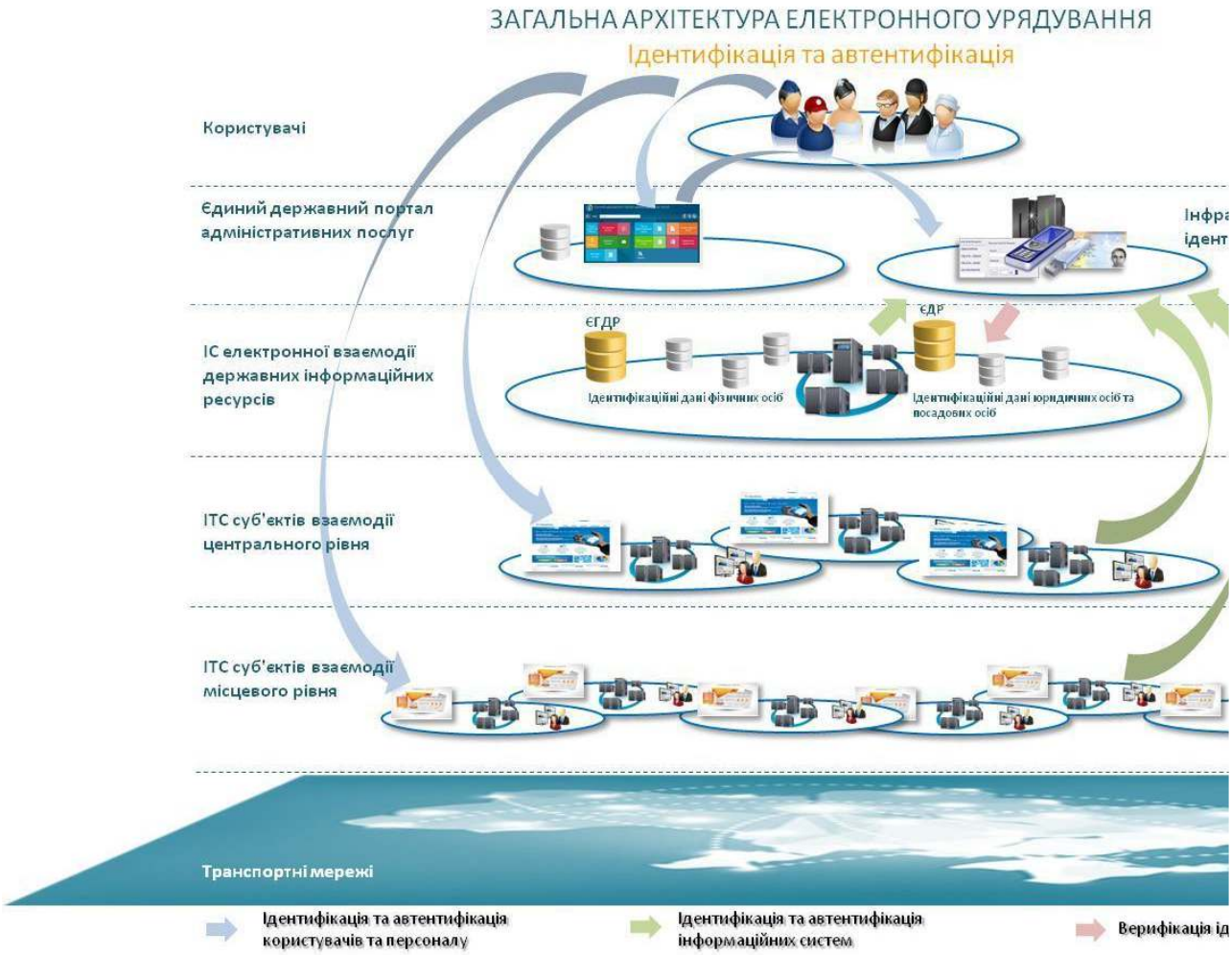


Рис.7.5.- Місце інфраструктури електронної ідентифікації в архітектурі електронного урядування України

7.2 Функціональна модель інфраструктури електронної ідентифікації України

Функціональна модель визначає та описує найбільш загальні процеси, функції, операції, що виконуються різними учасниками інфраструктури електронної ідентифікації. Під час її побудови були враховані підходи та рішення, запропоновані у функціональній моделі «Functional Model Representation of the Identity Ecosystem»[50], положення міжнародних стандартів ISO/IEC 291xx та рекомендацій ITU-T X.125x.

Функціональна модель складається с функціональних компонентів (рівнів, шарів). Кожній рівень визначає учасників та процеси, що необхідні для забезпечення надійної та довірчої *ідентифікації, автентифікації та авторизації* під час виконання будь-яких он-лайн транзакцій та надання електронних послуг. Ці рівні не визначають якусь ієрархію або пріоритет одного рівні над іншим. Їх потрібно розглядати як шари, які виконують функціональне навантаження у загальній функціональній сфері електронної діяльності.

Функціональна модель включає такі рівні (Рис. 7.6):

- функціонально-прикладний рівень ;
- експлуатаційний рівень;
- рівень функціональної сумісності (інтероперабельності);
- рівень управління.

Розглянемо більш детально кожний з цих рівнів моделі.

[50] Adam Madlin. Functional Model Representation of the Identity Ecosystem 2014

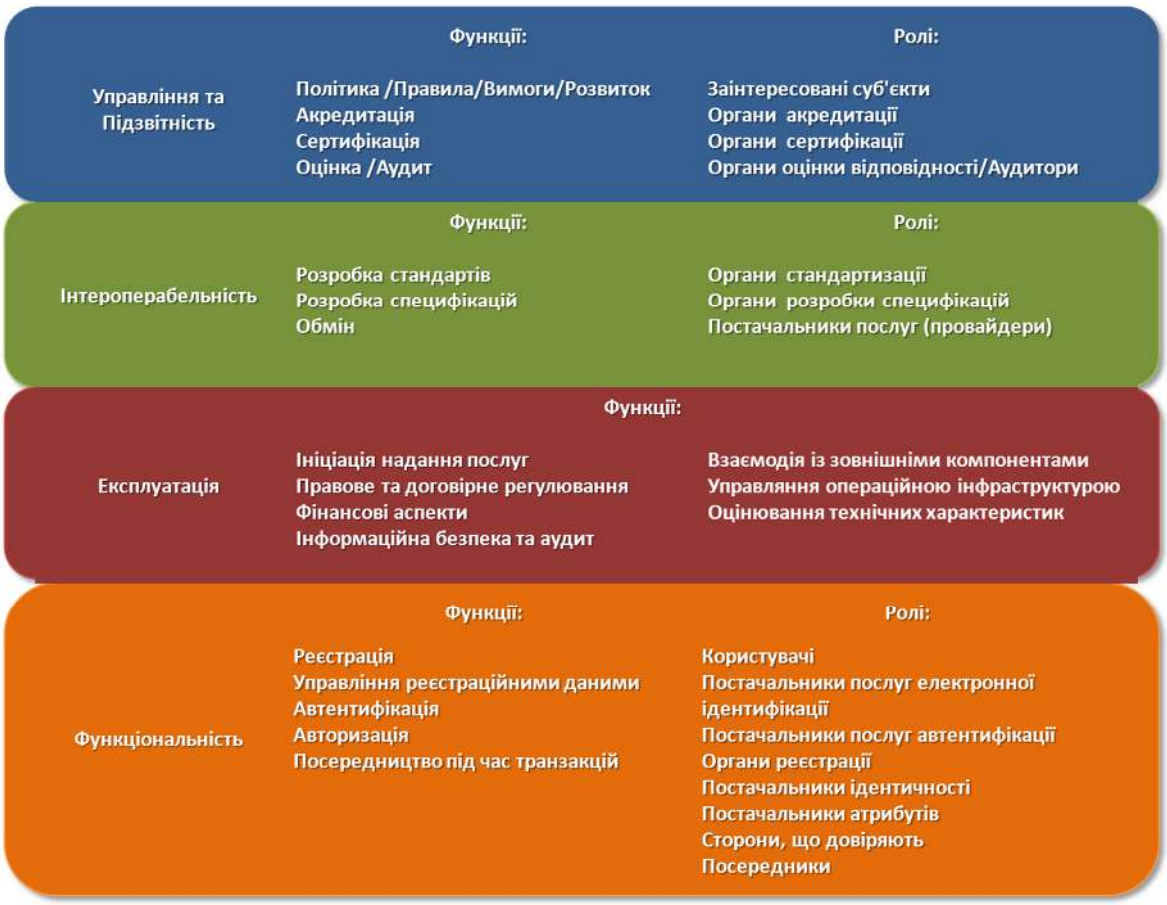


Рис 7.6 – Функціональна модель інфраструктури електронної ідентифікації.

7.2.1 Функціонально-прикладний рівень

Функціонально-прикладний рівень об'єднує окремих осіб, організації в їх взаємодії під час он-лайн транзакцій.

Як вже було зазначено, міжнародними стандартами ключовими суб'єктами в інфраструктурі електронної ідентифікації визначено користувача (User), постачальника (провайдера) послуг ідентифікації або послуг управління реєстраційними даними (Identity Service Provider або Credential Service Provider) та сторони, яка довіряє (Relying Party).

Також наголошувалось, що стандартами передбачено можливість організаційної побудови інфраструктури електронної ідентифікації

таким чином, що до складу постачальника (провайдера) послуг ідентифікації можуть входити, або окремо функціонувати такі суб'єкти як постачальники послуг автентифікації (Authentication Service Provider), органи реєстрації (Registration Authority), постачальники ідентичності (Identity Provider) та постачальники атрибутів (Attribute Provider), на котрих покладається виконання окремих ролей. Також доречно розглядати можливість включення до інфраструктури електронної ідентифікації суб'єктів – посередників (Intermediaries), які здійснюють надання послуг, направлених на підтримку приватності під час он-лайн транзакцій.

На функціонально-прикладному рівні здійснюються базові прикладні операції у відповідності до правил системи електронної ідентифікації. До базових операцій входять (рис 7.7):

- реєстрація;
- управління реєстраційними даними;
- автентифікація;
- авторизація;
- посередництво під час транзакцій.

Рис 7.7. Базові операції функціонально-прикладного рівня

Опис базових операцій (функцій) постачальників (провайдерів) послуг електронної ідентифікації наводиться із урахуванням положень стандарту ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework. Тому, відповідно до стандарту, у подальшому базові операції іменуються етапами.

На етапі реєстрації постачальник (провайдер) послуг електронної ідентифікації повинен забезпечити виконання чотирьох процесів:

- прийом та обробка заявок на реєстрацію;
- перевірка чинності ідентичності;
- верифікація ідентичності;
- ведення записів;

– реєстрація на ресурсі.

Ці процеси можуть виконуватися однією організацією - постачальником (провайдером) послуг електронної ідентифікації або включати різні відносини і можливості, забезпечувані різними організаціями, включаючи загальні або взаємодіючі компоненти, системи та послуги.

В залежності від рівня гарантій електронної ідентифікації, процеси розрізняються за суворістю. У разі реєстрації об’єкта з рівнем гарантій електронної ідентифікації «низький» (в контексті ISO 29115) ці процеси передбачають мінімум операцій (наприклад, людина може натиснути на кнопку «новий користувач» або «зареєструватись» на веб-сторінці і створити ім'я користувача та пароль). В інших випадках спектр процесів реєстрації може бути розширений. Наприклад, реєстрація відповідно до рівня гарантій електронної ідентифікації «високий» з вимагає особистої зустрічі об'єкта та органу реєстрації (Registration Authority, RA), а також розширеної перевірки чинності ідентичності об’єкта.

Прийом та обробка заявок на реєстрацію може ініціюватися різними способами. Наприклад, він може ініціюватися відповідно до запиту, зробленим об'єктами, які намагаються самостійно отримати певні реєстраційні дані (credentials) (наприклад, коли новий користувач веб-сайту має намір отримати ім'я користувача та пароль). Також можлива ситуація, коли процес реєстрації ініціюється третьою стороною, яка виступає від імені об'єкта, або самим постачальником (провайдером) послуг електронної ідентифікації (наприклад, посвідчення особи, видане державним органом, або пропуск співробітника). Наприклад, на високих рівнях гарантій електронної ідентифікації, заявки можуть прийматися тільки в тому випадку, якщо об'єкт користується порукою третьої сторони.

У будь-якому випадку процес ініціації етапу реєстрації для людей може включати заповнення форми заявки. Ця форма повинна містити достатню інформацію для гарантування однозначної ідентифікації об'єкта в даному контексті (наприклад, реєстрація повного імені, дати і місця народження). Для об’єкта, що не є фізичною особою, такий як мобільний пристрій, на етапі реєстрації може знадобитися ініціалізація шляхом установки на цьому пристрої реєстраційних даних, які дозволяють здійснювати унікальну ідентифікацію пристрою і отримувати налаштування конкретно для

цього пристрою на основі профілю конфігурації з криптографічним захистом.

Постачальники (провайдери) послуг електронної ідентифікації повинні встановлювати умови, згідно з якими проводиться реєстрація та повинні надавати послуги, пов'язані із реєстрацією. Умови надання послуг, пов'язаних із реєстрацією, можуть встановлюватися відповідно до тієї чи іншої основ довіри. У відповідних випадках, перш ніж продовжувати процеси реєстрації, об'єктом або особи, що виступає від його імені, також повинні прийматися умови звільнення від відповідальності або інші юридичні положення.

Перевірка чинності (верифікація) ідентичності - це процес збору та перевірки інформації, достатньої для ідентифікації об'єкта з певним або передбачуваним рівнем гарантії. Верифікація інформації про ідентичність є частиною процесу перевірки інформації про ідентичність і включає засвідчення підтвердження ідентичності інформації за допомогою видавців, джерел даних, внутрішніх або зовнішніх ресурсів таких джерел щодо автентичності, дієвості, правильності та відношення ідентифікаційних даних до об'єкта. Залежно від контексту для відповідності вимогам перевірки чинності ідентичності може використовуватися різна інформація, що підтверджує ідентичність (наприклад, документи, що посвідчують особу, водійські посвідчення, біометрична інформація, свідоцтво про народження), видана авторитетними джерелами або затверджена такими джерелами. Реальна інформація, що підтверджує ідентичність, та використовується для перевірки її чинності, повинна визначатись залежно від конкретного рівня гарантій електронної ідентифікації.

Перевірка справжності ідентичності може включати фізичну перевірку поданих документів про ідентичність для виявлення можливого шахрайства, злому або фальсифікації. Перевірка справжності ідентичності може також включати перевірку з метою набуття впевненості у тому, що ідентичність використовується в інших контекстах (тобто, *верифікована* іншими органами реєстрації). Чим вище необхідний рівень гарантій електронної ідентифікації, тим суворіше повинні бути вимоги до перевірки чинності ідентичності. Крім того, процес перевірки чинності ідентичності повинен бути більш суворим для об'єктів, які стверджують або заявляють про свою ідентичність дистанційно (наприклад, по каналу Інтернету),

порівняно з поданням ідентичності на місці (наприклад, особистий контакт з органом реєстрації).

Строгість вимог до перевірки чинності ідентичності ґрунтується на завданнях, які належить вирішити для кожного рівня гарантій електронної ідентифікації. На рівні гарантій електронної ідентифікації єдиним завданням є гарантія того, що дана ідентичність є унікальною в даному контексті.

Ідентичність не повинна бути пов'язана з двома різними об'єктами. На рівні гарантій електронної ідентифікації «середній» (в контексті ISO 29115) або «низький» (в контексті Регламенту eIDAS) виконуються два завдання. По-перше, ідентичність повинна бути унікальною у визначеному контексті. По-друге, об'єкт, якого стосується ця ідентичність, повинен існувати об'єктивно, що означає те, що ідентичність не повинна бути фіктивною або навмисно підробленою в шахрайських цілях. Наприклад, перевірка чинності ідентичності людини на рівні гарантій електронної ідентифікації «середній» (в контексті ISO 29115) або «низький» (в контексті Регламенту eIDAS) може включати перевірку записів про народження і смерть для гарантії певного походження (хоча це не доводить того, що об'єкт, який володіє документом, що посвідчує особу, є тією самою людиною, якій цей документ належить).

Вищі рівні гарантій електронної ідентифікації повинні включати завдання та процедури, що належать до нижчих рівнів гарантій, а також завдання більш суворого характеру.

Так, рівень гарантій «високий» (в контексті ISO 29115) або «суттєвий» (в контексті Регламенту eIDAS) повинен передбачати виконання завдання перевірки ідентифікаційних даних за допомогою одного або декількох авторитетних джерел, таких як зовнішня база даних. Верифікація інформації, що підтверджує чинність ідентичності підтверджує, що дана ідентичність використовується і відноситься до даного об'єкта. Однак гарантія того, що інформацією, яка підтверджує чинність ідентичності володіє реальний чи законний власник ідентичності, відсутня.

Для фізичних осіб на рівні гарантій електронної ідентифікації «дуже високий» (в контексті ISO 29115) або «високий» (в контексті Регламенту eIDAS) до завдань, відповідних до попереднього рівня гарантій, додається ще одне завдання - вимога засвідчити об'єкт особисто органом реєстрації для захисту від імітації законного користувача.

Зведені дані щодо вимог до завдань та процедур етапів перевірки чинності ідентичності та верифікації для різних рівнів гарантій у контекстах ISO 29115 та Регламенту eIDAS наведено у Таблиці 7.1.

Таблиця 7.1 Рівні гарантій електронної ідентифікації та вимоги до верифікації ідентичності

Рівні гарантій eIDAS	Рівні гарантій ISO 29115	Довіра до ідентичності	Характеристики заявленої ідентичності	Засоби перевірки чинності ідентичності	Спосіб верифікації
-	LoA1 – Low низький	Низька довіра до заявленої ідентичності або її відсутність	Ідентичність унікальна в межах контексту	Самостійно заявлена ідентичність	Локальна або віддалена обробка
Low - низький	LoA2 – Medium середній	Невисока довіра до заявленої ідентичності	Ідентичність унікальна в межах контексту та об'єкт, до якого належить ідентичність, об'єктивно існує	Перевірка чинності ідентичності за допомогою ідентифікаційних даних, отриманих з авторитетного джерела	Локальна або віддалена обробка
Substantial - суттєвий	LoA3 – High високий	Висока довіра до заявленої ідентичності	Ідентичність унікальна в межах контексту, об'єкт, до якого належить ідентичність, об'єктивно існує, ідентичність можливо перевірити, ідентичність використовується також в інших контекстах	Перевірка чинності ідентичності за допомогою ідентифікаційних даних, отриманих з авторитетного джерела + верифікація	Локальна або віддалена обробка
High – високий	LoA4 – Very high дуже високий	Дуже висока довіра до заявленої ідентичності	Ідентичність унікальна в межах контексту, об'єкт, до якого належить ідентичність, об'єктивно існує, ідентичність можливо перевірити, ідентичність використовується також в інших контекстах	Перевірка чинності ідентичності за допомогою ідентифікаційних даних, отриманих з авторитетного джерела + верифікація + персональне встановлення об'єкта	Тільки локальна

Необхідні засоби перевірки чинності ідентичності для захисту проти загроз для реєстрації користувача для кожного рівня гарантій електронної ідентифікації повинні визначатися відповідно до формалізованих процедур та ґрунтуватись на базі положень стандартів. Прийнятним стандартом варто вважати ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework, гармонізація якого повинна стати одним із пріоритетних завдань створення інфраструктури електронної ідентифікації України.

Будь-яка реалізація структури гарантій електронної ідентифікації об’єктів повинна ґрунтуватись на підмножині інформації про ідентичність об'єкта та джерелах такої інформації, які доступні для органів реєстрації або для самих об’єктів.

Надійність та точність інформації про ідентичність та джерел визначають реальну гарантію, що забезпечується на етапі реєстрації. Відповідно, суб’єкти, що реалізують структуру гарантій електронної ідентифікації, повинні ретельно оцінювати гарантію, яка забезпечується різними інфраструктурами управління ідентичністю, із використанням різних джерел ідентифікаційних даних, при ухваленні рішення про те, на чиї дані, що підтверджують ідентичність та/або на які джерела слід покладатися при перевірці чинності ідентичності та верифікації ідентифікаційних даних.

Будь-яка реалізація структури гарантій електронної ідентифікації повинна передбачати публікацію документа (наприклад, політики перевірки чинності ідентичності, згідно з відповідним описом в ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework), в якому наводиться переліки та огляд даних, які підтверджують чинність ідентичності, джерел та/або видавців ідентифікаційних даних, на яких слід покладатися на етапі реєстрації.

Процес ведення записів є передостаннім на етапі реєстрації. Саме під час цього процесу здійснюється створення реєстраційного запису щодо об’єкта електронної ідентифікації. Цей запис повинен включати інформацію та враховувати документацію, які були зібрані (і можуть бути збережені), інформацію про процес верифікації ідентифікаційних даних, результати цих кроків та інші відповідні дані. Потім виноситься і реєструється рішення про прийняття, відхилення або передачі запису для подальшої перевірки або інших подальших дій.

Реєстрація на ресурсі - це процес, в ході якого об'єкт здійснює запит використання послуги або ресурсу інформаційної системи. Хоча процес реєстрації на ресурсі зазвичай вважається частиною етапу реєстрації і виконується в кінці цього етапу, він також може виконуватися і пізніше. На відміну від інших процесів у межах етапу реєстрації, які, швидше за все, необхідні лише одного разу, реєстрація на ресурсі може вимагатися, коли об'єкт вперше здійснює запит використання кожної окремої послуги або кожного окремого ресурсу.

Етап управління реєстраційними даними (credential management) включає всі процеси, пов'язані з управління життєвим циклом реєстраційних даних або засобів для їх створення, що дають користувачеві можливість брати участь у будь-якої діяльності або в якому-небудь контексті. Етап управління реєстраційними даними може включати всі наступні процеси або їх частину:

- створення реєстраційних даних;
- випуск реєстраційних даних або засобів для їх створення;
- активацію реєстраційних даних або засобів для їх створення;
- зберігання реєстраційних даних;
- анулювання та/або знищення реєстраційних даних або засобів для їх створення;
- оновлення та/або заміну реєстраційних даних або засобів для їх створення;
- ведення записів.

Деякі з цих процесів залежать від того, чи розміщені реєстраційні дані в апаратному засобі електронної ідентифікації.

Процес *створення реєстраційних даних* охоплює всі необхідні процеси для створення реєстраційних даних вперше або засобів для їх створення. Ці процеси можуть включати попередню обробку, ініціалізацію і прив'язку.

Деякі реєстраційні дані або засоби для їх створення вимагають попередньої обробки перед випуском, наприклад індивідуалізації особистих даних (персоналізації), якщо реєстраційні дані адаптуються до ідентичності об'єкта. Індивідуалізація особистих даних може приймати різні форми залежно від реєстраційних даних. Наприклад, персоналізація смарт-карти, яка містить реєстраційні дані, може включати друк (на зовнішній стороні картки) або запис

(на чіпі карти) імені або біометричних даних об'єкта, для якого була випущена карта. Існують також реєстраційні дані, які не потребують персоналізації, наприклад паролі.

Ініціалізація реєстраційних даних охоплює всі кроки, які гарантують, що який-небудь засіб для створення реєстраційних даних згодом зможе забезпечувати весь запланований набір функцій. Наприклад, чіп на смарт-карті може знадобитися для обчислення пар криптографічних ключів, необхідних для підтримки подальшого створення цифрових підписів. Аналогічним чином, смарт-карта може бути випущена в "заблокованому" стані, що потребують PIN-коду в процесі активації.

Прив'язка як іще один можливий підетап створення реєстраційних даних - це процес встановлення зв'язку між реєстраційними даними чи засобами для їх створення і об'єктом, для якого вони були випущені. Спосіб прив'язки і впевненість у створеному зв'язку варіюються залежно від рівня гарантій ідентифікації. Наприклад, в он-лайновому режимі у разі прив'язки ідентифікатора постійного псевдоніма об'єкта до запису клієнта об'єкта, в ході процесу прив'язки безпечним каналом може бути переданий первинний "код активації" у вигляді одноразового зашифрованого куки-файлу. Інший варіант - код активації може бути запитаний в кінці процесу, після виконання кроку прив'язки об'єкта до постійного ідентифікатора, із подальшою прив'язкою постійного ідентифікатора до запису клієнта.

Випуск реєстраційних даних - це процес забезпечення об'єкта певними реєстраційними даними чи засобами для їх створення або встановлення іншого зв'язку між ними. Складність цього процесу різниться в залежності від необхідного рівня гарантій електронної ідентифікації. Для більш високих рівнів гарантій може бути потрібна захищена доставка апаратного засобу електронної ідентифікації (наприклад, смарт-карти), що містить реєстраційні дані, і може знадобитися особиста доставка. Для більш низьких рівнів гарантій процесом випуску може бути проста відправка пароля або PIN-коду на фізичну або електронну поштову адресу об'єкта.

Наступним процесом етапу управління реєстраційними даними повинна бути їх *активація*, під час якої реєстраційні дані або засоби для їх створення підготовляються до використання. Процес активації може включати різноманітні заходи, залежно від реєстраційних даних. Наприклад, реєстраційні дані або засоби для їх створення можуть бути "заблоковані" після їх ініціалізації до моменту їх випуску

для об'єкта, для запобігання проміжного неналежного використання цих даних. У деяких випадках активація може включати "розблокування" реєстраційних даних (наприклад, при використанні пароля). Реєстраційні дані або засоби для їх створення можуть також активуватися після призупинення, коли їх дію було тимчасово зупинено (заблоковано).

Зберігання реєстраційних даних - це процес, при якому реєстраційні дані або засоби для їх створення безпечно зберігаються таким чином, який захищає їх від несанкціонованого розкриття, використання, зміни або знищення. В зберіганні реєстраційних даних беруть участь об'єкт, пов'язаний з цими реєстраційними даними, і дії, необхідні для захисту від несанкціонованого використання цих даних.

Зберігання реєстраційних даних не повинно обов'язково включати захист інформації, яка використовується для перевірки того, що реєстраційні дані мають законну силу, якщо ця інформація не є частиною реєстраційних даних. Методи захисту інформації, такий як, наприклад, таблиці гешованих паролів, необхідних для автентифікації, потрібні на більш високих рівнях гарантій електронної ідентифікації.

Анулювання реєстраційних даних - це процес, при якому дійсність реєстраційних даних остаточно припиняється. Призупинення (блокування) - це пов'язаний процес, при якому дійсність реєстраційних даних призупиняється тимчасово. Анулювання повинно бути проведено у випадках, коли:

а) відомо, що реєстраційні дані або засоби для їх створення загублені, вкрадені чи іншим способом розкриті;

б) закінчився термін дії реєстраційних даних;

в) більше не існує підстави для подальшого існування реєстраційних даних (наприклад, при звільненні працівника);

г) реєстраційні дані використовувалися для несанкціонованих цілей;

д) були випущені інші реєстраційні дані для заміни тих, які підлягають анулюванню.

Постачальники (провайдери) послуг електронної ідентифікації повинні забезпечити, щоб час між повідомленням про подію, що передбачає анулювання, і завершенням процесу анулювання визначався політикою провайдера. При більш високих рівнях

гарантій електронної ідентифікації період, дозволений для анулювання, повинен бути максимально скорочений. Деякі види реєстраційних даних, такі як дані, що містяться на смарт-картах, після анулювання можуть знищуватися фізично. Однак інформація, пов'язана з реєстраційними даними, може бути знищена не завжди.

Поновлення - це процес, в ході якого термін дії існуючих реєстраційних даних подовжується. Заміна, у свою чергу, це процес, в ході якого для об'єкта випускаються нові реєстраційні дані або засоби для їх створення, з тим щоб замінити реєстраційні дані, які раніше використовувалися та/або були анульовані. Прикладом заміни реєстраційних даних може бути ситуація, коли постачальник (провайдер) послуг електронної ідентифікації відправляє тимчасовий пароль на адресу електронної пошти об'єкта, що дозволяє об'єкту створити новий пароль після отримання тимчасового. Строгість процесу оновлення і заміни реєстраційних даних може бути різною залежно від рівня гарантій електронної ідентифікації.

Ведення відповідних записів повинно здійснюватися постачальником (провайдером) послуг електронної ідентифікації протягом всього життєвого циклу реєстраційних даних. Записи повинні вестися задля реєстрації такої інформації:

а) факт створення реєстраційних даних;

б) ідентифікатор реєстраційних даних (у відповідних випадках);

в) об'єкт, для якого були випущені реєстраційні дані (у відповідних випадках);

г) статус реєстраційних даних (у відповідних випадках).

Записи повинні вестись щодо кожного процесу, що входить в етап управління реєстраційними даними.

Якщо реєстраційні дані були випущені для об'єктів-людей, то ведення записів, швидше за все, буде включати обробку персональних даних, що накладає на постачальника (провайдера) послуг електронної ідентифікації відповідні зобов’язання щодо захисту таких даних. При цьому, провайдером повинні виконуватись такі базові принципи конфіденційності щодо персональних даних: згода і вибір, визначення мети, обмеження збору, обмеження на використання, зберігання та розголошення, мінімізація даних, точність і якість, відкритість, прозорість, особиста участь і доступ, підзвітність, засоби контролю безпеки, а також відповідність. Поряд з

оцінкою ризиків для аналізу загроз, постачальники (провайдери) послуг електронної ідентифікації повинні виконувати оцінку впливу обраного способу автентифікації на конфіденційність, для того щоб оцінити, які компоненти їх систем потребують особливої уваги в аспекті заходів щодо захисту конфіденційності особистих даних споживачів.

Для отримання більш докладних керівних вказівок щодо вимог, принципів і проектів систем в аспекті захисту персональних даних, постачальникам (провайдерам) послуг електронної ідентифікації слід керуватись положеннями ISO/IEC 29100:2012, Information technology – Security techniques – Privacy framework та ISO/IEC 29101, Information technology – Security techniques – Privacy architecture framework, гармонізація яких також повинна стати одним із пріоритетних завдань створення інфраструктури електронної ідентифікації України.

Етапи *автентифікації* та *авторизації* об'єкта – наступні ключові етапи опису функціональної моделі інфраструктури електронної ідентифікації. На цих етапах об'єкт використовує свої реєстраційні дані, для засвідчення своєї ідентичності.

Процес автентифікації стосується виключно встановлення (або невстановлення) рівня впевненості в твердженні або заяві об’єкта (користувача) про ідентичність і не має будь-якого відношення до дій, сторони, яка довіряє, котрі вона може вжити на підставі цього твердження чи заяви.

Процес автентифікації повинен включати використання протоколу, що доводить володіння реєстраційними даними для встановлення впевненості в ідентичності. Вимоги до протоколу автентифікації варіюються залежно від обраного рівня гарантій електронної ідентифікації. Наприклад, для низького рівня гарантій автентифікація може включати використання пароля. На більш високому рівні гарантій автентифікація може включати використання криптографічного протоколу типу запит-відповідь. На ще більш високому рівні гарантій електронної ідентифікації можливо потрібно бути використання багатофакторної автентифікації для забезпечення високої стійкості. Засоби контролю загроз етапу автентифікації, у тому числі їх залежність від обраного рівня гарантій та необхідна кількість факторів автентифікації описані в стандарті ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework, який, як було сказано

доцільно розглядати як пріоритетний в процесі гармонізації нормативної бази України.

Процес автентифікації повинен уявляти собою послідовність прийому запитів на автентифікацію, верифікації реєстраційних даних та прийняття рішення щодо результатів попередніх підпроцесів.

Процеси *авторизації* об'єкта (користувача) уявляє собою реалізації притаманних, як правило стороні, яка довіряє (Relaying Party), механізмів, які забезпечують надання або відмову в наданні доступу до ресурсів інформаційної системи на запити об'єкта. Такі механізми повинні містити запити на авторизацію, верифікації атрибутів користувача та прийняття відповідного рішення щодо результатів обробки запитів, верифікації та надання доступу до ресурсів інформаційної системи.

Моніторинг подій і *ведення записів* про ці події на етапах автентифікації та авторизації може використовуватись в різних цілях, у тому числі для забезпечення обслуговування користувачів та інформаційної системи провайдерів електронної ідентифікації та електронних сервісів, оцінки відповідності обраних механізмів рівню гарантій електронної ідентифікації, обліку та/або реалізації правових норм.

У разі участі в електронних транзакціях об'єктів-людей інформація, що міститься в цих записах, може включати конфіденційну інформацію, що відноситься до персональних даних. Управління цими записами повинно здійснюватися таким способом, який враховує необхідність захисту і мінімізації використання персональних даних, мова про що вже йшла вище.

З огляду на це, в інфраструктурі електронної ідентифікації передбачено наявність суб'єктів-посередників, які можуть забезпечувати анонімізацію обміну, використання псевдонімів в якості ідентифікаційних даних, що, між тим, не повинно шкодити однозначній ідентифікації користувача у випадках, передбачених законодавством.

7.2.2 Експлуатаційний рівень

Даний рівень об'єднує учасників та функції, що пов'язані з експлуатацією та адмініструванням інфраструктури електронної

ідентифікації. Всі учасники інфраструктури електронної ідентифікації, які виконують прикладні функції, також виконують і функції з адміністрування та експлуатації схем та засобів електронної ідентифікації.

Досягнення бажаного рівня гарантій електронної ідентифікації залежить не тільки від технічних чинників, але й від нормативних положень, договірних угод зваженого розуміння того, як здійснюється управління наданням послуг та його організація. У відсутність належного управління та організації роботи будь-яке технічно надійне рішення може втратити свій потенціал забезпечення безпеки при забезпеченні певного рівня гарантій.

Базовими функціями рівня експлуатації принаймні повинно бути визначено:

- ініціація надання послуг;
- правове та договірне регулювання;
- фінансові аспекти;
- інформаційна безпека та аудит;
- взаємодія із зовнішніми компонентами;
- управляння операційною інфраструктурою;
- оцінювання технічних характеристик;

Ініціація надання послуг охоплює як юридичний статус постачальника послуг, так і функціональний статус забезпечення обслуговування. Наприклад, якщо відомо, що постачальник (провайдер) послуг електронної ідентифікації є зареєстрованою юридичною особою, то це дає впевненість у тому, що провайдер користується довірою серед інших організацій в межах своєї юрисдикції. Важливість цього зростає, коли компоненти обслуговування управляються різними юридичними особами (наприклад, якщо реєстрація є окремою функцією).

Хоча основні вимоги є однаковими для всіх рівнів гарантій електронної ідентифікації, на більш високих рівнях слід забезпечити більшу залежність від повноти та надійності обслуговування. Наприклад, на рівні гарантій «суттєвий» та «високий» постачальник (провайдер) послуг електронної ідентифікації, повинен підтримувати більш високу гарантію щодо забезпечення обслуговування, у тому числі з урахуванням знання корпоративних зв'язків і розуміння рівня незалежності, дозволеного при операціях.

В межах *правового та договірного регулювання*, всі учасники інфраструктури електронної ідентифікації повинні розуміти вимоги закону, покладені на них у зв'язку з організацією надання послуг, і забезпечувати відповідність цим вимогам. Це включає, зокрема, визначення типу інформації, яка може запитуватися, порядок виконання перевірки чинності ідентичності та визначення інформації, яка може бути збережена. Повинні бути враховані всі юрисдикції, в рамках яких діють учасники. Для рівнів гарантій електронної ідентифікації «суттєвий» та «високий» мають бути визначені також конкретні вимоги політики і договірні умови.

У контексті *фінансових аспектів*, якщо об'єкт і постачальник (провайдер) послуг електронної ідентифікації припускають довгострокову доступність послуг, то останні повинні продемонструвати фінансову стабільність, достатню для гарантування безперервного обслуговування та угоди про ступінь потенційної відповідальності сторін. Малоймовірно, що такі положення будуть розглядатися для рівня гарантій електронної ідентифікації «низький», але слід враховувати необхідність в них для послуг, що забезпечують більш критичні транзакції, та передбачають рівні гарантій електронної ідентифікації «суттєвий» та «високий».

Стосовно управління *інформаційною безпекою та аудиту* слід наголосити, що починаючи з рівня гарантій електронної ідентифікації «низький» (в контексті Регламенту eIDAS) постачальники (провайдери) послуг електронної ідентифікації повинні забезпечувати документально оформлені практику управління інформаційною безпекою, стратегії, підходи до управління ризиками та інші визнані засоби контролю, з метою забезпечення застосування ефективних методів захисту.

Для рівня гарантій «суттєвий» (в контексті Регламенту eIDAS) постачальники (провайдери) послуг електронної ідентифікації повинні використовувати офіційну систему управління інформаційною безпекою (наприклад, ISO/IEC 27000 або НД ТЗІ).

Залежно від угоди про відповідність правовим нормам, договірними умовами та технічними характеристиками провайдери повинні гарантувати виконання зобов'язань та забезпечення відшкодування в разі їх порушень. Вже починаючи з рівня гарантій електронної ідентифікації «низький» (в контексті Регламенту eIDAS) гарантії безпеки повинні підтримуватися перевірками захищеності інформаційних систем, як внутрішніми, так і зовнішніми, веденням журналів реєстрації подій тощо. Аудит може використовуватися для

перевірки того, що методи сторін відповідають угодам. У разі розбіжностей можуть використовуватися послуги вирішення спорів.

Відносно функції управління *взаємодією із зовнішніми компонентами обслуговування*, варто зазначити, що якщо постачальник (провайдер) послуг електронної ідентифікації залучає для забезпечення частини своїх послуг треті сторони, то загальна гарантія забезпечення якості обслуговування буде залежати від управління діями цих сторін і нагляду за ними. Зміст і масштаб домовленостей мають бути пропорційні необхідному рівню гарантій електронної ідентифікації та впровадженій системі управління інформаційною безпекою. При цьому, чим вище рівень гарантій, тим більше заходи взаємодії з третіми сторонами будуть впливати на загальний рівень забезпечення гарантії.

Описуючи функцію *управління операційною інфраструктурою*, треба наголосити на тому, що для забезпечення великомасштабних мереж довіри може використовуватися та чи інша структура довіри. У структурі довіри учасники процесів надання послуг електронної ідентифікації (провайдери послуг електронної ідентифікації, органи реєстрації, сторони, які довіряють) підтримують інформаційні потоки між собою. Залежно від угод можливе звернення до додаткових учасників, з тим щоб забезпечити виконання всіма сторонами зобов'язань і перспективи відшкодування у разі порушення.

В контексті функцій *оцінювання експлуатаційних характеристик*, органи технічного регулювання сфери електронної ідентифікації мають встановити технічні та договірні вимоги щодо структур довіри. Технічні вимоги можуть включати, наприклад, рівні версій продукту, конфігурацію системи, налаштування і протоколи, а договірні вимоги можуть містити політики використання інформації. При встановленні таких вимог органи технічного регулювання повинні включати в них критерії, за якими можна оцінити потенційні об'єкти структури довіри. Замість розробки таких критеріїв органи технічного регулювання можуть використовувати стандартні критерії, вже розроблені експертами, наприклад ISO/IEC 29115. Чим ширше органи технічного регулювання будуть використовувати стандартні критерії в різних структурах довіри, тим простіше для постачальників (провайдерів) послуг електронної ідентифікації буде узгоджено розуміти і застосовувати ці критерії. Крім того, поіменовані набори критеріїв можуть служити в якості

умовного позначення різних ступенів і типів строгості вимог або можливостей для різних рівнів гарантій електронної ідентифікації.

7.2.3 Рівень інтероперабельності (сумісності)

На рівні функціональної сумісності (інтероперабельності) основними функціями, притаманними цьому рівню інфраструктури електронної ідентифікації є:

- розробка, гармонізація та введення в дію державних стандартів сфери електронної ідентифікації щодо технологій та процедур;
- розробка та впровадження технічних специфікацій, форматів та протоколів, що визначають обмін ідентифікаційними даними між суб'єктами інфраструктури, процеси верифікації, автентифікації та авторизації;
- забезпечення сприяння сумісному обміну ідентифікаційними даними, інформаційними блоками, відповідних до затверджених специфікацій, форматів та протоколів верифікації, автентифікації та авторизації.

Розробка та гармонізація стандартів та технічних специфікацій повинні стати складовою частиною загальнодержавних процесів сфери технічного регулювання, охоплювати всі життєві цикли, що протікають в інфраструктурі електронної ідентифікації, бути нерозривними із сферами інформатизації, розбудови систем електронного урядування, надання електронних послуг та захисту інформації.

Розроблювані стандарти та специфікації повинні ґрунтуватись на діючих міжнародних стандартах та кодексах усталеної практики. Необхідною умовою досягнення мети визнання запроваджених в інфраструктурі схем електронної ідентифікації на єдиному цифровому ринку має стати приведення розроблюваних нормативних документів у відповідність до діючих нормативних актів Європейського Союзу, які набуватимуть чинності згідно з положеннями Регламенту eIDAS. Тому процеси стандартизації інфраструктури електронної ідентифікації України повинні бути синхронізовані з процесами, які протікають на міжнародному рівні в рамках діяльності міжнародних та європейських організацій із стандартизації.

Забезпечення ефективності процесів досягнення функціональної сумісності інфраструктури електронної ідентифікації повинно стати основним завданням органу технічного регулювання України у сфері електронної ідентифікації, а визначення такого органу на державному рівні – пріоритетною задачею реалізації Стратегії.

Сприяння сумісному обміну ідентифікаційними даними, інформаційними блоками, відповідних до затверджених специфікацій, форматів та протоколів верифікації, автентифікації та авторизації має стати спільним завданням розробників засобів та схем електронної ідентифікації, системних інтеграторів та провайдерів послуг електронної ідентифікації.

Виконання такого завдання має ґрунтуватись на створенні організаційно-технологічної інфраструктури забезпечення інтероперабельності, побудованої на принципах прозорості та добровільності її учасників, у тому числі, крім перелічених вище суб'єктів, до організаційної структури повинні входити також орган технічного регулювання та державні органи, залучені до процесів електронної взаємодії, адміністрування державних інформаційних систем, в яких здійснюються первинне завантаження та обробка ідентифікаційних даних.

Технологічна складова інфраструктури забезпечення інтероперабельності повинна спиратись на створенні технічної платформи, побудованої із залученням ресурсів приватного та державного сектору, поєднувати потенціал передових учасників ІТ – спільноти, науковців, розробників апаратних та програмних засобів електронної ідентифікації, захисту інформації, провайдерів електронних послуг.

Технічна платформа інфраструктури забезпечення інтероперабельності має стати майданчиком для впровадження пілотних проектів схем електронної ідентифікації з використанням різних засобів, протоколів та форматів, які стануть основою для створення загальнонаціональної інфраструктури електронної ідентифікації.

Одним із векторів діяльності інфраструктури забезпечення інтероперабельності повинна стати участь у широкомасштабних

європейських проектах, прикладам яких на сьогодні є проект та ISA (Interoperability Solutions for European Public Administrations)[51].

Проект ISA покликаний сприяти взаємодії між державними органами, допомагаючи встановити загальні підходи, які зроблять співпрацю між ними, громадянами та бізнесом набагато простіше. Спільне використання та повторне використання таких інструментів, як загальні платформи та загальні компоненти, а також розподіл послуг через спільні інфраструктури, буде грати вагому роль в зниження витрат і скорочення часу виходу України на загальний цифровий ринок.

7.2.4 Рівень управління

Рівень управління інфраструктури електронної ідентифікації повинен уявляти собою сукупність функцій, покладених на органи державного управління, що здійснюють нормативно-правове та технічне регулювання сфери електронної ідентифікації, а також органи оцінки відповідності.

На цьому рівні органи державного управління, визначені законодавством, повинні здійснювати створення нормативних засад, правил, керівних принципів та вимог для забезпечення функціонування інфраструктури електронної ідентифікації, а також здійснювати відповідний державний нагляд за діяльністю провайдерів послуг електронної ідентифікації, направлений перш за все на дотримання положень законодавства щодо захисту інформації та персональних даних.

Основними функціями рівня управління мають стати:

- розробка нормативної моделі інфраструктури електронної ідентифікації, політик, вимог та правил щодо електронної ідентифікації в тому або іншому секторі (контексті);
- розробка вимог до процедур та правил акредитації (підтвердження компетенції) провайдерів послуг електронної ідентифікації, впровадження таких процедур та правил на засадах добровільності щодо їх участі в процесах інтеграції із системами надання електронних адміністративних послуг, прозорих процесів входження провайдерів послуг електронної ідентифікації на ринок;

[51] http://ec.europa.eu/isa/index_en.htm

– впровадження процедур сертифікації засобів електронної ідентифікації для високих рівнів гарантій електронної ідентифікації для визначення відповідності нормативно визначеним вимогам щодо розробки та введення в обіг таких засобів та правилам надання послуг електронної ідентифікації згідно із рівнем гарантій;

– здійснення періодичної оцінки відповідності та аудиту провайдерів послуг електронної ідентифікації, які надаються для забезпечення функціонування систем електронного урядування, та у перспективі в рамках схем електронної ідентифікації, що пройшли нотифікацію згідно з вимогами Регламенту eIDAS.

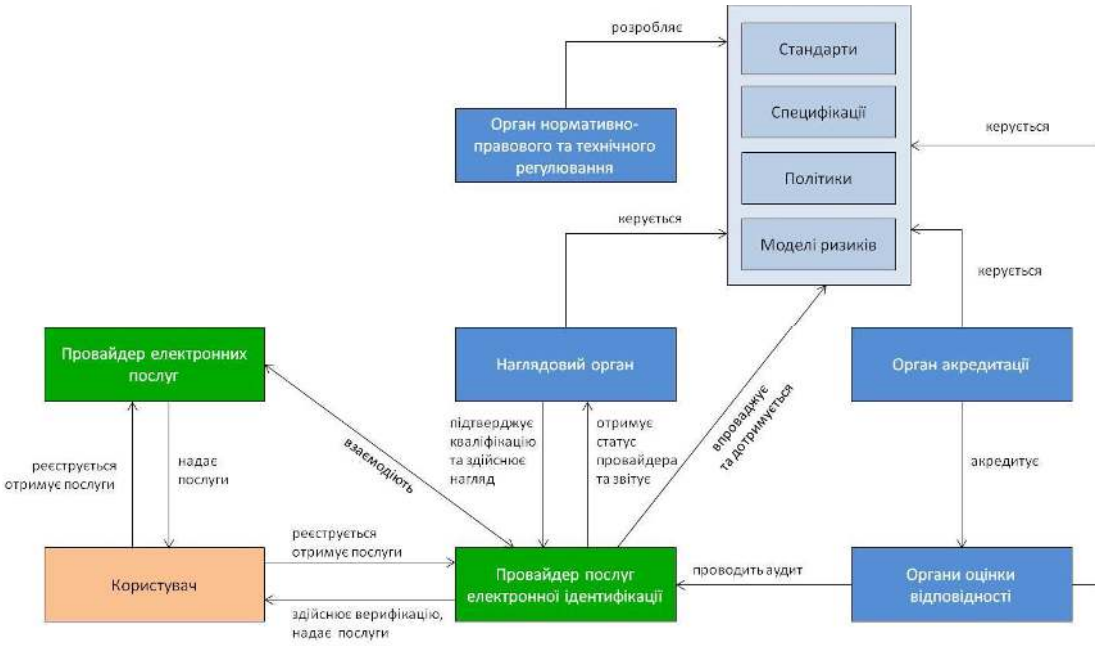


Рис 7.8. Рівень управління інфраструктури електронної ідентифікації

Завдання побудови нормативно-правової моделі рівня управління інфраструктури електронної ідентифікації повинно стати пріоритетним в череді заходів реалізації Стратегії та розглядатись як фундаментальна основа успіху вирішення проблеми та перспектив ефективного впровадження і розвитку електронних послуг в Україні.

7.3 Узагальнені характеристики системи електронної ідентифікації

У разі побудові системі електронної ідентифікації з урахуванням принципів, що викладені раніше, можна очікувати на такі характеристики системи:

1. Учасники електронних транзакцій можуть довіряти один одному та мають бути впевнені у безпеці електронних транзакцій. Автентифікація учасників здійснюється на основі надійних верифікованих ідентифікаційних даних з використанням електронної ідентифікації та у довіреному середовищі. Надання електронних послуг здійснюється з урахуванням оцінки ризиків, яка забезпечує гнучкість для довірчих сторін та встановлює рівні гарантій. Забезпечення гарантій спирається на балансі між безпекою, ризикам, зручністю, конфіденційністю та простотою використання.

2. Фізичні особи можуть здійснювати електронні транзакції з декількома організаціями без зниження рівня конфіденційності (або з вибором рівня конфіденційності). Користувач може обрати використання захищених реєстраційних даних для анонімного входу у систему або входу під псевдонімом. Розкриття персональних даних не є обов'язковим. Постачальники електронних послуг мають забезпечити недоторканість приватного життя шляхом застосування встановлених правил та етики обміну інформацією, при цьому забезпечуючи захист ідентифікаційних даних, що надаються постачальником послуг електронної ідентифікації. Фізичні особи мають право запитувати, отримувати, змінювати та редагувати персональні дані та особисту інформацію (але унікальній ідентифікатор має бути не змінюваним).

3. Технічні рішення електронної ідентифікації (засоби та схеми електронної ідентифікації) мають бути простими у використанні для користувачів та ефективними для постачальників ідентифікації та електронних послуг. Інфраструктура електронної ідентифікації має забезпечувати зручність користувачу, що перш за все виключає необхідність входу у різні системи з використанням різних облікових записів для різних постачальників електронних послуг та різних сторін, які довіряють. Інфраструктура електронної ідентифікації зменшує надлишковість процесів перевірки справжності, управління обліковими записами за рахунок довірі та розподілу послуг.

4. Технічні рішення з електронної ідентифікації мають бути такими, що модифікуються та розвиваються у часі. Ці рішення мають бути функціонально сумісними, використовувати модульні компоненти з чітко визначеними та специфікованими інтерфейсами. Це забезпечить можливість оновлювання та заміни окремих компонентів системи без зміни архітектури системи електронної ідентифікації у цілому. Система має будуватися на основі кращих практик та принципів, що забезпечують гнучкість та адаптацію до нових технологій та вимог безпеки.

8. Першочергові завдання з реалізації стратегії

Реалізація Стратегії вимагає складного комплексу заходів, що включають політичні, юридичні, технологічні та освітні процесі, які торкаються широкого кола зацікавлених сторін. У цьому розділі сформульовані першочергові дії, які уряд та приватний сектор можуть сумісно реалізувати для ефективного впровадження технології електронної ідентифікації у кіберпросторі Україні. Успіх реалізації Стратегії вимагає спільної участі, сумісної роботи та підзвітності всіх учасників як у державному, так і в приватному секторі. Наведені нижче першочергові дії мають вирішальне значення для реалізації Стратегії. При чому Уряд України має бути лідером у впровадження технології електронної ідентифікації та реалізації першочергових дій.

Першочергові дії не охоплюють всі заходи, що необхідні для досягнення цілей та задач Стратегії. Це основні напрямки діяльності, які будуть більш детально розкриті у плані впровадження електронної ідентифікації.

8.1. Призначення державної органу з питань реалізації Стратегії

Уряд України має здійснювати стратегічне управління та безпосередньо керівництво процесами впровадження системи електронної ідентифікації. Уповноважений орган виконавчої влади (далі - Агентство) має відповідати за координацію процесу впровадження системи електронної ідентифікації та контроль за іншими установами і підприємствами, які будуть здійснювати відповідні заходи Стратегії. Інші міністерства та відомства будуть примати участь у впровадження системи електронної ідентифікації, у частині, що пов’язана з їх сферою діяльності та відповідальності.

Основні задачі Агентства повинні полягати у наступному:

- здійснювати нормативно-правове та технічне регулювання сфери електронної ідентифікації;
- проведення оцінювання прогресу щодо досягнення цілей, виконання задач та дій, що викладенні у цій Стратегії;

- реалізовувати керівну роль уряду та держави у впровадженні, розробці та підтримки технологій електронної ідентифікації;
- координувати діяльність державних та приватних структур, що будуть залучені у процес створення системи електронної ідентифікації та наданні електронних довірчих послуг на принципах співробітництва та дольової участі;
- підтримувати міжвідомче співробітництво та координувати міжвідомчі зусилля з реалізації Стратегії, у тому числі у напрямку побудови інфраструктури забезпечення інтероперабельності;
- створювати консультативні механізми в державному та приватному секторах та механізми залучення всіх зацікавлених сторін у процеси впровадження електронної ідентифікації.

Агентство має активно сприяти міжвідомчому співробітництву, залучати різні організації та підприємства з метою гармонізації та інтеграції різних заходів з реалізації та впровадження Стратегії у державному та приватному секторах та забезпечення координацію діяльності всіх зацікавлених сторін в рамках існуючих та майбутніх ініціатив. Агентство має тісно співпрацювати с державними органами, що відповідають за забезпечення кібербезпеки та інформаційної безпеки держави, а також захисту персональних даних.

8.2. Розроблення Плану реалізації Стратегії

Заходи, що передбачені у Стратегії, створюють основу для майбутньої діяльності, яка має здійснюватися сумісно зі всіма зацікавленими сторонам з державного та приватного сектору. Уряд має розробити План реалізації Стратегії, які спрямовані на швидке впровадження інфраструктури електронної ідентифікації. Планування задач та термінів їх виконання має враховувати можливість використання існуючих розробок, стандартів, інновацій та передових практик всіх зацікавлених сторін у сфері інформаційних технологій, електронного цифрового підпису, криптографічних технологій, технологій забезпечення інформаційної та кібербезпеки.

Співробітництво державного та приватного секторів є ключовим фактором успішної інтеграції запланованих заходів, постановки

задач для індивідуальних та колективних виконавців, визначення термінів, вихідних даних та кінцевих результатів, визначення критичних факторів успіху, гарантії повноти та контрольованості досягнення цілей. План повинен враховувати створення робочих груп у форматі державно-приватного партнерства, передбачати запуск пілотних проектів за територіальним або секторальним принципом із залученням ресурсів приватних установ на добровільних та паритетних засадах.

За допомогою Плану має здійснюватися координація всіх заходів, що проводяться державними установами та приватними підприємствами.

Пропоновані переліки заходів нормативно-правового та технічного регулювання, а також організаційно-технічних заходів впровадження в Україні інфраструктури електронної ідентифікації наведено у Додатках Д та Е до цього документу.

8.3. Активне впровадження електронних послуг для населення та бізнесу

Уряд має виступати основною рушійною силою впровадження електронної ідентифікації та електронних послуг. Державні органи влади всіх рівнів мають приймати активну участь у впровадження системи електронної ідентифікації. Як головний постачальник електронних послуг, що охоплюють фізичних осіб, приватний сектор та інші сфери економіки, уряд має забезпечити як можна глибоке проникнення електронних послуг. Важливою частиною заходів впровадження електронних послуг є широка підтримка державою інноваційних програм та проектів, що спрямовані на впровадження адміністративних послуг з використанням схем електронної ідентифікації. Передача знань та технологій, що будуть отримані у ході реалізації урядових ініціатив, приватному сектору приведе до збільшення пропозицій у сфері електронних послуг і, як результат, до загального успіху.

Уряд має приділяти особливу увагу до впровадження електронних послуг у системи охорони здоров'я, освіти, інформаційних технологій, оборонної промисловості, енергетики, фінансового сектору та інших сфер урядування. З цією метою, Агентство у співпраці з профільними міністерствами, має

переглянути або підготувати державні програми з урахуванням впровадження технологій електронної ідентифікації.

Уряд має приймати участь у відповідних міжнародних та європейських проектах з метою забезпечення інтеорперабельності Національної інфраструктури електронної ідентифікації з відповідними європейськими системами, та системами третіх країн.

Уряд має прийняти відповідні рішення щодо визначення базових засад державної політики у сфері електронної ідентифікації та електронних послуг. Державна політика має бути спрямована на підтримку та розвиток інфраструктури електронної ідентифікації фізичних та юридичних осіб, що повинно стати позитивним фактором для зниження кіберзагроз по відношенню до державних інформаційних ресурсів, інформаційних активів приватного сектору та персональних даних окремих громадян.

8.4. Проведення заходів, спрямованих на підвищення інформаційної безпеки та захисту кіберпростору

Уряд та органи місцевого самоврядування мають проводити активну політику та заходи серед громадян та приватного сектору з метою підвищення рівня інформаційної безпеки, у тому числі конфіденційності даних. Концентрація зусиль на реалізації політики безпеки, процесах та технологіях захисту інформації та даних дозволить всім учасникам схем електронної ідентифікації розробити та впровадити сучасні методи, засоби та стандарти забезпечення конфіденційності, цілісності та доступності інформації та даних, забезпечити безпеку персональних даних та особистої інформації громадян. Уряд має розробляти, планувати та впроваджувати заходи щодо виконання політики безпеки інфраструктури електронної ідентифікації та вимагати від постачальників ідентифікації та електронних послуг:

- надавати короткі, змістовні, своєчасні та зрозуміли повідомлення для користувачів відносно збору, використання, розповсюдження та технічної обробки персональних даних та особистої інформації;
- обмежувати збір та передачу ідентифікаційних даних учасників системи електронної ідентифікації, використовувати мінімум інформації, яка потрібна для виконання конкретної операції (транзакції);

- обмежувати зберігання даних до терміну, який необхідний лише для надання послуг окремим користувачам, якщо інше не передбачено законом;
- мінімізувати накопичення даних та послинь, які формують у результаті здійснення електронних транзакцій в системи електронної ідентифікації;
- створювати механізми, що надають окремим особам можливість доступу, редагування та видалення інформації, а також мінімізувати перешкоди для задоволення відмови фізичних осіб від послуг електронної ідентифікації;
- встановлювати стандарти та специфікації стосовно протоколів форматів даних та ідентифікаторів, що використовуються в технічних рішеннях електронної ідентифікації;
- захищати та надійно знищувати інформацію у разі відмови юридичних або фізичних осіб від електронних послуг та послуг електронної ідентифікації;
- пропонувати механізми компенсації особам, які вважають, що їх персональні та особисті данні були використанні не за призначенням.

Орієнтована на користувача інфраструктура електронної ідентифікації відкриває нові можливості для фізичних осіб у сфері контролю та захисту персональних даних за допомогою сучасних технологій захисту інформації. Стратегія закликає до дій, які будуть визначати способи безпечного надання користувачами своїх персональних даних та особистої інформації державним та комунальним установам, приватним підприємствам, а також використовувати зручні механізми управління особистою інформацією.

8.5. Розробка моделей ризику електронної ідентифікації, електронних послуг та стандартів інтероперабельності

Рішення щодо використання технічних рішень електронної ідентифікації має ґрунтуватися на розроблених та затверджених моделях ризику. Модель ризиків, що має бути прийнята, має знижувати ризики безпеки у масштабах держави. Прискорення впровадження системи електронної ідентифікації також суттєво

залежить від розробки та прийняття стандартів, що визначають вимоги до рівнів гарантій електронної ідентифікації. Стандарти мають містити керівні принципи забезпечення конфіденційності та безпеки персональних даних, базові правили стосовно обробки персональних даних, їх накопичення та зберігання. Прийняття стандартів забезпечить незалежність та свободу вибору технічних рішень, гнучкість системи електронної ідентифікації та ефективну міжвідомчу та міжнародну взаємодію.

Базові рекомендації щодо побудови моделей ризику та вибору рівнів гарантій електронної ідентифікації, засновані на положеннях міжнародного стандарту ISO/IEC 29115 наведено у Додатку Г до цього документу.

8.6. Визначення відповідальності постачальників та користувачів послуг електронної ідентифікації

Уряд має визначити відповідальність всіх учасників інфраструктури електронної ідентифікації для забезпечення всебічної надійності та безпеки всіх учасників електронних транзакцій, а також для формування середовища довіри до реалізації протоколів ідентифікації та автентифікації.

8.7. Інформування, просвіта та пропаганда електронних довірчих послуг серед населення та бізнесу

Громадяни та приватній сектор відіграють дуже ключову роль в успішному створенні інфраструктури електронної ідентифікації. Громадяни мають розуміти ризики та переваги застосування електронної ідентифікації, розуміти свої можливості та переваги від отримання послуг електронної ідентифікації. Уряд має докласти зусиль щодо проведення ефективного інформування громадян про переваги електронної ідентифікації, реалізовувати відповідні освітні програми із залученням широкого кола громадських організацій, навчальних закладів та приватних підприємств. Освітня інформація має бути доступною та зрозумілою. Діяльність по підвищенню освіченості громадян має проводиться як у державному, так і у приватному секторі. Навчальні заклади мають впроваджувати відповідні просвітні програми.

Уряд разом с приватними організаціями має адаптувати просвітню діяльність до характеру аудиторії, використовувати засоби масової інформації з метою доведення до громадян відомості про ризики та переваги застосування електронної ідентифікації та електронних послуг. Має бути прийнята довгострокова соціальна рекламна компанія щодо електронних послуг, їх постачальників та переваги отримання електронних адміністративних послуг. На державному рівня необхідно реалізовувати механізми мотивування та добровільного використання електронних послуг населення та організаціями різної форми власності. Всі ці дії будуть підвищувати ефективність просвітньої діяльності та стануть важливим чинником подальшого поліпшення надання електронних послуг.

8.8. Міжнародне співробітництво

Україна має посилити рівень своєї участі у міжнародних організаціях та ініціативах щодо забезпечення кібербезпеки, впровадження схем електронної ідентифікації та надійних засобів електронної ідентифікації шляхом підбору відповідного персоналу та учасників міжнародних проектів та програм.

На національному рівні необхідно спрямувати свою діяльність щодо гармонізації міжнародних та європейських стандартів з метою виключення локальних розробок, обміну науково-технічною

інформацією, а також з метою впровадження сучасних підходів та технологій в сфері електронної ідентифікації.

Співробітництво на міжнародному рівні не має бути виключно відповідальністю Уряду. Приватні підприємства також повинні бути відповідальними за успіх реалізації Стратегії.

Уряд має підтримувати ініціативи приватних компаній щодо міжнародного співробітництва в цій сфері. Успіх Стратегії пов'язаний з використанням корпораціями та приватними компаніями національних схем електронної ідентифікації, включення національних ідентифікаторів до міжнародних систем електронної ідентифікації.

Уряд України має посилити пріоритетність, координацію та участь представників держави та приватного сектору у міжнародних та європейських органах стандартизації та інших органах (робочі групи, форми, науково-технічні ради тощо), що здійснюють діяльність в сфері електронної ідентифікації.

Кінцевою метою реалізації Стратегії на міжнародному рівні повинна стати успішна нотифікація схем електронної ідентифікації України на рівні Європейського Союзу та визнання електронної ідентифікації суб’єктів інших країн в України, а також отримання електронних послуг громадянами України у системах надання таких послуг за кордоном.

ЗАКЛЮЧНА ЧАСТИНА

ДОДАТКИ

Додаток А. Терміни та визначення

«Автентифікація»	-	Електронний процес, що дозволяє підтвердити електронну ідентифікацію фізичної або юридичної особи; або походження та цілісність електронних даних
«Авторизація»	-	Надання повноважень. Авторизація стосується: (а) повноважень автентифікованого об'єкта щодо виконання певної дії або використання певного сервісу / ресурсу; (б) процес визначення за оцінкою відповідних дозволів можливості автентифікованого об'єкта мати доступ до певного ресурсу. Після автентифікації користувачеві може бути надано повноваження щодо різних типів доступу або діяльності, засновані на тому, ким є користувач, які його посадові функції або інших аспектах політики безпеки
«Верифікація»	-	Процес перевірки інформації шляхом порівняння представленої інформації з раніше підтвердженою інформацією
«Верифікація ідентичності»	-	Процес перевірки інформації про справжність ідентичності та реєстраційних даних по видавцям, джерелам даних або іншим внутрішнім або зовнішнім ресурсам щодо автентичності, достовірності, правильності та зв'язку з об'єктом

«Гарантія електронної ідентифікації»	-	Ступінь довіри, отриманий в ході автентифікації, до того, що фізична або юридична особа є тією, яка вона є за її ствердженням, або тією, на яку очікується
«Електронна ідентифікація»	-	Процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну або юридичну особу або фізичну особу, що представляє юридичну особу
«Засіб електронної ідентифікації»	-	Матеріальний, та/або нематеріальний елемент, який містить ідентифікаційні дані особи і використовується для автентифікації в он-лайн послугах
«Ідентифікатор»	-	Унікальний атрибут, який дозволяє встановити ідентичність фізичної або юридичної особи
«Ідентифікаційні дані особи», «ідентичність»	-	Набір даних, який дозволяє встановити фізичну або юридичну особу, або фізичну особу, яка представляє юридичну особу
«Контекст»	-	Середовище з певними граничними вимогами, в межах якого існують та взаємодіють об’єкти
«Орган реєстрації»	-	Довірений учасник, який встановлює, здійснює верифікацію та гарантує ідентичність будь-якого об'єкта для постачальника послуг електронної ідентифікації
«Постачальник (провайдер) послуг електронної ідентифікації»	-	Довірений учасник, який випускає реєстраційні дані та/або керує ними
«Реєстраційні дані»	-	Набір ідентифікаційних даних, які надаються як доказ стверджуваної або заявленої ідентичності та/або прав

«Сторона, яка довіряє»	-	Фізична або юридична особа, яка покладається на електронну ідентифікацію
«Схема електронної ідентифікації»	-	Система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним або юридичним особам або фізичним особам, що представляють юридичних осіб

Додаток Б. Перелік міжнародних та європейських стандартів і рекомендацій, що регулюють вимоги до електронної ідентифікації

- Recommendation ITU-T X.1250: Baseline capabilities for enhanced global identity management and interoperability;
- Recommendation ITU-T X.1251: A framework for user control of digital identity;
- Recommendation ITU-T X.1252: Baseline identity management terms and definitions;
- Recommendation ITU-T X.1253: Security guidelines for identity management systems;
- Recommendation ITU-T X.1254: Entity authentication assurance framework;
- Recommendation ITU-T X.1255: Framework for discovery of identity management information;
- ISO 16609:2012 Financial services -- Requirements for message authentication using symmetric techniques;
- ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework;
- EN 726-1:1994 Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 1: Systems overview;
- EN 726-2:1995 Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 2: Security framework;
- EN 726-3:1994 Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements;

- EN 726-4:1994 Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 4: Application independent card related terminal requirements;
- EN 726-5:1999 Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 5: Payment methods;
- EN 726-6:1995 Identification card system - Telecommunications integrated circuit(s) cards and terminals - Part 6: Telecommunication features;
- EN 726-7:1999 Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 7: Security module;
- EN 1332-1:2009 Identification card systems - Human-machine interface - Part 1: Design principles for the user interface;
- EN 1332-2:1998 Identification card systems - Man-machine interface - Part 2: Dimensions and location of a tactile identifier for ID-1 cards;
- EN 1332-3:2008 Identification card systems - Man-machine interface - Part 3: Keypads;
- EN 1332-4:2007 Identification card systems - Man-machine interface - Part 4: Coding of user requirements for people with special needs;
- EN 1332-5:2006 Identification card systems - Man-machine interface - Part 5: Raised tactile symbols for differenciation of application on ID-1 cards;
- EN 1362:1997 Identification card systems - Device interface characteristics - Classes of device interfaces;
- EN 1375:2002 Identification card system - Intersector integrated circuit(s) card additional formats - ID-000 card size and physical characteristics;
- EN 1387:1996 Machine readable cards - Health care applications - Cards: General characteristics;
- EN 1545-1:2005 Identification card systems - Surface transport applications - Part 1: Elementary data types, general code lists and general data elements;

- EN 1545-2:2005 Identification card systems - Surface transport applications - Part 2: Transport and travel payment related data elements and code lists;
- EN 1546-1:1999 Identification card systems - Inter-sector electronic purse - Part 1: Definitions, concepts and structures;
- EN 1546-2:1999 Identification card systems - Inter-sector electronic purse - Part 2: Security architecture;
- EN 1546-3:1999 Identification card systems - Inter-sector electronic purse - Part 3: Data elements and interchanges;
- EN 1546-4:1999 Identification card systems - Inter-sector electronic purse - Part 4: Data objects;
- EN 1867:1997 Machine-readable cards - Health care applications - Numbering system and registration procedure for issuer identifiers;
- EN 15320:2007 Identification card systems - Surface transport applications - Interoperable Public Transport Applications – Framework;
- EN 419212-1:2014 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services;
- EN 419212-2:2014 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services;
- EN 419251-1:2013 Security requirements for device for authentication - Part 1: Protection profile for core functionality
- EN 419251-2:2013 Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application
- EN 419251-3:2013 Security requirements for device for authentication - Part 3: Additional functionality for security targets;
- CEN/TS 15291:2006 Identification card system - Guidance on design for accessible card-activated devices;
- CEN/TS 15480-1:2012 Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics;
- CEN/TS 15480-2:2012 Identification card systems - European Citizen Card - Part 2: Logical data structures and security services;

– CEN/TS 15480-3:2014 Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface;

– CEN/TS 15480-4:2012 Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use;

– CEN/TS 15480-5:2013 Identification card systems - European Citizen Card - Part 5: General Introduction;

– CEN/TS 16634:2014 Personal identification - Recommendations for using biometrics in European Automated Border Control.

Додаток В. Вимоги до захисту інформації в автоматизованих системах

Законодавством визначено, що відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі.

План захисту інформації розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованої політики безпеки інформації.

План захисту інформації в системі серед іншого повинен містити:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;
- визначення моделі загроз для інформації в системі;
- основні вимоги щодо захисту інформації та правила доступу до неї в системі.

У контексті цього документа саме ці розділи плану захисту інформації у підсумку визначають методи ідентифікації користувачів інформації та механізми автентифікації в системі.

Нормативним документом сфери захисту інформації «Типове положення про службу захисту інформації в автоматизованій системі» НД ТЗІ 1.4-001-2000, затвердженим наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації

Служби безпеки України від “ 04 ” грудня 2000 р. № 53[52] достатньо в повному обсязі визначено перелік заходів, які необхідно здійснити задля розробки плану захисту інформації та його реалізації. У тому числі це стосується обґрунтованого та адекватного вибору методів та механізмів захисту інформації, до яких належать і механізми ідентифікації та автентифікації користувачів інформації.

Базовим заходом, здійснення якого напряму впливає на адекватність вибору того чи іншого механізму ідентифікації та автентифікації в системі, є проведення класифікації інформації, що обробляється в системі.

Повинні бути класифіковані всі відомості за режимом доступу, за правовим режимом, а також за типом їхнього представлення в системі. Класифікація є підставою для визначення власником (розпорядником) інформації або системи методів і способів захисту кожного окремого виду інформації.

За режимом доступу інформація в системі має бути поділена на відкриту та з обмеженим доступом.

Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави, відкриту інформацію, вимога щодо захисту якої встановлена законом, важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

Основою для проведення аналізу ризиків і формування вимог до системи захисту, відповідно до згаданого документу, є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз визначається перелік суттєвих загроз, описується методи і способи їх здійснення.

У контексті цього документа важливим є визначення таких способів здійснення загроз як маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування програм та вкорінення комп’ютерних вірусів.

---

52 http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=03E3BD121B67C1CDD72AD8E02F86F9B4?id=106341

Обов'язково мають бути враховані такі види загроз для безпеки інформації як помилки персоналу і користувачів системи під час експлуатації та навмисні дії (спроби) потенційних порушників.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи системи або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад"), що важливо враховувати для вирішення завдань, порушених у Стратегії.

У кожному конкретному випадку, виходячи з технології обробки інформації в системі, має бути розроблено модель порушника, яка повинна бути адекватна реальному порушнику для даної системи. Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін.

Модель порушника повинна визначати:

- можливу мету порушника та її градацію за ступенями небезпечності для інформаційної системи;
- категорії осіб, з числа яких може бути порушник.;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Докладно вимоги та рекомендації щодо вибору моделі порушника наведено в НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

Важливим елементом при побудові системи захисту є розробка політики безпеки інформації в системі.

Під політикою безпеки інформації (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості обчислювальної системи, фізичного середовища та інші чинники.

В системі може бути реалізовано декілька різних політик безпеки, які істотно відрізняються. Це напряму стосується і вибору того чи іншого методу ідентифікації та автентифікації користувачів інформації.

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування в системі кожного з цих видів.

Одним із основних принципів політики безпеки, визначених в НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» є достатність механізмів і заходів захисту та їхньої адекватності загрозам, що потрібно враховувати у контексті завдань Стратегії.

Також слід враховувати, зокрема під час вибору методу ідентифікації та автентифікації користувачів інформації, що політика безпеки повинна доказово дає гарантії того, що:

- в системі (в кожній окремій складовій частині, в кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування системи забезпечується можливість оцінювання та перевірки захищеності інформації.

Для вирішення питань, порушених у цьому документі, під час розробки політики безпеки серед іншого необхідно провести аналіз ризиків, який передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в системі.

Під час проведення аналізу ризиків необхідним є виконання наступних робіт, безпосередньо пов'язаних із завданнями Стратегії.

1) Встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) системи. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс системи. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз.

2) Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо.

Існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Докладно вимоги та рекомендації щодо оцінки ризиків наведено в НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

Під час вибору моделі захисту системи взагалі і методів ідентифікації та автентифікації її користувачів, зокрема, обов'язковим є оцінювання величини можливих збитків, пов'язаних з реалізацією загроз.

Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені системі (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від

втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості системою внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків - відсутня, низька, середня, висока, неприпустимо висока).

У подальшому, в залежності від конфіденційності інформації, яка обробляється в системі, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника системи, а також інших чинників обґрунтовується пропозиція щодо доцільності застосування варіантів побудови системи захисту.

Можливі наступні варіанти:

- досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в системі;
- досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в системі;
- досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в системі.

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації. Під час розгляду різних варіантів реалізації рекомендується серед іншого враховувати наступні аспекти:

- реєстрація санкціонованих користувачів системи, авторизація користувачів в системі;
- керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів;
- забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів.

Підтвердження відповідності впроваджених заходів та засобів безпеки, у тому числі методів ідентифікації та автентифікації, здійснюється за результатами державної експертизи комплексної системи захисту інформації та її атестації, порядок проведення яких визначено наказом Адміністрації Держспецзв'язку від 16.05.2007 №93 «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації»[53].

[53] http://zakon4.rada.gov.ua/laws/show/z0820-07

Додаток Г. Моделі ризиків для інфраструктури електронної ідентифікації.

За основу розробки моделей ризиків для інфраструктури електронної ідентифікації слід брати положення міжнародного стандарту ISO/IEC 29115 та нормативних документів з питань технічного захисту інформації (НД ТЗІ).

Стандартом ISO/IEC 29115 визначено основні шляхи вибору рівня гарантій електронної ідентифікації відносно ризиків від впливу хибної ідентифікації та автентифікації та ймовірних загроз на кожному з етапів функціональної моделі.

Ставлячи у відповідність рівні впливу до рівнів гарантій електронної ідентифікації, сторони транзакції мають визначити, який рівень гарантій необхідний, встановити вимоги до послуг електронної ідентифікації у контексті безпеки. У Таблиці Г наведено можливі наслідки та впливи хибної автентифікації на різних рівнів гарантій електронної ідентифікації.

Таблиця Г Можливі наслідки та впливи хибної автентифікації на різних рівнів гарантій електронної ідентифікації

Можливі наслідки хибної ідентифікації та автентифікації	**Потенційний вплив хибної автентифікації відносно рівнів гарантій електронної ідентифікації за ISO 29115**			
	Low	Medium	High	Very High
Незручність, підрив репутації, шкода для репутації або стану	Мн.*	Пм.	Ст.	Вс.
Фінансові втрати або відповідальність організації	Мн.	Пм.	Ст.	Вс.
Нанесення шкоди організації, її програмам або суспільним інтересам	Н/З	Мн.	Пм.	Вс.
Несанкціоноване розкриття конфіденційної інформації	Н/З	Пм.	Ст.	Вс.
Особиста безпека	Н/З	Н/З	Мн. Пм.	Ст. Вс.

Адміністративні правопорушення або кримінальні злочини	Н/З	Мн.	Ст.	Вс.
* Мн. – мінімальний, Пм. – помірний, Ст. – суттєвий, Вс. – високий, Н/З – не можна застосовувати				

Визначення того, що є мінімальним, помірним, істотним та високим ризиком, обумовлено критеріями ризику, визначеними стороною, що довіряє (провайдером електронних послуг, адміністратора порталу адміністративних послуг) для кожного з можливих наслідків. Поряд з цим, можливо застосовувати сценарії з декількома видами впливу (наприклад, наслідки можуть включати шкоду для організації, а також несанкціоноване розкриття конфіденційної інформації). За сценаріями транзакцій з декількома видами впливу слід використовувати найбільш високий рівень гарантій електронної ідентифікації, відповідний до ймовірних наслідків.

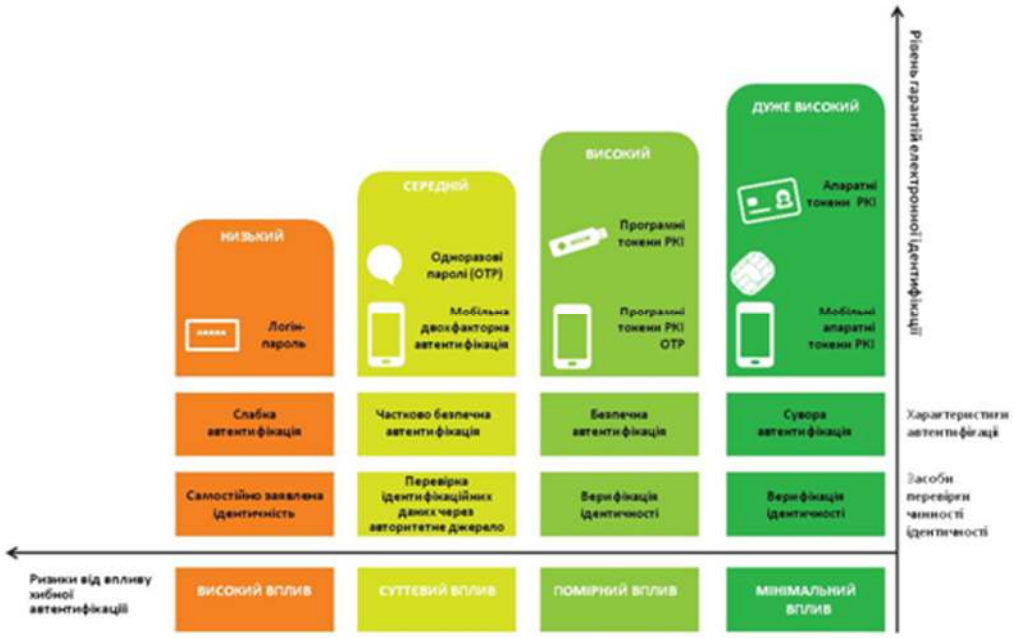


Рис.Г.1 Умовна матриця ризиків хибної автентифікації, рівнів гарантій електронної ідентифікації та засобів електронної ідентифікації

Кожний рівень гарантій електронної ідентифікації повинен бути визначений за силою та строгістю способів захисту від загроз та процесів, які постачальник (провайдер) послуг електронної ідентифікації застосовує відносно послуг, що ним надаються, для кожного етапу функціональної моделі.

Постачальники (провайдери) електронних послуг, в свою чергу, повинні встановити конкретні критерії виконання вимог кожного

рівня гарантій електронної ідентифікації, які вони планують забезпечувати. Ці постачальники повинні оцінити провайдерів послуг електронної ідентифікації, які заявляють про відповідність цим критеріям.

Аналогічно, провайдери послуг електронної ідентифікації повинні визначити рівні гарантій, яким їх послуги відповідають, шляхом оцінки своїх робочих процесів і технічних механізмів на відповідність конкретним критеріям.

Можливим варіантом такого визначення може бути впровадження процедур оцінки відповідності з боку незалежної компетентної організації, яка має відповідну акредитацію відповідно до законодавства.

Оцінка ризику транзакції може бути проведена в рамках загальної оцінки ризиків інформаційної безпеки в організації (наприклад, за ISO/IEC 27001 або за НД ТЗІ). Її слід проводити згідно конкретної потреби у забезпеченні безпеки передбачуваних транзакцій.

Результати оцінки ризику повинні порівнюватися з рівнями гарантій електронної ідентифікації. Вибиратися повинен той рівень гарантій, який найбільшою мірою відповідає результатам оцінки ризику.

Якщо надання електронних послуг передбачає декілька класів транзакцій, можливо застосовувати різні рівні гарантій електронної ідентифікації до кожної транзакції або до групи транзакцій. Іншими словами, в системі надання електронних послуг, яка належить одній організації, можуть бути прийняті кілька рівнів гарантій електронної ідентифікації в залежності від конкретної транзакції.

Додаток Д. Перелік заходів нормативно-правового та технічного регулювання впровадження в Україні інфраструктури електронної ідентифікації

№	Зміст заходу	Якісні та кількісні показники виконання	Строк виконання	Виконавці
1.	Розробка нових та внесення змін до чинних законодавчих та підзаконних актів з метою створення правової основи для сфери електронної ідентифікації фізичних та юридичних осіб в інформаційних системах, які використовуються для надання адміністративних та інших послуг в електронній формі, у тому числі з питань:			Мін'юст, Адміністрація Держспецзв'язку, Мінекономрозвитку, Державне агентство з питань електронного урядування, ДМС, МВС, МЗС, Мінфін, Національний банк України, Комітети Верховної Ради України, Громадські об'єднання та організації
	- законодавчого визначення уповноваженого органу з питань нормативно-правового та технологічного регулювання сфери електронної ідентифікації;	Рішення Уряду	III квартал 2015	
	- нормативного визначення альтернативних засобів електронної ідентифікації для надання адміністративних послуг в електронній формі	Рішення Уряду	IV квартал 2015	

	- нормативного визначення засад надання послуг електронної ідентифікації	Рішення Уряду	IV квартал 2015	
	- внесення електронного посвідчення особи до переліку документів, що посвідчують особу громадянина України;	Зміни до Закону України «Про Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус	IV квартал 2015	
	- умов взаємного визнання засобів електронної ідентифікації з урахуванням вимог статті 6 Регламенту №910/2014;	нормативно-правовий акт України проект міжнародного акту	IV квартал 2015	
	- розробки нормативно-правових актів, гармонізованих із виконавчими актами Європейської Комісії, які визначають умови, формати та процедури нотифікації схем електронної ідентифікації та прийняті згідно із вимогами статей 9 та 10 Регламенту №910/2014;	нормативно-правовий акт України проект міжнародного акту	IV квартал 2015	
	- вимог щодо призупинення або відкликання схем електронної ідентифікації та автентифікації у разі порушення безпеки з урахуванням вимог статті 10 Регламенту №910/2014;	нормативно-правовий акт України проект міжнародного акту	IV квартал 2015	
	- законодавчого закріплення вимог щодо відповідальності сторін, які видають засоби електронної ідентифікації, за шкоду, заподіяну фізичним та юридичним особам через недотримання вимог	Зміни до Кодексів України	II квартал 2016	

	законодавства з урахуванням вимог статей 7 та 11 Регламенту №910/2014;			
	- розробка проекту нормативно-правового акта, який визначає сфери використання алгоритмів та протоколів криптографічного захисту інформації у засобах електронного цифрового підпису, електронної ідентифікації в інформаційних системах, в яких здійснюється обробка та захист державних інформаційних ресурсів, та в системах транскордонної взаємодії;	Рішення Уряду	IV квартал 2015	
	- гармонізація стандартів, прийняття технічних специфікацій та процедур стосовно рівнів гарантії, які повинні застосовуватись для схем електронної ідентифікації, які повинні бути уведені до 18 вересня 2015 року виконавчими актами Європейської Комісії у відповідності до статті 8 Регламенту №910/2014;	Наказ Мінекономрозвитку	II квартал 2016	
	- гармонізація стандартів, технічних специфікацій та процедур з урахуванням критеріїв функціонування інфраструктури сумісності схем електронної ідентифікації, які повинні бути уведені до 18 вересня 2015 року виконавчими актами Європейської Комісії згідно із вимогами статті 12 Регламенту №910/2014;	Наказ Мінекономрозвитку	II квартал 2016	
2.	Міжнародне співробітництво з Європейською Комісією та			Мін'юст, Адміністрація

	державами-членами Європейського Союзу з питань впровадження схем електронної ідентифікації та транскордонних електронних довірчих послуг, у тому числі:			Держспецзв'язку, Мінекономрозвитку, Державне агентство з питань електронного урядування, Національний банк України, ДМС, МВС, МЗС, Мінфін, Громадські об'єднання та організації
	- інтеграція до створюваної в рамках Європейського Союзу інфраструктури інтероперабельності схем електронної ідентифікації з урахуванням складових співробітництва та процедурних механізмів, прийнятих до 18 березня 2015 року виконавчими актами Європейської Комісії згідно із вимогами статті 12 Регламенту №910/2014;	Міждержавні (міжгалузеві угоди)	III квартал 2016	

Додаток Е. Перелік організаційно-технічних заходів впровадження в Україні інфраструктури електронної ідентифікації

№	Зміст заходу	Якісні та кількісні показники виконання	Строк виконання	Виконавці
1.	Розробка нормативно-технічної документації та впровадження існуючих нормативно визначених засобів електронної ідентифікації для надання пріоритетних електронних послуг	Діюча система надання пріоритетних електронних послуг	III квартал 2015	Державне агентство з питань електронного урядування, Мін'юст, Адміністрація Держспецзв'язку, Мінекономрозвитку, Мінфін, інші зацікавлені органи виконавчої влади та місцевого самоврядування, акредитовані центри сертифікації ключів
2.	Розробка нормативно-технічної документації та запуск пілотного проекту схеми електронної ідентифікації з використанням прототипу документу, що посвідчує особу у форматі електронної старт-картки	Діючий пілотний проект із функціональними можливостями інтеграції із системами надання електронних послуг	IV квартал 2015	Державне агентство з питань електронного урядування, Мін'юст, Адміністрація Держспецзв'язку, Мінекономрозвитку, Національний банк України, ДМС, МВС, МЗС, ЦВК, Мінфін, інші зацікавлені органи виконавчої влади та місцевого самоврядування
3.	Розробка нормативно-технічної документації та	Діючий пілотний проект із	I квартал	Державне агентство з питань електронного

	запуск пілотного проекту схеми електронної ідентифікації з використанням засобів банківської електронної ідентифікації	функціональними можливостями інтеграції із системами надання електронних послуг	2016	урядування, Мін'юст, Адміністрація Держспецзв'язку, Мінекономрозвитку, Мінфін, інші зацікавлені органи виконавчої влади та місцевого самоврядування, банківські установи
4.	Розробка нормативно-технічної документації та запуск пілотного проекту схеми електронної ідентифікації з використанням засобів мобільної ідентифікації	Діючий пілотний проект із функціональними можливостями інтеграції із системами надання електронних послуг	I квартал 2016	Державне агентство з питань електронного урядування, Мін'юст, Адміністрація Держспецзв'язку, Мінекономрозвитку, Мінфін, інші зацікавлені органи виконавчої влади та місцевого самоврядування, оператори мобільного зв'язку
5.	Аналіз показників результатів роботи пілотних проектів та визначення пріоритетних напрямків інтеграції схем електронної ідентифікації до інфраструктури електронної ідентифікації України	Рішення щодо подальшого розвитку інфраструктури електронної ідентифікації	II квартал 2016	Державне агентство з питань електронного урядування, учасники пілотних проектів
6.	Розробка нормативно-технічної документації на інтегровану інфраструктуру електронної ідентифікації України	Затверджене технічне завдання на створення інтегрованої інфраструктури електронної ідентифікації України	III квартал 2016	Державне агентство з питань електронного урядування, учасники пілотних проектів
7.	Проектування та введення в експлуатацію інтегрованої	Діюча інфраструктура електронної	II квартал 2017	Державне агентство з питань електронного

	інфраструктури електронної ідентифікації України	ідентифікації України		урядування, учасники пілотних проектів