УКРАЇНСЬКИЙ ЦЕНТР ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ

3/3

Андрій Дресвянніков

НА ШЛЯХУ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС: ДОВІРЧІ ПОСЛУГИ

#дослідження

www.ucep.org.ua

Рецензія:

Дмитро Науменко
старший аналітик ГО "Український центр європейської політики"

Дослідження політики в контексті імплементації
Додатку XVII-3 Угоди про асоціацію

НА ШЛЯХУ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС: ДОВІРЧІ ПОСЛУГИ

Д-р Андрій Дресвянніков

Літературна корекція: Катерина Потапенко

Дизайн та верстка: Олександр Іванов

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного Фонду Відродження в межах грантового компоненту проєкту EU4USociety.

Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду Відродження та Європейського Союзу.

ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

УКРАЇНСЬКИЙ ЦЕНТР ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ

ЗМІСТ

4 ВСТУПНЕ СЛОВО

7 РЕЗЮМЕ

9 МЕТА РОБОТИ

11 ПЕРЕДУМОВИ

13 ОГЛЯД ЧИННОЇ ПОЛІТИКИ У СФЕРІ ДОВІРЧИХ ПОСЛУГ

23 ЗМІНИ В СЕРЕДОВИЩІ, ЯКІ ВІДБУВАЮТЬСЯ ТА ВПЛИВАЮТЬ НА РОЗВИТОК ДОВІРЧИХ ПОСЛУГ В УКРАЇНІ

24 АНАЛІЗ ДОСТУПНИХ АЛЬТЕРНАТИВ

27 ВІЗІЯ АВТОРІВ ДОСЛІДЖЕННЯ

28 БАЧЕННЯ БАЖАНОГО РЕЗУЛЬТАТУ

29 РЕКОМЕНДАЦІЇ ЩОДО НЕОБХІДНИХ ДІЙ

32 ОГЛЯД РИЗИКІВ

33 ОЧІКУВАНИЙ ДОВГОСТРОКОВИЙ ВПЛИВ

ВСТУПНЕ СЛОВО

За останні декілька років відбувся суттєвий прогрес у сфері цифровізації та новітніх технологій. Розвиток цифрових технологій стосується багатьох сфер сучасного життя, від освіти та робочих місць до системи соціального забезпечення та впливу на систему державного управління. Цифрові інструменти забезпечують прозорість влади та ефективніше електронне урядування, сприяють економічному зростанню, виробництву та експорту, через підвищення продуктивності існуючих індустрій, та створення принципово нових сфер цифрової економіки з підвищеною доданою вартістю. Також цифровізація веде до спрощення умов для розвитку бізнесу, залучення інвестицій, та надає ширші можливості для задоволення інтересів та захисту прав споживачів.

Саме тому цифровізація розглядається як важливий елемент сталого розвитку економіки та суспільства, а такі технології як інтернет речей (IoT), хмарні технології, електронна ідентифікація (eID) та штучний інтелект (AI) можуть сприяти досягненню Глобальних Цілей Сталого Розвитку Організації Об'єднаних Націй до 2030 року.

Технологічні зміни відбуваються швидко. Це вимагає якісного та своєчасного реагування, у тому числі і в питаннях адаптації законодавчого та регуляторного полів. Європейський Союз та інші розвинені країни не тільки декларують підтримку розвитку цифрового простору, але й роблять практичні кроки в цьому напрямі.

Підхід ЄС до цифрової трансформації означає розширення можливостей та залучення до неї кожного громадянина, посилення потенціалу кожного бізнесу та вирішення глобальних викликів, і передбачений рамковими та стратегічними документами, такими як: Стратегія Єдиного цифрового ринку (Digital Single Market Strategy for Europe)[1], Підключення до Європейського Гігабітного суспільства (Connectivity for a European Gigabit Society)[2], нещодавно розробленої стратегії Цифрова Європа 2025 (Digital Europe 2025) та Програми розвитку загальноєвропейських стандартів у сфері телекомунікацій та цифрових технологій тощо[3].

Стратегія Єдиного цифрового ринку ЄС була запропонована Європейською Комісією у 2015 році з метою досягнення синергії між країнами ЄС у царині новітніх технологій, транскордонної торгівлі та надання послуг в межах Єдиного цифрового ринку (далі - ЄЦР). Стратегія спрямована на те, щоб економіка, промисловість та суспільство Європи в повній мірі скористатися перевагами нової цифрової ери. ЄС активно створює вільний та безпечний ЄЦР, де люди можуть безпечно спілкуватись, здійснювати покупки в інтернеті без кордонів, а підприємства можуть продавати свої товари/послуги через інструменти електронної комерції по всьому ЄС[4]. Тобто, ЄЦР[5] пропонує розширені можливості для: користувачів, малого та середнього бізнесу, інноваційних стартапів, креативного сектору, наукового та безпекозміцнюючого співробітництва у додаток до модернізації вже існуючих індустрій.

1) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%253A52015DC0192

2) https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society

3) https://www.digitaleurope.org/policies/strongerdigitaleurope/

4) https://www.consilium.europa.eu/en/policies/digital-single-market/

5) За оцінками, цифровізація виробництва до 2025 року принесе ЄС 1,25 трлн. євро.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192
https://www.consilium.europa.eu/en/policies/digital-single-market/

> Головна мета Єдиного цифрового ринку ЄС – усунення зайвих регуляторних бар'єрів і перехід від окремих національних ринків до єдиного, із загальноєвропейськими уніфікованими правилами у трьох секторах Телекомунікації, Довірчі Послуги, та Електронна Комерція.

Надважливим складником у розбудові Єдиного цифрового ринку ЄС є:

- Розбудова телекомунікаційної інфраструктури, яка є основою розвитку цифрового ринку та цифрової економіки включно з впровадженням технологій наступного покоління (розгортання мереж 5G, які покликані забезпечити доступ до ультрашвидкісного інтернету не тільки на рівні громадян, але і цілих міст, секторів економіки, та індустрій важливих для сталого розвитку (як-то: енергетика, екологія, охорона здоров'я, інклюзивність, транспорт, смарт-міста, контроль якості води[6]);
- Впровадження та поширення довірчих послуг та інструментів віддаленої ідентифікації (eID), юридично значимого обміну контрактами та іншими документами;
- Створення передумов для розвитку систем транскордонної електронної комерції та захист прав споживачів електронної комерції по всій Європі.

Формування ЄЦР було невід'ємною складовою частиною Цифрового порядку денного для Європи 2020, який був прийнятий з метою забезпечення сталих економічних та соціальних переваг на основі швидкісного та надшвидкісного інтернет-зв'язку та додатків, що мають багатоцільове призначення. Ці компоненти є ключовими і для концепції створення «Гігабітного суспільства» до 2025 року та «Цифрової Європи 2025».

Останні передбачають гігабітний зв'язок для всіх основних соціально-економічних об'єктів, таких як школи, транспортні вузли, постачальники державних послуг та підприємства, які інтенсивно використовують цифрові технології, розгортання безперебійного 5G покриття для всіх міст та головних наземних транспортних шляхів, розширення можливостей безкоштовного доступу громадян до WI-FI, подальший розвиток конкуренції і захист прав суб'єктів цифрового ринку, в тому числі і на основі нового Європейського Кодексу електронних комунікацій, прийнятого ЄС в грудні 2018 року.

Стратегія Єдиного цифрового ринку ЄС була також продовжена звітом «Формування цифрового майбутнього Європи» (Communication 'Shaping Europe's Digital Future')[7] (2020 року). ЄС поставив за мету стати глобальним зразком для наслідування світової цифрової економіки, а також підтримати країни, що йдуть шляхом відповідального та сталого розвитку. Розвиток та впровадження загальноєвропейських стандартів та координація зусиль між державами-членами ЄС, їх регіонами, суспільством та приватним сектором є ключем до досягнення мети сталого розвитку, цифрового та технологічного лідерства ЄС. Цей план, серед іншого, передбачає можливості для розвитку в країнах сусідах.

Отже, варто зазначити, що ЄС проводить комплексну політику у сфері цифрової економіки та цифрової трансформації, створюючи цілу екосистему. Тому, для України важливо та необхідно формувати координовані з ЄС політики, беручи до уваги стратегічні документи, акти ЄС та задекларовані цілі в комплексі, а не у відриві один від одного. Адже розглядаючи та реалізуючи політики вибірково, на основі набору фрагментованих систем, неможливо забезпечити кумулятивний ефект збільшення якості та кількості при зменшенні витрат. Важливим елементом цієї комплексної політики є встановлення чітких показників, яких планується досягти (KPI), і систем моніторингу їх досягнення та/чи відхилення від запланованого.

6) https://ec.europa.eu/digital-single-market/en/towards-5g

7) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52020DC0067

Такий підхід, зокрема, дозволяє відповідальне коригування політик, визначення впродовж виконання сфер/показників, які потребують додаткової уваги/інвестицій/фінансування, а також допомагає вирішувати новітні виклики (наприклад, COVID-19). Підкреслимо, що важливими є саме незалежні інструменти моніторингу реалізації програм цифрової трансформації та конкурентоспроможності економіки, наприклад Індекс Цифрової Економіки та Суспільства (DESI)[8], що дозволяє інвесторам та міжнародним партнерам відстежувати прогрес кожної держави-члена ЄС у розбудові цифрової економіки та суспільства.

> Україна, як одна з найбільших сусідніх країн ЄС, може бути важливим партнером, який сприяє зростанню європейського цифрового ринку.

Більше того, Україна чітко заявляє про свій намір інтегруватися до ЄЦР ЄС і визначає цей намір одним із ключових пріоритетів і завдань, у тому числі і шляхом імплементації Угоди про асоціацію включно з Додатком XVII-3, який містить положення щодо узгодження в сфері телекомунікацій, частотного нагляду, довірчих послуг, електронної комерції, IT-послуг, аудіовізуальних засобів масової інформації, авторського права та суміжних прав та захисту персональних даних. З огляду на зазначене, важливим є аналіз стану виконання Україною зобов'язань за Додатком XVII-3 та визначення основних шляхів і заходів, яких необхідно вжити для забезпечення розвитку цифрової економіки в Україні та приєднання до ЄЦР ЄС.

8) https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi

РЕЗЮМЕ

Цей документ є дослідженням політики щодо стану довірчих послуг (ДП) та перспектив їх подальшого розвитку в Україні. Початково дослідження планувалося як незалежна експертна оцінка прогресу України у наближенні нормативно-правових актів Додатку XVII-3 Угоди про асоціацію між Україною та ЄС (телекомунікаційні послуги, довірчі послуги та електронна комерція). Однак, у зв'язку із заявою про майбутнє оновлення регламенту ЄС eIDAS з пропозицією щодо підготовки проекту, що надійде до червня 2021 року[9], автори розширили сферу дослідження, щоб забезпечити аналіз українських ДП за чотирма компонентами: юридичний контекст, нагляд, аудит постачальників довірчих послуг, найкращі практики[10]. Також були досліджені: варіанти політик, сценарії, фактори ризику, особливості надання довірчих послуг та електронної ідентифікації в державному секторі. Запропоновані опції пов'язані з розвитком ДП у наданні державних послуг, які є більш ефективними та створюють кращу вартість. Документ націлений на фахову аудиторію, яка обізнана з основними концепціями та положеннями у сфері довірчих послуг та електронної ідентифікації обох сторін Угоди про асоціацію між Україною та ЄС. Зокрема, Міністерство цифрової трансформації України, якого ми бачимо головним поборником української євроінтеграції у сфері довірчих послуг.

Поки що в Україні відсутній програмний документ або програма розвитку довірчих послуг та електронної ідентифікації, що містить систему принципів та заяв про наміри, на основі яких здійснюється прийняття рішень у цій сфері. Однак, проведений аналіз показує, що схема розвитку довірчих послуг в України подібна до ЄС, хоча в певних сферах (стандарти, нагляд і контроль, захист персональних даних) необхідне вдосконалення практик. Це дослідження визначає стратегії, які можуть підтримати український уряд в успішному вирішенні питань та, як наслідок, сприяти кращій позиції України щодо подальших євроінтеграційних кроків, а саме підписання Угоди про взаємне визнання електронних довірчих послуг між Україною та ЄС, набуття режиму внутрішнього ринку та започаткування інтеграції в Єдиний цифровий ринок (ЄЦР).

Основні рекомендації:

- Розробити програмні документи щодо цифрового уряду, довірчих послуг, електронної ідентифікації, захисту персональних даних, електронного архівування, доступності та інклюзивності цифрових продуктів та інформаційно-комунікаційних систем, публічних служб та сервісів, інших суміжних галузей (популяризації цифрових навичок), телекомунікації (мережа 5G, Інтернет речей), наукових досліджень тощо.
- Розробити моделі захисту даних і формування довіри, включивши їх до програмних документів.
- Ініціювати включення України до міжнародних індексів: a) Індекс цифрової економіки та суспільства (I-DESI), b) Індекс обмеженості цифрової торгівлі (DTRI), c) Глобальне визнання довірчих послуг ЄС (ETSI TR 103 684).

9) https://data.consilium.europa.eu/doc/document/ST-14351-2020-INIT/en/pdf

10) https://esignature.ec.europa.eu/intl-comp/dss-demo/downloads/MRAinfo_Cookbook_v1.0.pdf

- Оновити статус підписанта міжнародних угод для Національного Агентства з Акредитації України (НААУ). Змінити чинне законодавство щодо оцінки відповідності українських кваліфікованих надавачів довірчих послуг (КНДП), в тому числі і європейськими органами оцінки відповідності, що зменшить ризики невідповідності.
- Усунути розбіжності в стандартизації щодо кваліфікованих довірчих послуг, кваліфікованих надавачів довірчих послуг, віддаленого кваліфікованого електронного підпису, кваліфікованого пристрою для створення підпису, апаратного модуля безпеки та оцінки відповідності шляхом перегляду та оновлення відповідних стандартів.
- Запровадити міжнародні Загальні критерії рівня достовірності оцінювання для апаратного обладнання, що використовується під час шифрування, забезпечити інфраструктуру відкритих ключів та надання довірчих послуг.
- Доопрацювати та прийняти розроблену у 2020 Стратегію у сфері архівування електронних документів, зокрема щодо довгострокового збереження електронних документів, вивчаючи та переймаючи досвід країн-членів ЄС у цій сфері.
- Створити сервіс перевірки електронних підписів, який може працювати з міжнародними форматами електронних підписів (на основі ECDSA, RSA) у відповідності до міжнародних стандартів.
- Прийняти та розпочати впровадження стандарту EN 301 549 - Вимоги щодо доступності/інклюзивності електронних продуктів та послуг загального користування. Оновити законодавчу базу для включення Європейської директиви про веб-доступність.

Основні ризики можуть бути пов’язані з можливістю розходження у використанні стандартів та принципів, на яких базуються засади політики ЄС щодо електронної ідентифікації та довірчих послуг.

МЕТА РОБОТИ

Як і багато країн у всьому світі, українське суспільство (люди, уряд та бізнес) зазнає трансформаційних змін завдяки цифровим технологіям, які швидко входять у повсякденне життя. Зміни відбуваються у багатьох сегментах - від освіти до сільського господарства. Однією з основних передумов для ефективного функціонування нових цифрових технологій є формування довіри в часто дистанційному цифровому середовищі включно з інтернетом. Довірчі послуги саме і є механізмом формування довіри у цифровому середовищі, і тому дотичні до багатьох областей цифрової трансформації. Для України фактори цифрової трансформації мають два основні вектори: внутрішній та пов'язаний із співпрацею між Україною та ЄС.

Внутрішні фактори розвитку довірчих послуг визначаються головним чином урядом. У 2019 році Президент України Володимир Зеленський публічно оголосив про наміри та початок розбудови "цифрової держави" та "держави в смартфоні". Для їхньої реалізації було створено Міністерство цифрової трансформації, відповідальне за цифрову трансформацію, цифровізацію державних послуг та інтеграцію довірчих послуг. Міністерство цифрової трансформації розпочало новий цикл оцифрування державних послуг. Однак, оновлена стратегія чи програма розвитку у формі загальнодоступного програмного документа не була визначена.

Другий рушій розвитку довірчих послуг в Україні пов'язаний з Угодою про асоціацію між Україною та ЄС та перспективами для України укласти Угоду з ЄС про взаємне визнання електронних довірчих послуг, телекомунікацій та електронної комерції, що дозволить приєднатись до ЄЦР ЄС. Щодо довірчих послуг, Україна та ЄС розробили спільний план[11] співпраці з метою можливого укладання угоди, заснованої на наближенні до законодавства та стандартів ЄС.

Незважаючи на безсумнівний прогрес в цій сфері (про що буде детальніше йтися далі), існують також можливості покращення як у практичних аспектах, так і в баченні, що, на погляд авторів, в разі ігнорування може уповільнити як внутрішні, так і міжнародні зусилля у сфері розвитку довірчих послуг. Ми припускаємо, що розвитку цифрового уряду та довірчих послуг в Україні може сприяти:

1. Програмний документ, який визначає довгострокове бачення суспільства та уряду щодо розвитку довірчих послуг та електронної ідентифікації.
2. Адаптація європейських досліджень щодо порівняння різних моделей захисту даних та моделей формування довгострокової довіри як міцної бази для розбудови електронної ідентифікації в Україні.
3. Включення України до Міжнародного індексу цифрової економіки та суспільства (I-DESI)[12], Глобального визнання довірчих послуг ЄС (ETSI TR 103 684), Індексу обмеженості цифрової торгівлі (DTRI)[13].
4. Проведення оцінки відповідності українських кваліфікованих надавачів довірчих послуг на основі міжнародних стандартів.

11) https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/lyudmila-rabchinska-ukraina-ta-es-spivpratsyuvatimut-zadlya-vzaemnogo-viznannya-elektronnikh-dovirchikh-poslug/20_12_08_EU_UA_Joint_Working_Plan_on_mutual_recognition_of_trust.pdf

12) https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies

13 https://www.oecd-ilibrary.org/trade/the-oecd-digital-services-trade-restrictiveness-index_16ed2d78-en

5. Удосконалення політики та підходів щодо пристроїв створення кваліфікованих підписів (токенів), що здатні забезпечити високий рівень особистого контролю власника над електронним підписом/електронною печаткою, відповідно до Регламенту 910 ЄС (eIDAS).

6. Адаптація та впровадження стандартів Європейського інституту телекомунікаційних стандартів, що регулюють створення та роботу мережевих провайдерів\служб\сервісів надання кваліфікованого електронного підпису - QSCD TYPE 2.

7. Створення Служби перевірки електронних підписів, яка може працювати з міжнародним електронним підписом (на основі ECDSA, RSA).

8. Використання програмних продуктів з відкритим кодом у інформаційних системах та додатках щодо довірчих послуг (особливо у державних КНДП), що зменшує залежність від постачальників та розробників, а в довгостроковій перспективі підвищує безпеку та надійність використовуваних ІКТ-рішень.

9. Усунення торгових бар'єрів з ЄС, спричинених вітчизняними технічними криптографічними стандартами.

Існує також необхідність адаптації українського законодавства до Європейської директиви про веб-доступність/ інклюзивність та Стандарту ETSI 301 549 для українських загальнодержавних чи муніципальних (публічних) інформаційних систем, веб-сервісів та мобільних додатків.

Невизначеність вносить і те, що ЄС та Україна планують значне оновлення законодавства про довірчі послуги у спосіб, який на сьогодні не є узгодженим. Уряд України вже підготував пропозицію[14] оновити понад 80 законів, які можуть спричинити подальші зміни в більше 150 нормативних актах, включаючи суттєві зміни до Закону №2155-VIII "Про довірчі послуги та електронну ідентифікацію". Сьогодні складно зважено та обґрунтовано оцінити запропоновані законодавчі пропозиції, за відсутності Стратегії розвитку та програмних документів бачення майбутнього в цій сфері. З точки зору інтеграції між ЄС та Україною, запропоновані зміни можуть розглядатися як передчасні, оскільки європейське регулювання щодо довірчих послуг та електронної ідентифікації також оновлюється, а проект має бути опублікований у червні 2021 року.

14) https://thedigital.gov.ua/storage/uploads/files/page/ministry/План_роботи_Мінцифри_2021.pdf

ПЕРЕДУМОВИ

Рух українського суспільства в напрямку якісних державних послуг протягом останніх двох десятиліть включав численні ініціативи втілення технологічних інновацій у різноманітних сферах, починаючи від семантики/термінології, законодавства, закінчуючи розробкою національних стандартів. У 2014 році була досягнута суттєва віха, коли ЄС та Україна підписали Угоду про зону вільної торгівлі (DCFTA) та Угоду про асоціацію (АА)[15]. Це зміцнило євроінтеграційний вектор розвитку України, а також встановило дорожню карту для узгодження з регламентами і технічними стандартами ЄС. Вимоги наближення нормативних актів у трьох взаємопов'язаних областях - телекомунікації, довірчі послуги та електронна комерція - були визначені в Додатку XVII-3[16] Угоди. Ці наближення вимагають змін у стандартах та в деяких випадках можуть суперечити існуючим практикам і системам. У сфері довірчих послуг зміни в стандартах, зокрема, стосуються ділових інтересів виробників обладнання та програмного забезпечення (QSCD-Tokens, HSM - Crypto Modules, хеш-функцій та криптобібліотек).

Ідентифікація проблеми. Протягом багатьох років сфера надання загальнодержавних послуг в Україні сприймалася як найменш ефективна і однаково відокремлена від потреб громадян та нових технологій, створюючи брак довіри в суспільстві щодо цих послуг та породжуючи корупцію. Низька якість послуг була пов'язана з низькою ефективністю державних органів та незадовільним дизайном послуг. Були, однак, і численні спроби модернізації, здебільшого пов'язані з окремими міністерствами, відомствами та муніципалітетами. Проте дисфункціональність систем державних закупівель та фрагментація створили набір локалізованих ICT-систем із стандартним набором проблем: суперечливі формати даних, слабка взаємодія та інтероперабельність, вендорні та технічні блокування, неврегульованість прав інтелектуальної власності, з малою чи взагалі відсутньою взаємосумісністю цих систем.

Позитивні реформи державної служби розпочалися після Революції гідності 2014 року та з неурядової ініціативи громадянського суспільства[17], яка розробила систему державних закупівель із відкритим кодом - згодом названу "ProZorro"[18]. Система була запущена у 2015 році та швидко здобула популярність серед постачальників та навіть міжнародне визнання[19], що, серед іншого, забезпечило прогрес у подальшій розробці інформаційних систем для державного сектору та пізніше щодо довірчих послуг.

Правовий контекст. Щоб забезпечити та підтримати перехід на електронні послуги та електронні документи, парламент України у 2017 році прийняв законодавство про довірчі послуги - Закон 2155-VIII[20]. Закон в значній мірі узгоджується з Регламентом ЄС eIDAS

15) https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf

16) https://eeas.europa.eu/archives/docs/ukraine/pdf/dcfta-annexes-xvii-xx_en.pdf - AA appendixes text can (and one may argue should be) the subject of mutually agreed and beneficial renewals

17) NGO - Transparent Public Procurement - https://www.facebook.com/transparentprocurement.UA

18) https://prozorro.gov.ua/en

19) https://openprocurement.io/en/cases/prozorro

20) https://zakon.rada.gov.ua/laws/show/2155-19#Text

910[21] та відповідає принципам технологічної нейтральності. Однак, підзаконні акти, що обумовлюють практичне впровадження законодавства щодо інформаційної безпеки та довірчих послуг, можуть розглядатися як менш технологічно нейтральні й такі, що створюють подвійність у технічних стандартах. Ці положення (Постанови КМУ № 991, 992[22] та інші[23, 24]) з одного боку регламентують, що довірчі послуги та апаратно-програмні системи, що їх надають, мають відповідати стандартам Міжнародної організації зі стандартизації (МОС) та ЄІТС, а з іншого вимагають відповідність місцевим стандартам, а також проходження перевірки щодо Комплексної системи захисту інформації (КСЗІ)[25]. Остання насамперед базується на дотриманні стандарту ДСТУ 4145 (про який мова йтиме далі). Відповідно, українські кваліфіковані надавачі довірчих послуг (QTSP) та їхні послуги лише вибірково дотримуються міжнародних стандартів без визнаної ЄС чи міжнародно визнаної оцінки відповідності цих вимог та стандартів.

Зміни у зовнішніх обставинах та середовищі

1. Розвиток довірчих послуг та відповідна сфера законодавства мають свою динаміку як в Україні, так і в ЄС. Тому гармонізація, яка вимагається Додатком XVII-3 Угоди про асоціацію станом на 2014 рік, підлягає змінам після оновлення Регламенту 910 (eIDAS) ЄС, що заплановано на 2021 рік.
2. В 2021 експертна група Єврокомісії опублікувала детальні керівні принципи взаємного визнання довірчих послуг (біла книга Угоди про взаємне визнання (MRA Cookbook)[26], які включають, крім законодавчих наближень, зазначених у Додатку XVII-3 Угоди, узгодження у сфері нагляду та аудиту, найкращих практик та представництва довіри.
3. Цифрова стратегія ЄЦР[27] була сформульована через рік після підписання Угоди про асоціацію між Україною та ЄС і з 2015 року концепція ЄЦР значно розвинулась.
4. Зміни в телекомунікаційних послугах (5G), які, можливо, змінять способи і навіть сутність надання державних та довірчих послуг, також слід брати до уваги.
5. Технологічні досягнення та відповідні розробки в галузі міжнародної стандартизації (наприклад, кількість послідовних оновлень стандарту Cryptographic Suite ETSI TS 119 312, та оновлення FIPS 140-2 до FIPS 140-3 = ISO/IEC 19790).
6. Україна має низку нових та амбітних цифрових ініціатив, які ще не створили цілісної картини, сформульованої в конкретних політиках, однак, на практиці спостерігається швидкий розвиток.

21) https://www.ims-ukraine.org/sites/default/files/Evaluation of the Ukrainian Trust Services - eID legislation %28Law 2155-VIII%29%2C and related implementing decisions in view of the eIDAS EU regulation.pdf

22) https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#n458

23) https://zakon.rada.gov.ua/laws/show/z0728-18#Text НАКАЗ № 222 від 31.05.2018

24) https://zakon.rada.gov.ua/laws/show/z1039-20#n21 НАКАЗ № 140/614 30.09.2020

25) Complex System of Information Protection – applicable to hardware and software used by QTSP and public ICT systems - https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11

26) https://esignature.ec.europa.eu/intl-comp/dss-demo/downloads/MRAinfo_Cookbook_v1.0.pdf

27) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

ОГЛЯД ЧИННОЇ ПОЛІТИКИ У СФЕРІ ДОВІРЧИХ ПОСЛУГ

Політика в галузі довірчих послуг та електронної ідентифікації в Україні базується на основі Закону 2155-VIII, низки імплементаційних НПА, а також набору національних стандартів. Окрім проекту "Цифрового порядку денного - 2020", розробленого у 2016 році[28], де довірчі послуги та електронна ідентифікація згадуються три рази в загальних рисах, засади та принципи політики не представлені у формі програмних документів. Ми спробуємо реконструювати їх на основі наявних постанов, стандартів, положень, зіставляючи з політичними заявами та рекламними матеріалами, доступними з публічних джерел.

Довірчі послуги в Україні включають:

i) надання кваліфікованих сертифікатів для електронних підписів,

ii) надання кваліфікованих сертифікатів для електронних печаток,

iii) надання кваліфікованих сертифікатів для автентифікації веб-сайтів,

iv) кваліфікована служба перевірки для кваліфікованих електронних підписів,

v) кваліфікована служба перевірки кваліфікованих електронних печаток,

vi) кваліфікована служба збереження кваліфікованих електронних підписів,

vii) кваліфікована служба збереження кваліфікованих електронних печаток,

viii) надання кваліфікованих штампів часу,

ix) кваліфіковані служби електронної доставки.

28) https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf - Цифровий порядок денний України – 2020 (Draft 2016)

Електронний підпис

Концепція електронного підпису та електронних документів формувалась по аналогії з паперовими документами, власноручним підписом та мокрою печаткою. Знадобилися століття для розробки загальноприйнятих конвенцій щодо паперових документів. Електронний підпис та електронний документ мають свої концепції, технології та правила, які ще не дуже узгоджені і можуть відрізнятися в різних країнах. Тому визначення термінів, процесів та стандартів, що регулюють створення, застосування, підтвердження та збереження юридично обов'язкових електронних підписів та електронних документів, є важливим.

Типи/формати/міцність/упаковка/конверти/ та інші характеристики електронного підпису - Європейська директива про електронні підписи (1999) визначає електронний підпис як: "дані в електронній формі, які додаються до інших електронних даних або асоціюються з ними та служать методом автентифікації". Закон України № 2155-VII (2017) "Про електронні довірчі послуги", а також Європейський Регламент 910 про електронну ідентифікацію і довірчі послуги (eIDAS) (2014) визначають три типи електронних підписів: простий (ОЕП), вдосконалений (ВЕП=AdES) та кваліфікований (КЕП=QES). Вдосконалені та кваліфіковані електронні підписи найбільш захищені та для набуття юридичної сили повинні відповідати таким критеріям:

1. бути однозначно пов'язаними з підписантом;
2. мати можливість однозначної ідентифікації підписанта;

3. підпис знаходиться та використовується під постійним особистим контролем підписанта;

4. зміст документа, підписаного електронним підписом не може бути зміненим без змін у цілісності підпису.

Подальше розрізнення між вдосконаленим та кваліфікованим типом електронного підпису визначається технічною специфікацією та юридичними вимогами до надавача електронного підпису, а також способом зберігання електронного підпису, оцінкою відповідності надавача цього електронного підпису. Критичною відмінністю між AdES та QES є вимога зберігати QES на кваліфікованому пристрої для створення підпису (токені), що також передбачає використання інтерфейсу криптографічного маркера (PKCS # 11) з QcStatement (стандарт ETSI EN 319 412-5 у вимогах ЄС до електронної ідентифікації та довірчих послуг). Слід зазначити, що доволі широке визначення AdES(ВЕП), приведене в Регламенті eIDAS, залишає достатньо місця для альтернативних варіантів технічної реалізації та впровадження такого підпису. Тому в світі існують різні формати вдосконалених електронних підписів, а саме CAdES, XAdES, PAdES, які можна розуміти як різні технічні реалізації AdES(ВЕП). CAdES базується і працює з бінарними файлами CMS, XAdES відповідно з типом файлу XML та PAdES з типом файлу PDF. Крім того, існують "підформати", що беруть до уваги наявність або відсутність позначки часу накладання підпису та\або силу шифрування; відповідно розрізняють: рівень BB - без позначки часу накладання підпису, рівень BT - з позначкою часу, рівень B-LT - з технічною реалізацією довгострокового зберігання та рівень B-LTA - з технічною реалізацією довгострокового зберігання та архівним зберіганням. Існує також чимало способів упаковки та зберігання електронно підписаного цифрового документа. Набір елементів, що разом є підписаним електронним документом складається у так званий конверт електронно підписаного документа, що містить: 1) цифрові дані, що підписуються (текст, але не тільки), + 2) електронний цифровий підпис, + 3) позначку часу, + 4) результат перевірки кваліфікованого електронного підпису на час підписання (або архів списку відкликаних сертифікатів (CRL), або результати протоколу перевірки статусу онлайн-сертифіката (OCSP)). Різні способи пакування та архівування електронно підписаного електронного документа створили декілька розширень файлів - p7s, ASIC (zip) та інші. Усі ці критерії встановлені та керуються ETSI (ЄІТС)[29] або іншими локалізованими стандартами. Для України це 76 різних стандартів (додаток 2, таблиця 3, положення 991)[30].

Електронна печатка

Обмін документами між бізнесом (b2b) та бізнесом і державою (b2g) становить 95% електронного документообігу та діловодства в Україні, що потребує застосунку електронної автентифікації. Однак, з 2017 року випуск електронних печаток зменшується, що, вірогідно, пов'язано зі зняттям вимог щодо обов'язкового використання електронних печаток при податковій звітності (Наказ Міністерства фінансів України 557)[31]. Випуск нових електронних печаток зменшився на 48% у 2020 році порівняно з 2019 роком (було видано на 558 864 менше електронних печаток у порівнянні з минулим роком)[32]. Електронна печатка в Україні має ті ж технічні та стандартизовані особливості, що й електронний підпис. Зменшення видачі електронних печаток є, швидше за все, результатом вищезгаданих змін у законодавстві, а також зміни способу обробки електронної печатки державними кваліфікованими надавачами послуг податкової служби та державних банків (Приватбанк), що може вплинути на спосіб збору статистичних даних. З 2020 року електронна печатка випускається разом з електронним підписом (технічно один файл), що містить два сертифікати: електронний підпис директора компанії та електронну печатку юридичної особи.

29) ETSI Electronic Signatures and Infrastructures (ESI) — set of 200+ standards - https://www.etsi.org/committee/esi

30) https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991

31) https://zakon.rada.gov.ua/laws/show/z0959-17#Text

32) https://czo.gov.ua/development?cat=4&fromyear=2019&toyear=2020

Головні характеристики українських кваліфікованих підписів[33]

Кількість кваліфікованих надавачів довірчих послуг	21 (2021)
Формат електронного підпису в Україні	CAdES(на ДСТУ 4145) -99.9%, ECDSA -0.05%, RSA - одиниці
Кількість виданих електронних підписів	2019 – 4 283 000; 2020 - 7 274 000
Електронні підписи на QSCD (токенізоване безпечне сховище е-підпису[34])	› 11% електронних підписів (2020)
Послуги віддаленого підпису (RSS) за допомогою QSCD TYPE 2	Так (запроваджено в 2021 році PrivatBank QTSP), з від 17 травня 2021 має бути у державному додатку «Дія»
Використовувані хеш-функції	GOST/DSTU 34.311-95 - за технічними характеристиками дещо подібний до FIPS140-2[35]
Тривалість дії електронного підпису	Два роки
Архівування електронного документа	Не застосовується
Стандарти, що регулюють	до 76 внутрішніх стандартів[36] - основний ДСТУ 4145, ДСТУ 34.311-95, ДСТУ 28147, ДСТУ 7564-2014 / міжнародні - ETSI TS 119 312

NB: Із перерахованого найбільше відповідає форматам електронного підпису ЄС - XadES - ASiC з міткою часу (B-LT та B-LTA). Українське законодавство теоретично дозволяє використання цього формату[37], однак, підпису, що відповідав би таким вимогам на середину 2021 року, в Україні в вільному комерційному доступі не існує.

33) https://czo.gov.ua/development?tab=1

34) Кваліфікований пристрій генерації підписів на базі DSTU 4145 з - Криптографічний інтерфейс токена PKCS # 11

35) Federal Information Processing Standard Publication 140-2

36) https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991

37) https://zakon.rada.gov.ua/laws/show/z1039-20#n21

Хоча такий підхід може мати певне обґрунтування (предмет окремого дослідження), він також змінює бізнес-логіку застосунку електронної печатки. Обґрунтованість такого підходу наразі не може бути оцінена через відсутність політики та відомостей про бажаний кінцевий результат, в тому числі і щодо використання електронних печаток.

Політика щодо криптографічних стандартів (вітчизняні криптографічні стандарти, що регулюються Законом України № 124-VII[38], Наказом КМУ № 991[39] та 992[40]).

38) https://zakon.rada.gov.ua/laws/show/124-19#n71 -ЗАКОН УКРАЇНИ Про технічні регламенти та оцінку відповідності

39) https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991 - Про затвердження Технічного регламенту засобів криптографічного захисту інформації

40) https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#Text - Про затвердження вимог у сфері електронних довірчих послуг

Криптографічні системи та стандарти, які кодують та захищають електронний підпис та електронну ідентифікацію, також служать базовим елементом інфраструктури відкритих ключів (PKI) та інфраструктури довірчих послуг. Теоретично довірчі послуги мають бути технологічно нейтральними, проте на практиці стандарти можуть формуватися на основі конкретних криптографічних бібліотек та алгоритмів, і вони не є легко взаємозамінними. З 2001 року Закон про стандартизацію в Україні ініціював розробку набору стандартів та технологічних рішень щодо шифрування та криптографічного захисту інформації, заснованого на ECC (криптографія еліптичних кривих)[41].

41) Elliptic Curve Cryptography (ECC) -Technical Guideline BSI TR-03111 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf

З 2002 року були введені стандарти ГОСТ/ДСТУ 34.311-95[42], ДСТУ 4145 та ГОСТ/ДСТУ 28147[43], які сформували основні технічні вимоги та базовий набір технологій загальнодержавної інфраструктури відкритих ключів та кореневих сертифікатів (Root CA) - це було основним полем застосунку криптографії на той час. Де-факто це було зроблено відповідно до стандартів колишнього СРСР та Російської Федерації, поглиблюючи розбіжність українських внутрішніх стандартів із стандартами, що використовувались тоді у Європі та світі (RSA, ECDSA). Але математично ДСТУ 4145 базується на досить передовій математичній базі (криптографії еліптичних кривих), подібній до ECDSA алгоритмів. З подальшим поверненням до активного впровадженням міжнародних стандартів (ISO та ETSI) Україна сформувала подвійні стандарти щодо інформаційної безпеки і довірчих послуг, які залишаються чинними у 2021 році. Усі урядові та державно-адміністративні системи в Україні (включаючи ті, що мають відношення до надання адміністративних та довірчих послуг) відповідно до законодавства[44] зобов'язані проходити перевірку на відповідність Комплексної Системи Захисту Інформації (КСЗІ), що базується на вітчизняних стандартах (зокрема ДСТУ 4145 і ДСТУ 7564-2014 ГОСТ/ДСТУ 34.311-95, ГОСТ/ДСТУ 28147). ДСТУ 7564-2014[45] - відносно новий вітчизняний стандарт щодо хеш-функцій, що використовуються для перевірки електронних підписів, який повинен бути впроваджений з січня 2021 року. Схема оцінки криптографічних даних SOG-IS[46], яка допомагає регуляторам та розробникам криптографічних систем у ЄС та у всьому світі оцінити очікуваний термін служби безпечної (рекомендованої) та застарілої криптографії, передбачає, що криптоалгоритми можуть стати вразливими через розвиток квантових обчислень та нових підходів до розшифровки[47]. Стабільна та еластична загальнодержавна система цифрової безпеки та довірчих послуг повинна враховувати потребу швидкої міграції до новіших алгоритмів криптографії. Проте безпека - не єдине питання, яке можна вирішити за допомогою кращого застосування міжнародних стандартів. Транскордонна та навіть внутрішня сумісність/інтероперабельність довірчих послуг є більш актуальною в короткостроковій перспективі.

Політика щодо кваліфікованих пристроїв для створення підписів

Токени (QSCD). Захищений маркер електронної печатки і підпису - це портативний пристрій створення кваліфікованого підпису (QSCD в термінах eIDAS), який захищає електронну печатку і підпис відповідно до стандартів і створює єдиний контроль користувача над електронним підписом і печаткою. Кваліфікований пристрій для створення підпису передбачений Законом України про довірчі послуги 2155-VII, що встановлював перехідний період до 07.11.2020. Однак, в Україні все ще переважає використання вдосконалених електронних підписів (88% підписів це ВЕП=AdES, хоча вони і називаються QES, КЕП українською мовою). ВЕП (AdES) не відповідають критеріям єдиного контролю. Недостатнє використання токенів розуміється як тимчасовий компроміс, який спрямований на збільшення проникнення та використання електронних підписів в межах та за умовами експерименту[48].Щодо токенів (QSCD), їхнє використання в Україні підлягає: a) затвердженню Державною службою спеціального зв'язку та захисту інформації України, b) місцевій КСЗІ експертизі та відповідності національним стандартам, переліченим у таблиці 3 додатка 2 Постанови КМУ № 991[49]. Фактично, це накладає нетарифний бар'єр і зачиняє ринок

42) https://en.wikipedia.org/wiki/GOST_(hash_function)

43) https://uk.wikipedia.org/wiki/ГОСТ_28147-89

44) https://zakon.rada.gov.ua/laws/show/z0728-18#Text НАКАЗ № 222 від 31.05.2018

45) https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-7564-2014.pdf

46) https://www.sogis.eu/documents/cc/crypto/obsolete/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf

47) novel technique to modify the SHOR'S algorithm https://ieeexplore.ieee.org/document/8117822

48) https://zakon.rada.gov.ua/laws/show/193-2020-%D0%BF#Text - ПОСТАНОВА 193

49 https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991

для попередньо визначених виробників токенів QSCD до 2027 року. В Україні є чотири вітчизняних бізнес-постачальники кваліфікованих пристроїв для створення підпису та іншого обладнання та програмного забезпечення для захисту.

Служби віддаленого підпису (RSS). TYPE2 QSCD - технологічне рішення, яке зберігає кваліфіковані електронні підписи та кваліфіковані електронні печатки на сервері кваліфікованого надавача довірчих послуг (QTSP). RSS стає все більш популярним в ЄС і являє собою альтернативу токенам (QSCD). Ця технічна реалізація називається TYPE2 QSCD або RSS. Однак, сертифікація QSCD TYPE2, де QSCD управляється від імені підписувача, виходить за рамки сертифікації криптомодуля, який обробляє дані створення електронного підпису, і охоплює робоче середовище кваліфікованого постачальника довірчих послуг (QTSP). Стандарти ETSI (ЄІТС), якими керуються RSS в ЄС, знаходяться на завершальній стадії розробки. Україна вже має RSS (Smart-Id[50] від ПриватБанку запущений у 2021 році), проте технічні аспекти та відповідність технічного рішення міжнародним стандартам залишаються невідомими. Побоювання можуть бути пов'язані з модулем апаратної безпеки (HSM), що зберігає КЕП, оскільки Україна має власний набір стандартів для криптографічного обладнання, яке не у всьому співпадає з сертифікацією за Common Criteria (Загальними критеріями)[51], тому оператори RSS, скоріш за все, обмежені в апаратних опціях.

MobileID. QSCD можна вбудувати в мобільну SIM-карту, і після цього таке технічне рішення може створювати та накладати на документи кваліфікований електронний підпис, пов'язаний з мобільним телефоном та його власником. В Україні MobileID пропонують три мережеві провайдери: KyivStar, Vodafone та LifeCell. KyivStar використовує алгоритм RSA та ECDSA та частково впроваджує міжнародні стандарти; рішення Vodafone та LifeCell базуються на місцевій DSTU 4145 на основі ECC. В обох випадках MobileID формат електронного підпису - CadES. Окрім технічних труднощів, основною проблемою українського MobileID, незалежно від використовуваної технології, є неможливість його використання в цифрових застосунках податкової служби України та інших державних онлайн-сервісах (включно з «Дія»). Як результат, стандарти е-підписів RSA та ECDSA не отримали адаптацію та поширене використання.

Політика щодо інтероперабельності урядових та комунальних онлайн сервісів та застосунків

Система "Трембіта" - система взаємодії державних органів України щодо оцифрування державних послуг. Трембіта дозволяє та технічно реалізує централізоване управління та розподілення рівнем обміну даними (за допомогою API) між існуючими інформаційними системами міністерств, що забезпечують урядовій та місцевій владі можливості електронного обміну даними (EDI) у поєднанні з іншою системою СЕВ ОВВ (див. детальніше в "електронній доставці"). Проект був започаткований у 2016 році, і завдяки "коробковому рішенню" (x-road) система запрацювала в 2017 році. Розгортання системи "Трембіта" було пов'язане з реалізацією антикорупційної стратегії, яка створила відкритий онлайн-реєстр декларацій державних службовців. Система "Трембіта" підключає та відкриває тисячі баз даних та наборів даних, тим самим виконуючи один із 6 основних принципів відкритості цифрового уряду[52] і позиціонується як система інтероперабельності. Незважаючи на успіх "Трембіти", слід вжити додаткових заходів, щоб сприяти її поглибленому використанню деякими міністерствами та місцевою владою, інтеграції до Єдиних державних реєстрів[53] та застосуванню принципів управління ризиками[54] для подальшого розвитку стратегії відкриття даних.

50) https://privatbank.ua/ru/smart-id

51) https://www.commoncriteriaportal.org/products/

52) https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=P

53) https://nais.gov.ua/

54) https://en.wikipedia.org/wiki/Once-only_principle

Електронна доставка. В Україні на 1 квартал 2021 року немає кваліфікованої служби електронної доставки. Однак, існують програми для бізнесу та уряду, які здійснюють електронну доставку. Системою електронної взаємодії органів виконавчої влади (СЕВ ОВВ)[55] користуються понад 2600 юридичних осіб; вона виконує функції електронного обміну державними даними та електронними документами. Завдяки СЕВ ОВВ було затверджено формат електронних документів (ASiC) і вперше введено юридично значимий обмін електронних документів в уряді. Примітка. У 2020 році в рамках Східного партнерства EU4Digital реалізовувався пілотний проект щодо сприяння електронній торгівлі між Україною та Польщею[56] - він використовував умови електронної доставки для обміну електронними рахунками через PEPPOL[57]. Проте слід зазначити, що електронний рахунок-фактура в ЄС не є предметом електронного підпису, а PEPPOL не є кваліфікованою службою електронної доставки. Чи є наразі в Україні постійна точка доступу PEPPOL для обміну електронними рахунками-фактурами з контрагентами ЄС, як результат пілотного проекту, незрозуміло.

Додаток "Дія" - ще один загальнодержавний цифровий продукт, який було запущено на початку 2020 року. Він складається з : а) веб-порталу "Дія", б) додатку "Дія" для Android, с) додатку "Дія" для iOS, d) API "Дія". Додаток "Дія" приєднаний до Єдиних державних реєстрів України і спочатку позиціонувався як засіб централізованої цифрової комунікації між урядом та громадянами. Додаток приєднано до бази цифрових особистих документів (водійське посвідчення), які можна використовувати як замінник звичайних. Продовжується робота з підвищення рівня безпеки[58], зручності використання та розширення переліку державних послуг, документів та підключення, доступних у додатку "Дія" та через нього. "Дія"[59] має план впровадити 94 адміністративні процедури від місцевих та державних органів (робота триває). Державне підприємство, розпорядник додатку "Дії", також зареєстрований як кваліфікований надавач довірчих послуг (КНДП=QTSP) і може стати віддаленим (хмарним) сервісом зберігання (RSS) для кваліфікованого електронного підпису та е-ідентифікації/електронного паспорта. Електронний паспорт був запроваджений Законом № 1368-IX "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус" в березні 2021 року[60]. Новий Закон передбачає, що з 23 серпня 2021 року всі українські компанії та державні установи прийматимуть електронні паспорти через додаток "Дія" Міністерства цифрової трансформації. Будучи КНДП, "Дія" також може стати кваліфікованим постачальником послуг електронної доставки, що здійснює юридично значущі сповіщення g2c, g2b.

Політика щодо надавачів довірчих послуг

Надавачі довірчих послуг (TSP QTSP). Як уже згадувалося, в Україні існує змішана модель довірчих послуг, тоді як кваліфіковані довірчі послуги (QTS) можуть надаватися приватними та державними кваліфікованими надавачами довірчих послуг. Кількість КНДП (QTSP) станом на 2021 рік становить 21[61]: шість - перебувають у приватній власності, три - належать державним банкам, а решта - або державні органи, або державні підприємства. Модель ведення бізнесу щодо довірчих послуг наразі є складною, оскільки більшість (90% +) електронних підписів у 2020 році було видано державними банками, податковою службою та іншими урядовими організаціями безкоштовно. Частка видачі електронного підпису комерційним КНДП (QTSP) зменшилась з 18% до 9,5% 2019/20 рр.

55) https://dir.gov.ua/projects/sev-ovv - Система електронної взаємодії органів виконавчої влади

56) https://eufordigital.eu/eu4digital-and-edelivery-what-do-they-mean-for-digitalisation-in-ukraine/

57) https://peppol.eu/

58) Diiy Bug Bounty Program — report - https://thedigital.gov.ua/storage/uploads/files/news_post/2020/12/diya-proyshla-perevirku-bagbaunti-ta-pidtverdila-bezpechnist-zastosunku/Bounty_17-DEC-2020_DIIA.pdf

59) https://plan2.diiy.gov.ua/projects

60) https://www.kmu.gov.ua/en/news/mihajlo-fedorov-ukrayina-persha-derzhava-svitu-v-yakij-cifrovi-pasporti-u-smartfoni-stali-povnimi-yuridichnimi-analogami-zvichajnih-dokumentiv

61) https://czo.gov.ua/ca-registry

Довірчий список (ДС, = TL) є важливим елементом системи довіри і технологічним вибором країн ЄС, який замінює Root CA, створюючи більш розподілену екосистему (ІВК) PKI. Законом України № 2155-VIII "Про електронні довірчі послуги" (відповідно до Положення про eIDAS) також було введено перший національний довірчий список[62]. Його технічні характеристики регулюються постановою КМУ № 775[63] і базуються на стандартах ETSI TS 119 612 Trusted List. Український довірчий список доступний у машинно читаному форматі XML і відповідає технічним характеристикам, встановленим виконавчим рішенням Європейської комісії (EU) 2015/15053 щодо довірчих списків, встановлених у статті 22 (5) Регламенту eIDAS. Довірчий список, як зазначено в ETSI TS 119 612, дозволяє будь-якій зацікавленій стороні визначити, чи здійснюється або здійснювалась довірча послуга згідно з чинними вимогами (наприклад, на момент надання послуги або в час, коли відбулася транзакція, що залежить від цієї послуги). Вважається, що український довірчий список містить машинно читану інформацію, на основі якої можна встановити поточний та минулий статус надавача довірчих послуг (TSP) та їхніх служб QT. Оператор схеми довірчих списків - це центральний засвідчувальний орган (ЦЗО, = CCA)[64], підпорядкований Міністерству цифрової трансформації. Склад та підтримка довірчого списку є прекрасним прикладом практичних кроків, які Україна робить для створення еквівалентної Моделі представлення довіри та прогресу на шляху до реалізації угоди про взаємне визнання (УВВ = MRA), що базується на статті 14 Регламенту eIDAS.

Згідно з вимогами УВВ, Україна повинна буде створити, опублікувати та підтримувати довірчий список, що містить інформацію щодо тих надавачів довірчих послуг/довірчих послуг (TSP/TS), які можуть бути визнані юридично еквівалентними QTSP/QTS ЄС. Не зменшуючи успіх українського довірчого списку та його важливість у питаннях інтеграції до ЄС, залишаються невирішеними питання щодо: а) механізмів перевірки послуг кваліфікованого електронного підпису за міжнародними стандартами ; б) прийняття електронних підписів на основі міжнародних стандартів (ECDSA, RSA) при наданні загальнодержавних послуг, включаючи подання податкової декларації державній податковій службі в режимі онлайн та в) щодо тих питань, які безпосередньо пов'язані з використанням/не використанням Довірчого Списку, який на сьогодні, здається, використовується недостатньо та мало відомий українським вітчизняним користувачам.

NB! Представництво довіри через Довірчий Список - це інформаційний елемент системи, метою якого є створення еквівалентності між ключовими URI, що використовуються в ДС держав-членів ЄС та ДС третьої країни (потенційно Україна). Стандарт ETSI TS 119 615 пропонує процес перевірки КДП (QTS), що не походять з ЄС, але які є еквівалентними до КДП (QTS) ЄС.

Контроль та нагляд за довірчими послугами QTS/QTSP/QSCD

В Україні здійснення контролю та нагляд є складним завданням. Національний банк України (НБУ) здійснює нагляд за довірчими послугами у банківській системі (Закон України від 5 жовтня 2017 року № 2155-VIII "Про електронні довірчі послуги")[65]. Міністерство цифрової трансформації (Мінцифра)[66] та Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок)[67] здійснюють державне регулювання решти довірчих послуг (TS/QTSP/QSCD/PKI) та апаратно-програмного забезпечення. Національне агентство з акредитації (НААУ) також залучене до регулювання довірчих послуг як установа, що здійснює акредитацію органів з оцінки відповідності та стандартизації. Питання, що стосуються телекомунікацій, захисту даних, кібербезпеки або ідентифікації регулюються іншими державними органами[68].

62) https://czo.gov.ua/trustedlist

63) https://zakon.rada.gov.ua/laws/show/1068-2019-п#n40

64) https://czo.gov.ua/

65) https://zc.bank.gov.ua/

66) https://czo.gov.ua/

67) https://cip.gov.ua/en

68) https://naau.org.ua/?lang=en

Спробуємо розібрати це на прикладах: як стати кваліфікованим надавачем довірчих послуг (QTSP) - за запитом зацікавленої сторони та відповідно до вимог Закону 2155-VII, Мінцифра включає нову організацію до довірчого списку та видає сертифікат відкритого ключа (Сертифікат від ЦЗО=CCA=Root CA). Однак, на практиці від надавача також вимагають : а) щоб затвердження/ погодження регламентів роботи КНДП (QTSP) проводилось Держспецзв'язоком; б) наявності Комплексної системи захисту інформації (КСЗІ) та позитивного експертного висновку щодо такої системи; в) схвалення криптографічного обладнання, що використовується та відповідні експертні висновки. Комплект ліцензійних документів, необхідний для КНДП (QTSP), можна переглянути на веб-сайті одного з таких надавачів - Державної прикордонної служби України[69].

Політика щодо інфраструктури відкритих ключів (PKI)

Інфраструктура відкритих ключів (PKI) - це набір інструкцій, політик, обладнання, програмного забезпечення та процедур, необхідних для створення, управління, розповсюдження, використання, зберігання та скасування цифрових сертифікатів та управління шифруванням відкритих ключів. Існують різні архітектури PKI, які забезпечують надійність і стійкість до шифрування відкритим ключем, стандарт X.509[70] визначає формат PKI, який використовується найчастіше. Окрім довірчого списку, український орган (Мінцифра) також виконує функції Центрального засвідчувального органу (ЦЗО = CCA). ЦЗО - це організація, яка забезпечує додатковий рівень контролю. Ієрархічна структура PKI допомагає забезпечити наступні послуги безпеки в онлайн та цифрових комунікаціях: а) бути точкою початкової довіри - органом реєстрації (RA), що видає "самопідписний" кореневий сертифікат українського надавача КНДП(QTSP); б) ведення списку відкликаних сертифікатів (CRL) або забезпечення у інший спосіб чинності сертифікатів через Протокол статусів онлайн-сертифікатів (OCSP); с) може відігравати важливу роль в автентифікації веб-сайтів (поки що не застосовується, оскільки більшість користувачів інтернету в Україні, як і в інших місцях, використовують SSL/TLS та передають на кореневі центри сертифікації операційних систем або браузерів (Microsoft, Apple, Google, Mozilla тощо), які наразі не містять за замовчуванням національних кореневих сертифікатів.

Центральний Засвідчувальний Орган (ЦЗО = CCA = Root CA)[71], функції якого виконує Міністерство цифрової трансформації (MoDT), видає "самопідписні" сертифікати відкритих ключів і підтримує список відкликаних сертифікатів (CRL)[72].

Заява про практику сертифікації (CPS) = Сертифікат PS існують вони в Україні у форматі розпоряджень, виданих урядом через Держспецзв'язок або Мінцифру.

Політика щодо електронного ідентифікатора (eID) - український електронний ідентифікатор

Взаємозв'язок між особистими даними та механізмами автентифікації набуває все більшого значення в глобальному масштабі та актуалізується пандемією covid-19. Переважно особи, які можуть пройти автентифікацію, здійснюють електронну активність у відповідальний спосіб. Дієздатні особи/агенти можуть реалізувати свої права та обов'язки онлайн. І навпаки, неможливість або уникання ідентифікації онлайн створює простір для зловживань та шахрайства, викрадення особистих даних тощо. Стурбованість, викликана широкими можливостями стеження в інтернеті і порушенням приватності, є однією з відомих і поважних причин несприйняття громадянами зусиль держави щодо запровадження електронної ідентифікації (eID). Створене

69) https://acsk.dpsu.gov.ua/registration-examples

70) X.509 2019 - https://www.itu.int/rec/T-REC-X.509-201910-I/en - спочатку (1988) X.509 складався з трьох організацій: органу з сертифікації (CA), власника сертифіката (або суб'єкта) та Довіряючої сторони (RP). Центр сертифікації виконує роль довіреної третьої сторони між власником сертифіката та РП. У багатьох випадках використання ця модель довіри працювала успішно.

71) https://czo.gov.ua/about - Central Certificate Authority CCA

72) https://czo.gov.ua/crls

в Україні середовище та передумови для впровадження ширшої електронної ідентифікації сильно розвинулось протягом останнього десятиліття. Україна має 21 кваліфікованого надавача електронних довірчих послуг (QTSP), які мають право видавати електронний кваліфікований підпис і які вже видали понад 7 мільйонів електронних підписів. Крім електронного підпису (AdES + QESig), українці мають альтернативний спосіб електронної ідентифікації - BankID[73]. BankID підтримується 35 банками і використовується для захисту онлайн-входів на банківські рахунки та підтвердження дій в інтернеті. Зазначимо, що BankID не можна використовувати для підписання електронних документів. Україна - далеко не перша країна, де уряд намагається реалізувати масштабну програму надання громадянам цифрового електронного ідентифікатора для використання в онлайн-послугах електронного уряду. Моделі формування Довіри (TM) та Управління цифровими ідентифікаційними даними (DIM) використовуються для формування політики електронного ідентифікатора (eID), яка враховує потреби збереження приватності при онлайн автентифікації, контролю доступу, конфіденційності та зменшення цифрового сліду, що виникає як наслідок використання електронних ідентифікаторів (eID). Авторам невідомо про політики електронних ідентифікаторів, ані TM, ані DIM, чи пов'язані з ними дослідження, моделювання щодо Української концепції eID, проте в Україні існує новий Закон про електронний паспорт. Нова редакція Закону України № 5492-VI "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус"[74] передбачає, що з 23 серпня 2021 року всі українські компанії та державні установи прийматимуть електронні паспорти у додатку «Дія». Було б цікаво дізнатись, як будуть отримані нові можливості, і яким чином Закон 5492-VI дотримуватиметься логіки загального регламенту захисту даних ЄС (GDPR EU), забезпечуючи при цьому цифрові державні послуги, з точки зору технології див. більше в розділі Аналіз доступних альтернатив, альтернативи в електронній ідентифікації(eID).

73) https://bank.gov.ua/en/bank-id-nbu Bank ID

74) https://zakon.rada.gov.ua/laws/show/5492-17#n3

Політика щодо архівування електронного документа (довгострокове збереження даних)

Загалом, архівна справа в Україні регулюється Законом 1993 року про архіви 3814-XII[75]. Вимоги щодо створення, обробки та архівування електронних документів для бізнесу, банківських, державних, адміністративних та інших електронних документів встановлені двома Положеннями Міністерства юстиції а) № 578/5[76] від 12.04.2012 та б) № 1886/5[77] від 11.11.2014, які містять досить вичерпні інструкції щодо уніфікації та передачі інформації в електронному форматі. Подальшим розвитком цього напряму став Наказ Державного агентства з електронного урядування № 60[78] від 07.09.2018 р., що встановлює ASiC як формат для електронних документів та Проект Стратегії розвитку архівної справи до 2025 р.,[79] що є візіонерським документом, який має закріпити прогрес в архівній справі. Зазначимо, що з технічної точки зору практики щодо архівування електронних документів, передбаченого у Стратегії, можуть бути вдосконалені та опрацьовані більш докладно. Автори розуміють, що розвиток архівної справи ускладнюється недостатнім технічним забезпеченням Національного архіву України та місцевих архівів. Хоча є й позитивний приклад - Банківський архів, який веде Національний банк України (НБУ). З 2016 року НБУ застосовує процедури електронного архівування, включаючи процедури електронних документів з КЕП та довгострокової перевірки (LTV).

75) https://zakon.rada.gov.ua/laws/show/3814-12#Text

76) https://zakon.rada.gov.ua/laws/show/z0571-12#Text

77) https://zakon.rada.gov.ua/laws/show/z1421-14#Text

78) https://zakon.rada.gov.ua/laws/show/z1309-18#n17

79) https://archives.gov.ua/wp-content/uploads/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8F-%D1%80%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BA%D1%83-%D0%B0%D1%80%D1%85%D1%96%D0%B2%D0%BD%D0%BE%D1%97-%D1%81%D0%BF%D1%80%D0%B0%D0%B2%D0%B8.pdf

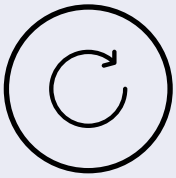
Розвиток довірчих послуг - кількісні показники

Спектр довірчих послуг в Україні демонструє різні рівні зрілості, розвитку та застосунку щодо надання державних послуг, внутрішньоурядового документообігу та використання у бізнес-середовищі. Електронний підпис є найбільш поширеною довірчою послугою з 7,2 мільйонами дійсних електронних підписів (AdES + QESig) станом на 2020 рік[80], що на 69% більше, ніж у 2019 році (4,3 мільйона). Українці все більше використовують електронні підписи у взаємодіях з державою та між бізнесами (c2g, g2b, b2g та b2b). Також зростає кількість відміток часу, що побічно вказує на кількість підписаних електронних документів (3 922 809 328 відміток часу в 2020 році порівняно з 1 670 258 087 в 2019 році); Це дає 39% річного зростання використання електронних підписів. Це позитивна тенденція, яка свідчить про те, що користування цифровими послугами громадянами та бізнесом в Україні переживає період стрімкого зростання[81].

80) https://czo.gov.ua/development?cat=1&fromyear=2019&toyear=2020

81) https://czo.gov.ua/development?cat=1&fromyear=2019&toyear=2020

ЗМІНИ В СЕРЕДОВИЩІ, ЯКІ ВІДБУВАЮТЬСЯ ТА ВПЛИВАЮТЬ НА РОЗВИТОК ДОВІРЧИХ ПОСЛУГ В УКРАЇНІ



- Український уряд зацікавлений у встановленні взаємного визнання довірчих послуг з ЄС. Коли такий запит був зроблений в 2019 році, з боку ЄС не існувало чітких рекомендацій щодо його досягнення. На початку 2021 року рекомендації про взаємне визнання (MRA) були опубліковані, і відповідно, більш зрозумілим став шлях та конкретні кроки щодо досягнення взаємного визнання (MRA).

- Законодавство з регулювання довірчих послуг та електронної ідентифікації вимагає змін у зв'язку з реформуванням громадських сервісів та діджиталізацією державних процедур. Особливо щодо реформування сфер нагляду та аудиту, наближення до найкращих практик, механізмів забезпечення довіри.

- Вдосконалення механізмів сертифікації, формування Органу з Оцінки Відповідності (CAB) у сфері захисту інформації та довірчих послуг, що особливо актуально у зв'язку з закінченням перехідного періоду.

- Зміни технічних стандартів, пов'язані з розвитком дистанційної ідентифікації, форматами КЕП, QSCD тощо.

- Зміни у підходах та наближення до норм ЄС у галузях: а) обробки персональних даних, б) оцінки відповідності та дотримання вимог стандартів та законодавства, в) управління та розпорядження даними цифрової ідентифікації.

- Зростання уваги громадян до проблем забезпечення конфіденційності та маскування цифрового сліду при розширеному застосунку eID.

- Зміни та розвиток стандартів щодо доступності/інклюзивності у інформаційно-комунікаційних системах державних послуг для людей з обмеженими можливостями в ЄС (EN 301 549).

АНАЛІЗ ДОСТУПНИХ АЛЬТЕРНАТИВ

Сучасні цифрові інформаційно-комунікаційні технології базуються на здатності інтернету об'єднувати дані, ресурси та людей таким чином, як це ніколи раніше не було можливо; у суспільному житті це може бути як цінним, так і шкідливим. Протягом чотирьох десятиліть уряди та бізнес у всьому світі будують електронну та цифрову інфраструктуру, розробляють концепції та впроваджують системи електронного обміну даними (EDI), цифрової ідентифікації та довірчих послуг щодо використання інтернету у цифровій ідентифікації та отримання послуг та інформації. Розглянемо наявні варіанти та підходи.

Бізнес-моделі надання довірчих послуг:

- Централізована, з провідною роллю державного сектору/уряду.
- Федеральна, з провідною роллю комерційного сектору.
- Змішана модель (коли і державний, і комерційний сектори співпрацюють та конкурують).

Україна на даний момент використовує змішану модель надання довірчих послуг з домінуванням уряду та державних кваліфікованих надавачів довірчих послуг (найбільший провайдер довірчих послуг - це державний банк "Приватбанк", з часткою ринку 70% у 2020 році). В сегменті апаратного та програмного обладнання, що використовується для надання довірчих послуг, працюють четверо приватних постачальників.

Альтернативи в обладнанні апаратного захисту та стандартизації кваліфікованих пристроїв для створення підпису (QSCD)

Ця сфера майже не має альтернативних підходів, і навіть великі економіки (США, ЄС та Японія) уніфіковують підходи до стандартизації апаратного захисту. Недотримання стандартів безпеки Common Criteria Evaluation Assurance Level (EAL) у цій сфері створює ризики (в тому числі в сферах національної безпеки та оборони). Використання автономної та ізольованої екосистеми апаратного та програмного забезпечення та криптографії може бути значним викликом. Такий підхід може бути нежиттєздатним у довгостроковій перспективі та перешкоджає інтеграції України та ЄС.

Оцінка відповідності кваліфікованих надавачів довірчих послуг (QTSP)

Застосування підходу оцінки відповідності українських QTSP органом з оцінки відповідності у сфері довірчих послуг та інформаційної безпеки має певні перешкоди, але може бути реалізовано в довгостроковій перспективі.

Для оперативного вирішення питання оцінки відповідності українських QTSP доцільно дозволити оцінку відповідності української QTSP європейськими органами з оцінки відповідності у сфері довірчих послуг (CAB), принаймні, для транскордонних довірчих служб і до тих пір, поки не буде сформовано вітчизняний CAB.

Враховуючи євроінтеграційні прагнення України, доцільно розвивати підхід, за якого український орган оцінки відповідності буде відповідати тим же вимогам, що і європейський.

Альтернативи в електроній ідентифікації (eID)

Електронна ідентифікація (eID) - це процес використання даних осіб в електронній формі для унікальної верифікації фізичної/юридичної особи, або навіть пристрою. На даний момент Україна має дві основні схеми електронного ідентифікаційного ідентифікатора: електронний підпис (AdES + QESig) та BankID. Однак, за відсутності програмних документів щодо eID, обмежимось переліком відомих та поширених варіантів eID:

- Федеративні схеми eID;
- Схеми самопідтверджених ідентифікаторів (SelfServing eID);
- Поліморфні схеми eID;
- Схеми електронних ідентифікаторів на основі атрибутів;
- Централізовані схеми електронних ідентифікаторів;
- Схеми електронної ідентифікації на основі біометрії.

Сфера електронної ідентифікації (eID) та управління цифровими посвідченнями є динамічною. Кожна із згаданих вище схем eID може використовуватися в поєднанні з іншими та мати технічні деталі, які виходять за межі даного огляду.

Огляд можливих сценаріїв

Розглянемо три основні сценарії - базовий, прогресивний, та негативний - у двох вимірах: внутрішньому та в контексті євроінтеграції. Оскільки Україна на конституційному рівні заявила про свої євроінтеграційні наміри, то ми розглядатимемо сценарії, що передбачають імплементацію європейських підходів, приділяючи менше уваги катастрофічним варіантам.

Базовий. Україна зберігає існуючу динаміку євроінтеграції, вибірково приймаючи норми, стандарти та практики ЄС із затримкою та модифікаціями у 3-5 років. Українська інфраструктура відкритих ключів (PKI) та довірчих послуг продовжує базуватись на місцевих стандартах, а передові міжнародні технології для застосунку на внутрішньому ринку вимагатимуть відповідності цим стандартам. Уряд проводить політику поступового оцифрування вже створених державних послуг та сервісів, застосовуючи інтернет-технології, та за допомогою розгортання централізованого мобільного додатку «Дія». Уряд відіграє головну роль у розробці та у впровадженні довірчих та державних електронних послуг, способах їх доставки та засобах управління цифровими ідентифікаційними послугами (eID) з меншою увагою до захисту персональних даних та маскування цифрового сліду. Угода про взаємне визнання (MRA) довірчих послуг між ЄС та Україною може бути укладена протягом 4-6 років, залежно від зрілості української інфраструктури довірчих послуг, відповідності нагляду та зближення стандартів. Торгові вигоди, отримані в результаті MRA та DSM, реалізовуватимуться поступово, залежно від технологічної та операційної сумісності та потреб бізнесу.

Прогресивний. Україна та ЄС послідовно прискорюють інтеграцію, тоді як український уряд, громадянське суспільство та бізнес розвиваються та беруть активну участь у цифровій трансформації вітчизняних установ. Україна розвиває міжнародні компетенції у сфері оцінки відповідності довірчих послуг. Вітчизняний орган оцінки відповідності (CAB) працює як європейські CABs. Моделі довірчих послуг та захисту даних узгоджені та впроваджені. Українське обладнання апаратного захисту та криптографічне програмне забезпечення відповідають спільним критеріям оціночного рівня довіри (Evaluation Assurance Level (EAL) by Common Criteria). Українські довірчі послуги наближаються до європейських за стандартами та надійністю, відповідають оновленому Регламенту ЄС 910/2014 (eIDAS) на семантичному, юридичному, адміністративному та технологічному рівнях. Український уряд реалізує наступні принципи цифрової трансформації: a) цифровий дизайн, b) керування даними, c) відкритість для перегляду та перевірки, d) керованість користувачами. Взаємне визнання довірчих послуг між ЄС та Україною відбувається протягом 1-3 років, можливо, з

попереднім взаємним визнанням довірчих послуг між Україною та однією з країн Східного партнерства (Молдова, Грузія). Процес взаємного визнання (MRA) та вступ до Єдиного цифрового ринку (DSM) ЄС, підтримується пілотними проектами та схемами сприяння, призводить до динамічного зростання торгівлі та інвестицій, створюючи умови для взаємнобажаної подальшої інтеграції.

Негативний. Україна та ЄС гальмують співпрацю. Український уряд, незважаючи на заявлені наміри здійснити цифрову трансформацію та побудувати цифровий уряд (як визначено ОЕСР[82]), зазнає невдачі. Невдачу можна визначити як систематичне ігнорування або нездатність впроваджувати та підтримувати міжнародні та європейські стандарти в галузі інформаційно-комунікаційних технологій, електронної ідентифікації, телекомунікаційних послуг та довірчих послуг. Систематичні та грубі порушення щодо захисту даних пов'язані з наданням довірчих послуг. Якщо систематичні порушення захисту персональних даних будуть мати місце, це ймовірно призведе до знецінення суспільної довіри до цифрових інструментів, електронних послуг, та залишить обмін документами на паперовій основі, навіть за наявності і зручності використання електронних документів та послуг. Запроваджені урядом цифрові інструменти (додаток «Дія», eID) матимуть низький чи недостатній рівень адаптації та використання, а в громадян може виникнути недовіра до електронних та довірчих послуг в цілому. Довірчі послуги лише вибірково відповідають міжнародним та європейським стандартам. Вищезазначене формує низький рівень довіри та суперечить міжнародній практиці. Взаємне визнання довірчих послуг між ЄС та Україною за такого сценарію навряд чи відбудеться, оскільки потенційні економічні вигоди від MPA не можуть бути реалізовані, якщо вони становитимуть ризик для країн ЄС.

82) https://www.oecd-ilibrary.org/governance/the-oecd-digital-government-policy-framework_f64fed2a-en 'The OECD Digital Government Policy Framework'.

ВІЗІЯ АВТОРІВ ДОСЛІДЖЕННЯ

Прагнення досягти швидкого прогресу у розвитку довірчих послуг та електронної ідентифікації з боку українського уряду повинно бути посилене системними підходами у стратегічному плануванні, стандартизації, оцінці відповідності, захисті даних та конфіденційності, відповідно до спільних політик ЄС та базуватись на міжнародних та європейських стандартах. Додаткова увага необхідна для зменшення ризиків системних технологічних вразливостей та ризиків зниження довіри населення до цифрових послуг та електронної ідентифікації.

Український прогрес в діджиталізації маловідомий на міжнародному рівні та навіть в ЄС, Міжнародний Індекс цифрової економіки та суспільства (I-DESI)[83] не включає Україну, тоді як Цифровий інформаційний бюлетень ЄС (I-DESI)[84] вперше включив Україну в 2019 році, але тільки в інформаційному форматі. Перелічимо вже досягнутий прогрес: а) Семантика та архітектура українських довірчих послуг подібна до загальноєвропейської; б) Бізнес-модель надання довірчих послуг є змішаною, що передбачає залучення як державного, так і приватного сектору; в) Уряд обізнаний з основними принципами цифрової трансформації та розуміє ключову роль телекомунікаційних та довірчих послуг у новій парадигмі; г) Закон про довірчі послуги в цілому відповідає вимогам Регламенту ЄС 910/2014; д) В Україні існує внутрішня система нагляду та контролю за наданням кваліфікованих довірчих послуг, яка може стати гарною відправною точкою для розробки вітчизняних органів з оцінки відповідності; е) Україна має реєстр електронних ключів, що узгоджується з європейською моделлю формування довірчих послуг; є) Швидко зростає використання електронних підписів та електронних документів у b2g та c2g у 2019 та 2020 роках; ж) Було здійснено кілька успішних розгортань загальнонаціональних систем (Trembita, СЕВ ОВВ, «Дія»); з) Очікується, що позитивна тенденція буде продовжуватися, оскільки розгортаються нові проекти (ініціюється електронний паспорт/eID, Єдиний державний реєстр/віддалений сервіс зберігання електронного підпису (RSS)).

Щоб зберегти досягнуте та забезпечити подальшу євроінтеграцію зі зменшенням ризиків, слід зробити наступне: а) усунути існуючі розбіжності між ЄС та Україною щодо стандартів, що регулюють застосунок криптографії та шифрувального обладнання, які використовуються при наданні довірчих послуг; б) усунути недоліки в аудиті та нагляді довірчих послуг, а саме відсутність оцінки відповідності кваліфікованих постачальників довірчих послуг (QTSP) міжнародно визнаними органами з оцінки відповідності (CAB); в) привести існуючу систему нагляду за кваліфікованими надавачами довірчих послуг (QTSP) та кваліфікованими довірчими послугами (QTS) у відповідність міжнародним стандартам; г) змінити підходи до оцінки відповідності обладнання внутрішньої безпеки (Tokens/QSCD, HSM; вони мали б оцінюватись компетентними та незалежними ліцензованими лабораторіями для визначення відповідності вимогам інформаційної безпеки та/або вже запровадженим на національному рівні ДСТУ / ISO 15408, ДСТУ ISO 18045, ДСТУ EN 419 211, ДСТУ ISO / IEC 19790, ДСТУ ISO / IEC 19896-2); д) змінити підходи щодо широкого використання продуктів безпеки (апаратних та програмних) без міжнародно визнаних процедур тестування (Evaluation Assurance Level (EAL) by Common Criteria).

Дефіцит ресурсів у поєднанні з бажанням швидких перемог та/або протекціонізмом може призвести до використання стратегій високого ризику. Це підвищує ймовірність негативного сценарію (див. попередній розділ).

83) https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies

84) https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Ukraine_2019_0.pdf

БАЧЕННЯ БАЖАНОГО РЕЗУЛЬТАТУ

1. Розробляються та імплементуються стратегії/технічні документи з Моделями Захисту Даних та Моделями Формування Довіри.
2. Оцінка відповідності українського кваліфікованого надавача довірчих послуг (QTSP) проводиться відповідно до міжнародних стандартів вітчизняними та іншими європейськими органами оцінки відповідності (CAB).
3. Українське обладнання для безпеки та криптографії, що використовується кваліфікованими надавачами довірчих послуг (QTSP), отримує рівень оцінки (EAL) за Common Criteria.
4. Внутрішня та транскордонна перевірка електронної печатки та електронного підпису виконується відповідно до стандартів ЄС (ETSI).
5. Українські оператори та розробники програмного забезпечення для довірчих послуг починають використовувати бібліотеки з відкритим кодом включно з DSS.
6. Українська довірча інфраструктура, QTSP, QSCD, RSS відповідає вимогам та отримує визнання в ЄС.
7. Угода про взаємне визнання (MRA) щодо довірчих послуг, телекомунікацій та електронної комерції з ЄС укладена впродовж наступних 2 років (до кінця 2023).
8. Архівування електронних документів технічно та організаційно можливе та проводиться по всій країні, з дотриманням стратегії та стандартів.
9. ICT системи, що впроваджуються в Україні, відповідають Європейським директивам про веб-доступність\ інклюзивність та стандарту ETSI 301 549.

РЕКОМЕНДАЦІЇ ЩОДО НЕОБХІДНИХ ДІЙ

1. Розробка програми, що формулює бачення та політику щодо деталей реалізації цифрової трансформації, особливо щодо довірчих послуг та електронної ідентифікації.

Пояснення: Відсутність чітко сформульованої політики створює з одного боку свободу дій, а з іншого веде до непередбачуваності результату, зниження стандартів, збільшує ризики та перешкоджає залученню у процес цифрової трансформації. Конституційно визначений вектор євроінтеграційного розвитку України полегшує створення такої програми, завдяки можливості використовувати дослідження та досвід ЄС (в тому числі і негативний) через вже існуючі дослідження. Електронний уряд передбачає використання ICT систем, зокрема інтернету, для реалізації державних послуг, однак, досліджено та відомо, що це мало впливає на робочі процеси надання послуг, а також не трансформує послуги у цифрові за дизайном. На відміну від такого підходу цифровий уряд розуміється як "використання цифрових технологій як інтегрованої частини стратегій модернізації урядів для створення суспільної цінності" (визначення з дослідження OECD 2020[85]), що також описує шість характеристик політики цифрового уряду: 1) цифровий за дизайном, 2) розвиток керований даними, 3) уряд як платформа (в IT-розумінні), 4) базово відкритий, 5) зміни керовані користувачами, 6) проактивний.

У контексті довірчих послуг це може означати, що уряд працює як постачальник послуг в конкурентному бізнес-середовищі. Певна ступінь конкуренції є ключем до підвищення якості та еволюційного розвитку довірчих послуг. Це має застосунок до послуг електронного підпису, токенів QSCD, мобайл ID, та RSS (служб віддаленого управління та накладання електронного підпису) і допомагає поліпшити якість, одночасно стримуючи вартість послуг.

Дії: Розробити програмні документи щодо цифрового уряду, довірчих послуг, електронної ідентифікації, захисту даних, електронного архівування, доступності/інклюзивності систем надання державних послуг онлайн, інших галузей освіти (здобуття цифрових навичок), телекомунікацій (мережа 5G, IoT), наукових досліджень та розробок; докласти зусиль для включення України до міжнародних та європейських індексів оцінки цифрового розвитку (I-DESI) та інших індексів.

2. Розробити моделі довірчих послуг + модель захисту даних + цифрові моделі управління ідентифікацією

Пояснення: Продукти (державні послуги, електронна ідентифікація, довірчі послуги) є результатами процесів. Продукти і процеси вимагають бачення, ресурсів, стандартів та участі зацікавлених сторін. Моделювання допомагає зрозуміти та інколи передбачити взаємодію в складних системах, а також покращує розуміння залучених держслужбовців, що може бути корисним у подальшій розробці програм та стратегій. У контексті довірчих послуг та захисту даних, відчувається потреба у підвищенні обізнаності та, можливо, в адаптації концепцій: маскування цифрового сліду, незалежної ідентифікації (SSI), різних шляхів забезпечення онлайн-псевдонімності користувачів тощо.

Дії: Розробити моделі довірчих послуг та захисту даних, включивши їх до програм розвитку.

85) https://bit.ly/3cBBLo2

3. Оцінка відповідності українських надавачів довірчих послуг (QTSP) згідно з міжнародними та європейськими стандартами

Пояснення: Зараз всі українські кваліфіковані надавачі довірчих послуг (QTSP) працюють з місцевою (без міжнародно визнаної) оцінкою відповідності. Така ситуація створює ризики для якості кваліфікованих довірчих послуг (QTS) та не відповідає законодавству та вимогам щодо взаємного визнання довірчих послуг з ЄС. Є кілька способів вирішити цю проблему. Швидкий шлях вирішення цих ускладнень - дозволити оцінку відповідності українських надавачів довірчих послуг (QTSP), в тому числі і органами з оцінки відповідності (CAB) країн ЄС. В довгостроковій перспективі Україна має створити вітчизняний орган з оцінки відповідності, який підпадає під дію стандартів ISO/IEC 1701, ISO/IEC 17065, EN 319 403 згідно з правил Європейської кооперації з питань акредитації та IAF. Додаткове ускладнення пов'язане з тим, що Українське Агентство з Акредитації (НААУ) не пройшло експертну перевірку; після цього статус підписанта НААУ BLA було призупинено з 24 березня 2021 р[86]. Це, серед інших факторів, впливає і на спроможність створити вітчизняний орган оцінки відповідності (CAB) щодо оцінки надавачів довірчих послуг, що відповідає вимогам ЄС MRA. У довгостроковій перспективі бажаним кінцевим результатом буде внутрішній орган з оцінки відповідності (CAB) та доступ інших європейських CAB до оцінки відповідності українських надавачів QTSP та QTS на конкурентних, але не обмежених законодавством засадах.

Дії: Поновити статус підписанта НААУ BLA (нова повторна оцінка, що відбудеться у травні 2023); змінити чинне законодавство щодо оцінки відповідності українських надавачів довірчих послуг (QTSP), в тому числі і європейськими органами оцінки відповідності (CABs ЄС), що зменшить ризики невідповідності.

4. Виправити розбіжності стандартизації в рамках QTS, QTSP, RSS та оцінки відповідності (CAB)

Пояснення: Україна вже йде шляхом країн-членів ЄС у впровадженні довірчих послуг, а отже може отримати перевагу від досвіду, вже створених найкращих практик та проведених досліджень[87], під час першої хвилі впровадження Регламенту ЄС 910/2014 (eIDAS) в ЄС (2015-2018). Основними перешкодами для подальшого розвитку ринку довірчих послуг в опитуванні ЄС-2017 були визначені прогалини в стандартизації. Такі висновки були зроблені як наглядовими органами, так і органами з оцінки відповідності (80% та 86% відповідно). Стандартизація була визнана головним питанням. Саме тому Європейська комісія та наглядові органи довірчих послуг сформували наступу відповідь: а) переглянути стандарти[88]; б) розширити мандат на стандартизацію M-460, в) виділити ресурси; г) почати підготовку до оновлення регулювання Регламенту ЄС 910/2014 (eIDAD), яке, ймовірно, вже в 2021 запровадить покращені стандарти для AdTS, QTS, QTSP, а також до оцінки відповідності з боку CAB щодо процедур та обладнання, що використовується для QTS[89].

На відміну від ЄС Україна приділяє суттєво менше уваги та ресурсів для вдосконалення стандартизації, як наслідок, рівень міжнародного визнання українських Органів Стандартизації (НААУ) був знижений через невдалий аудит. Це залишає Україні менше можливостей та перешкоджає євроінтеграційним зусиллям. Тоді як задоволення вимог щодо взаємного визнання довірчих послуг (MRA), крім очевидних переваг у спрощенні торгівлі, також може бути корисним для зміцнення надійності українських довірчих послуг, та за певних умов навіть суттєвого збільшення експорту обладнання та технологій у цій сфері. Стандарти, що потребують уваги: ETSI TR 103 684, ETSI TS 119 101, ETSI TS 119 102-1, ETSI TS

86) https://op.europa.eu/s/oTON

87) https://op.europa.eu/s/oTON

88) https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas-i

89) https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020

119 102-2, ETSI EN 319 132, ETSI EN 319 142, ETSI EN 319 162. Стандарти, щодо оцінки CAB ISO/IEC 1701, ISO/IEC 17065, EN 319 403. Стандарти, що розробляються чи змінюються: ETSI EN 319 411-2, ETSI TS 119 432, ETSI 419 241-2, ETSI TR 103 684, ETSI TR 119 460. Внутрішні українські стандарти щодо безпековажливого обладнання (QSCD HSM): DSTU / ISO 15408, DSTU ISO 18045, DSTU EN 419 211, DSTU ISO/IEC 19790, DSTU ISO/IEC 19896-2, які перешкоджають чи не сприяють покращенню якості та отримують міжнародних EAL від Common Criteria (важливо в тому числі і для розвитку військових застосунків).

Дії: Усунення недоліків у стандартизації щодо QTS, QTSP, RSS, QSCD, HSM та оцінки відповідності (CAB) шляхом перегляду та оновлення вищезазначених стандартів. Надання дозволу CAB ЄС брати участь в оцінці відповідності українських надавачів довірчих послуг QTSP. Запровадження міжнародних Загальних Критеріїв (Common Criteria) Оцінки Рівня Відповідності (ELA)[90] для апаратного обладнання, що використовується під час шифрування, забезпечення інфраструктури PKI та надання довірчих послуг

5. Архівування електронних документів (довгострокове збереження даних)

Пояснення: Документи на паперовій основі в державному та бізнес-діловодстві упродовж наступних 10 років будуть повністю замінені електронними. Отже, виникає нагальна потреба в зберіганні та архівуванні таких електронних документів з атрибутами електронних підписів, печаток, міток часу тощо. Архівування також ще довгий час матиме справу з потребою оцифрування документів на паперових носіях, та одночасно буде створювати нові процеси архівування електронних документів. Щоб узгодити ці робочі процеси, архівам необхідно покращити підготовку та технологічне оснащення, а це потребуватиме співпраці та додаткових ресурсів для: а) збереження електронного документа - найочевиднішої функції, яка потрібна для архівування; б) забезпечення доступу до електронних документів; в) збереження цілісності та доступності електронного документа. Остання функція у технологічному сенсі є найвибагливішою, тому що архівування електронних документів з атрибутами, які забезпечують цілісність, задача відмінна від забезпечення резервного копіювання такого документа. Це доволі складні технологічні питання, які враховують криптографічну стійкість архівованих електронних документів з урахуванням швидкого технологічного розвитку. Країни-члени ЄС стикаються і вирішують подібні проблеми в архівній справі, як і Україна.

Дії: Доповнити розроблену Національну Архівну Стратегію України баченням довгострокового збереження електронних документів (LTP), організувати системне та фахове вивчення досвіду країн-членів ЄС щодо архівів - проводити підвищення кваліфікації працівників архівів щодо роботи з архівуванням електронних документів.

6. Доступність електронних та онлайн систем надання державних послуг та реалізації інших служб та функцій з урахуванням потреб та можливостей людей з інвалідністю (включаючи, але не обмежуючись довірчими послугами)

Пояснення: Потреба в дотриманні вимог щодо доступності надання державних послуг для людей з інвалідністю вже добре розуміється в українському суспільстві[91]. Але у відносно новій сфері електронних та онлайн-послуг не було запроваджено стандартів, що регулюють вимоги доступності державних та муніципальних систем, наприклад, як це визначено в Європейській директиві про веб-доступність (Директива 2016/2102).

Дія: Прийняти та розпочати впровадження стандарту EN 301 549 - Вимоги щодо доступності продуктів та послуг електронних державних та муніципальних інформаційно-комунікаційних систем. Оновити законодавчу базу, включивши Європейську директиву про веб-доступність.

90) https://www.commoncriteriaportal.org/ccra/index.cfm

91) https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.01.01_60/en_301549v030101p.pdf -EN 301 549 -Accessibility requirements for ICT products and services

ОГЛЯД РИЗИКІВ

Короткий перелік ризиків, які можуть перешкоджати розвитку та взаємному визнанню довірчих послуг між Україною та ЄС:

- Відокремлений розвиток українських технологій щодо довірчих послуг та електронних ідентифікаторів (eID) в результаті самоізоляції від міжнародних стандартів.
- Невідповідність українських стандартів (а як наслідок - продуктів та процесів) щодо довірчих послуг та електронних ідентифікаторів (eID), побудова систем та технологічних рішень, несумісних із вимогами ЄС.
- Втрата громадської довіри до цифрових інструментів, що може призвести до низького рівня адаптації\використання технологій громадянами, бізнесами та державними установами.
- Недотримання національного законодавства та законодавства ЄС при оцінці відповідності вітчизняних надавачів QTSP.
- Відсутність та можлива невідповідність новоствореного органу з оцінки відповідності (CAB) в галузі інформаційної безпеки.
- Невідповідність розробленої схеми управління електронними ідентифікаторами (eID) Загальному регламенту ЄС про захист даних (GDPR).
- Ризики, пов'язані з тим, що новостворені системи електронної ідентифікації (eID) та пов'язані з ними довірчі послуги, виходячи з дизайну, будуть не здатні забезпечити маскування цифрового сліду користувачів.
- Монополізація та обмеження торгівлі на внутрішньому ринку пристроїв криптографічного захисту та накладання електронних підписів (QSCD) та інших засобів системного забезпечення мережевої безпеки довірчих послуг.
- Нестача цифрових навичок для надання та користування цифровими послугами (серед державних службовців та громадян).
- Виключення з цифрової трансформації деяких груп суспільства (літні люди, люди з інвалідністю, мешканці сільської місцевості, малі бізнеси, мігранти, інші групи, у яких бракує відповідних цифрових навичок або які гостріше відчувають обмеження в правах щодо захисту персональних даних).
- Неархівування (або хибне архівування) електронних документів, які вимагали тривалого збереження даних.

Дефіцит ресурсів у поєднанні з бажанням швидких помітних досягнень та/або протекціонізмом може призводити до надмірного використання стратегій високого ризику. Це підвищує ймовірність негативного сценарію розвитку щодо довірчих послуг да діджиталізації.

ОЧІКУВАНИЙ ДОВГОСТРОКОВИЙ ВПЛИВ

Бажаний довгостроковий вплив у разі впровадження запропонованих змін міг би виглядати наступним чином:

1. Український уряд, громадяни та бізнес беруть активну участь у проектах цифрової трансформації.
2. Електронні ідентифікатори (eID), е-підпис та електронні документи набувають широкої адаптації протягом найближчих п'яти років і стають основними (90% +) до 2030 р.
3. Менші ризики та кращі шанси на успішне цифрове перетворення, коли державні послуги стають цифровими за дизайном, керуються даними, відкриті та надійні, та сформовані навколо вимог користувачів.
4. Оцінка відповідності всіх елементів української системи надання довірчих послуг (QTSP+QSCD+CAB) проводиться відповідно до міжнародних стандартів вітчизняними та іншими європейськими CAB.
5. Взаємне визнання довірчих послуг між ЄС та Україною відбувається протягом 1-3 років; MRA спирається на основу правової технічної та організаційної взаємодії, впровадження та обмін найкращими практиками, прозорий нагляд та міжнародний аудит, з взаємовизнаним представництвом довіри.
6. Україна набуває режиму внутрішнього ринку ЄС у сфері довірчих послуг, телекомунікацій та електронної комерції. Це створює взаємні економічні вигоди та додає до 12% ВВП України (кращі послуги довіри, краща відповідність ЄС)92.
7. Цифрова трансформація уряду та державних служб працює як рушій реалізації концепцій Industry 4.093 та Society 5.094. Цифрові екосистеми в Україні слугують зразком і позитивним прикладом для наслідування іншими країнами регіону.

92) http://ucep.org.ua/wp-content/uploads/2021/02/dig_ukraine_eu_ENG-_2_WEB.pdf

93) https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf

94) https://www.jica.go.jp/activities/issues/ict/ku57pq00002ma0c1-att/Keidanren_JICA_Co-Creation_en.pdf

3/3 | ДОСЛІДЖЕННЯ

НА ШЛЯХУ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС

[Електронна комерція]

[Телекомунікації]

[Довірчі послуги]

Український центр європейської політики (УЦЄП) – це незалежний аналітичний центр аналізу та вироблення політики, який був заснований у 2015 році.

Наша місія — сприяти проведенню реформ в Україні задля сталого економічного зростання та побудови відкритого суспільства в партнерстві з інституціями на всіх рівнях.

Пріоритетні напрями діяльності:

- підготовка та розповсюдження експертно-аналітичних матеріалів для сприяння євроінтеграційним реформам в Україні;
- популяризація європейських цінностей в українському суспільстві;
- інформування суспільства про можливості і переваги тісної співпраці з ЄС;
- сприяння посиленій економічній, політичній та торгівельній співпраці України з Європейським Союзом;
- інформування міжнародної спільноти про виклики і досягнення в здійсненні Україною реформ, передбачених Угодою про асоціацію між Україною та ЄС.

01001, Київ, Україна
проспект Глушкова 9В,
офіс 294

www.ucep.org.ua
press@ucep.org.ua
facebook.com/UCEP.org.ua

Київ, 2021

ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

УКРАЇНСЬКИЙ ЦЕНТР ЄВРОПЕЙСЬКОЇ ПОЛІТИКИ