RELIANCE

Юридичний висновок

1. Вступна частина

Назва документа:	**Юридичний висновок щодо відповідності алгоритму роботи мобільного застосунку «Pakto» вимогам законодавства України про електронну ідентифікацію та електронні довірчі послуги**
Дата складення:	**02.07.2026**
Місце складення:	**місто Миколаїв**
Виконавець:	**ЮК RELIANCE**
Юрист (адвокат):	**Дмитро Слободянюк**
Клієнт:	**Дмитро Дійкун**
Перелік матеріалів:	**Документ «Pakto_UA.docx» як базовий вхідний матеріал, що описує призначення застосунку та юридично значущу логіку дій користувача.**

2. Перелік питань, поставлених для дослідження

- **Питання 1:** Чи відповідає описана логіка алгоритму застосунку «Pakto» вимогам до удосконаленого електронного підпису (AES / УЕП) відповідно до ст. 17-1 Закону України № 2155-VIII в межах офлайн-сценарію (QR)?
- **Питання 2:** Чи відповідає описана логіка алгоритму застосунку «Pakto» вимогам до удосконаленого електронного підпису (AES / УЕП) відповідно до ст. 17-1 Закону України № 2155-VIII в межах онлайн-сценарію (посилання)?
- **Питання 3:** Чи є юридично достатнім для встановлення рівня підпису AES одноразове підтвердження особи користувача через КЕП (Дія.Підпис) із подальшим використанням локального апаратного ключа пристрою?

3. Нормативно-правова база

- **Цивільний кодекс України** (зокрема, ч. 3 ст. 207 щодо використання аналога власноручного підпису за згодою сторін).
- **Закон України «Про електронну ідентифікацію та електронні довірчі послуги»** (зокрема, ст. 1, ст. 17-1, норми щодо УЕП та КЕП).
- **Регламент ЄС № 910/2014 (eIDAS)** (зокрема, ст 26).

4. Дослідження та обґрунтування

Аналіз відповідності описаної в документі логіки застосунку Pakto вимогам до удосконаленого електронного підпису (УЕП / AES) відповідно до ст. 17-1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги.

Закон встановлює чотири обов’язкові вимоги для УЕП (ст. 17-1). Розглянемо, як описана логіка (з одноразовим підтвердженням особи через КЕП у Дія.Підпис та подальшою прив'язкою до апаратного ключа пристрою) задовольняє ці вимоги окремо для двох сценаріїв.

4.1. Офлайн-сценарій (QR)

У цьому сценарії сторони підписують договори на власних телефонах без використання інтернету, обмінюючись даними через QR-коди.

4.1.1. **Вимога 1:** Однозначний зв’язок підпису з підписувачем

- **Як забезпечується:** Кожен користувач має індивідуальний криптографічний ключ, що генерується в захищеному апаратному середовищі його пристрою. Підписи двох сторін криптографічно розрізняються, а дані підтвердженої особи фіксуються безпосередньо у підписаному тексті.
- **Відповідність: ВІДПОВІДАЄ.** Однозначний зв'язок між створеним підписом та криптографічним ключем конкретного користувача зберігається.

4.1.2. **Вимога 2:** Можливість ідентифікувати підписувача

- **Як забезпечується:** На етапі онбордингу (за наявності інтернету) користувач підписує своїм КЕП (Дія.Підпис) документ-запит. Сервер перевіряє цей КЕП, витягує перевірені державою дані особи (ПІБ, РНОКПП) і прив’язує їх до згенерованого локального ключа пристрою.

Надалі під час офлайн-підписання саме ці раніше верифіковані дані вшиваються у договір.

- **Відповідність: ВІДПОВІДАЄ.** Закон не вимагає проводити ідентифікацію особи під час кожного окремого акту підписання УЕП. Достатньо, щоб технологія дозволяла ідентифікувати автора підпису. Оскільки локальний ключ жорстко і криптографічно пов'язаний з ідентифікаційними даними, отриманими з Кваліфікованого електронного підпису (КЕП), вимога щодо можливості ідентифікації виконується.

4.1.3. Вимога 3: Створення підпису з використанням засобів, які підписувач може контролювати одноосібно (високий рівень довіри)

- **Як забезпечується:** Ключ створюється всередині апаратного модуля безпеки смартфона, копіювання програмного ключа не допускається, а доступ до його активації захищено біометрією власника.

- **Відповідність: ВІДПОВІДАЄ.** Використання апаратного сховища пристрою у поєднанні з біометричною активацією є надійним юридичним аргументом для підтвердження одноосібного контролю користувача над засобом підпису.

4.1.4. Вимога 4: Виявлення подальших змін у підписаних даних

- **Як забезпечується:** Документ криптографічно «запечатується» (хешується та підписується). Підпис другої сторони математично пов'язаний із підписом першої. Будь-яка модифікація тексту після процедури підписання порушить цілісність криптографічного ланцюжка і буде виявлена під час перевірки.

- **Відповідність: ВІДПОВІДАЄ.**

Важливий нюанс офлайн-сценарію: Для УЕП критичним є фіксація часу. Оскільки в офлайні немає прямого доступу до серверів точного часу (TSA), застосунок за відсутності мережі бере час із пристрою та ставить Попередження. З юридичної точки зору це не скасовує статус УЕП, але у разі судового спору сторона може намагатися оскаржити точний момент підписання. Проте сама логіка алгоритму підпису повністю вкладається у критерії AES.

4.2. Онлайн-сценарій (посилання)

У цьому сценарії сторони взаємодіють дистанційно, а обмін даними та підписами координується через сервер застосунку.

4.2.1. Вимога 1: Однозначний зв’язок підпису з підписувачем

- **Відповідність: ВІДПОВІДАЄ.** Аналогічно до офлайну, кожна сторона використовує власний унікальний апаратний ключ. Оскільки пристрої фізично різні та розділені, зв'язок **«ключ — конкретна особа» фіксується ще чіткіше.**

4.2.2. Вимога 2: Можливість ідентифікувати підписувача

- **Відповідність: ВІДПОВІДАЄ.** Використовується той самий надійний принцип: одноразова первинна ідентифікація через КЕП у Дії з довгостроковою прив'язкою результату до особистого ключа. Державні ідентифікаційні дані інтегруються у фінальний PDF-документ.

4.2.3. Вимога 3: Одноосібний контроль над ключем

- **Відповідність: ВІДПОВІДАЄ.** Застосовується підписання на власному пристрої під контролем особистої біометрії. Сервер виступає лише каналом передачі підписаних даних, але сам не має доступу до закритих ключів користувачів і не може згенерувати підпис замість них.

4.2.4. Вимога 4: Виявлення подальших змін у підписаних даних

Відповідність: ВІДПОВІДАЄ. Забезпечується аналогічне криптографічне запечатування файлу. Додатковою перевагою онлайн-сценарію є те, що проміжний обмін фіксується сервером, а мітка часу (Timestamp) гарантовано береться з незалежних акредитованих європейських джерел точного часу.

5. Висновки та відповіді на питання

Описана логіка алгоритму застосунку Pakto повністю відповідає вимогам до удосконаленого електронного підпису (AES / УЕП) за ст. 17-1 Закону № 2155-VIII як для офлайн- (QR), так і для онлайн- (посилання) сценаріїв.

Рішення розробників — здійснювати ідентифікацію особи один раз через КЕП (Дія.Підпис), а потім делегувати створення підписів локальному апаратному ключу пристрою під біометричним контролем — є абсолютно коректним з погляду законодавства про електронні довірчі послуги.

Такий підхід трансформує підпис у застосунку в удосконалений (УЕП), оскільки засоби підпису створюють стійкий математичний зв'язок із підтвердженою особою та гарантують незмінність документа.

6. Рекомендації та застереження

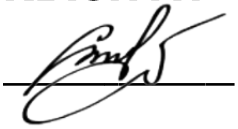
6.1. Юридичні застереження:

- Юридичний висновок базується виключно на логіці, описаній у документі «Pakto_UA.docx» (без аудиту вихідного коду), та відображає стан законодавства на момент його складення.

6.2. Практичні рекомендації:

- Чітко зафіксувати в Публічній оферті застосунку (Terms of Service) статус підпису як УЕП (а не КЕП) та обмеження щодо сфер його використання (наприклад, не застосовувати для правочинів, що потребують нотаріального посвідчення).

7. Підпис та реквізити

- Юрист ЮК RELIANCE  **Дмитро Слободянюк**