ВИТЯГ
з Положення про криптографічний захист інформації в АТ «ТАСКОМБАНК»

ПОРЯДОК
застосування Електронного підпису (ЕП) та цифрового власноручного підпису (ЦВП) в АТ «ТАСКОМБАНК»

1. Порядок застосування ЕП та ЦВП в АТ «ТАСКОМБАНК» (далі - Порядок) є внутрішнім документом Банку, якій розроблений відповідно до вимог законодавства України, нормативно-правових документів Національного банку України, з метою встановлення єдиного порядку застосування ЕП в Банку.
2. Порядок визначає критерії рівня довіри (високий, середній, низький) до засобів електронної ідентифікації, якими будуть підписуватись банківські електроні документи та можливість використання ЕП (кваліфікований ЕП, удосконалений ЕП, простий ЕП, простий ЕП на базі OTP-паролю/коду) та ЦВП.
3. ЕП є обов’язковим реквізитом електронного документа. Підписувач, який створює електронний документ з ЕП, цим самим засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, не має заперечень до тексту документа (або його заперечення внесені як окремий реквізит документа) і свідомо застосовував свій ЕП у контексті, передбаченому документом (підписав, затвердив, погодив, завізував, засвідчив, ознайомився).

   На документ (договір) в електронній формі одразу після його підписання цифровим власноручним підписом Клієнта накладається кваліфікована електронна позначка часу. Після цього уповноважений працівник Банку зобов'язаний невідкладно підписати цей документ власним кваліфікованим електронним підписом або засвідчити кваліфікованою електронною печаткою банку з кваліфікованою електронною позначкою часу.
4. ЕП створюються у послідовності, визначеній застосованою технологією оброблення інформації, якщо електронний документ підписується двома або більше посадовими особами суб’єкта електронної взаємодії чи представниками двох або більше суб’єктів електронної взаємодії. Технологія оброблення інформації розробляється Банком з урахуванням законодавства України.

   Створення електронного документа завершується створенням останнього ЕП відповідно до технології створення такого електронного документа.

   Для ідентифікації автора електронного документа може використовуватися електронний підпис.

   Відносини, пов’язані з використанням удосконалених та кваліфікованих електронних підписів, регулюються Законі України "Про електронні довірчі послуги".

   Порядок використання електронного підпису банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторами платіжних систем та/або учасниками платіжних систем, технологічними

операторами платіжних послуг визначається Національним банком України.

Порядок використання електронного підпису учасниками ринків капіталу та професійними учасниками організованих товарних ринків визначається Національною комісією з цінних паперів та фондового ринку.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів в Банку відбуваються згідно вимог Закону України «Про електронні документи та електронний документообіг».

Створення електронних документів, що згідно із законодавством України підлягають передаванню на архівне зберігання, здійснюється із застосуванням кваліфікованих ЕП та/або кваліфікованих електронних печаток, що забезпечують можливість перевірки відповідних кваліфікованих ЕП та/або кваліфікованих електронних печаток у довгостроковому періоді згідно з вимогами національних стандартів, визначеними в Переліку стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг, що є додатком до вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992 (зі змінами).

5. Використання удосконаленого ЕП, удосконаленої електронної печатки та простого ЕП здійснюється на підставі договору між Банком і Клієнтом, який укладається в письмовій формі (у формі паперового документа з власноручними підписами сторін або як електронний документ із кваліфікованими ЕП сторін) після проведення ідентифікації та верифікації Клієнта відповідно до вимог законодавства України у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму.

   Договір має містити умови та порядок (процедуру) визнання суб'єктами електронної взаємодії правочинів у вигляді електронних документів із використанням удосконаленого ЕП, удосконаленої електронної печатки або простого ЕП відповідно.

   Договір має також містити умови щодо розподілу ризиків збитків, що можуть бути заподіяні підписувачам і третім особам у разі використання удосконаленого ЕП або удосконаленої електронної печатки відповідно.

   Банк та Клієнт мають право укласти договір про використання удосконаленого ЕП, удосконаленої електронної печатки та простого ЕП у формі електронного документа з використанням електронних підписів, щодо яких між Клієнтом та Банком вже укладено договір.

   Укладення окремого договору щодо використання кваліфікованого ЕП не вимагається.

6. Використання простого ЕП, удосконаленого ЕП (зокрема удосконаленої електронної печатки), кваліфікованого ЕП (зокрема кваліфікованої електронної печатки), цифрового власноручного підпису в електронних

документах Банку відбувається згідно вимог Положення про використання електронного підпису та електронної печатки, затвердженого постановою Правління Національного банку України від 20.12.2023 № 172. УВАГА! Змінами внесеними Постановою Кабінет міністрів України № 617 від 24.05.2022 до приписів Постанови Кабінету Міністрів України № 300 від 17.03.2022 «Деякі питання забезпечення безперебійного функціонування системи надання електронних довірчих послуг» подовжена можливість застосування УЕП (удосконалених електронних підписів) тільки на час дії воєнного стану в Україні та ще на шість місяців з моменту його скасування чи припинення.

7. Банк має право застосовувати процедури фото та/або відеофіксації, інші процедури з метою документування та контролю за процесом підписання документа Клієнтом з використанням цифрового власноручного підпису.

   Застосування зазначених процедур повинно здійснюватися за умови попередньо отриманої згоди Клієнта.

   Інформаційна система, яку Банк використовує для створення, зберігання електронних документів із цифровими власноручними підписами Клієнтів Банку, повинна забезпечувати фіксування дій Клієнтів та працівників Банку, пов'язаних з підписанням документів цифровим власноручним підписом, у захищеному від модифікації та знищення електронному журналі подій.

8. Обов’язкові вимоги для створення та застосування Електронного підпису в електронних документах Банку:

   ЕП має юридичну силу незалежно від технологій, що застосовуються для створення ЕП, якщо відповідає таким умовам (п. 3.5 Положення):

   - електронні дані, що використовуються для створення ЕП, є унікальними та однозначно пов’язані із підписувачем і не пов’язані з жодною іншою особою;
   - ЕП дає змогу однозначно ідентифікувати підписувача;
   - технологія застосування ЕП забезпечує підписувачу під час підписування контроль електронних даних, які підписуються, та електронних даних, які використовуються для створення ЕП;
   - під час перевірки відповідно до затвердженого в Банку порядку не виявлено будь-яких змін в електронному документі;
   - під час перевірки відповідно до затвердженого в Банку порядку не виявлено будь-яких змін ЕП після підписання електронного документа.

9. Клієнти для підписання договору з Банком можуть використовують кваліфікований ЕП, удосконалений ЕП або простий ЕП, що має юридичну силу та відповідає вимогам законодавства України (вимоги до ЕП зазначено в п. 3.5. Положення або 8.1. Порядку).

10. Обов’язкові вимоги до криптоалгоритмів, ключів, Гешування наведені в Додатку 2 Положення («Порядок управління криптографічними алгоритмами та терміном дії криптографічних ключів»).

11. Обов’язкові вимоги до ОТР-паролю/коду в разі застосування його ЕП в Банку:

- При формуванні OTP-паролю/коду використовується Гешування електронного документу, дата формування пароля, симетричний критографічний ключ (для кожного клієнта генерується криптографічний симетричний ключ, всі ключи повинні бути зашифрованими), унікальне число або унікальним ідентифікатором (UUID-Universally Unique Identifier). OTP-пароль/код обов'язково повинен мати обмежений час існування. Можливо додавання додаткових даних для формування OTP-паролю/коду, що підвищать його криптостійкість.
- Власник інформаційної системи в Банку, зокрема підрозділ Банку, що є власником відповідного бізнес процесу та якій використовує OTP-пароль/код в якості ЕП повинен затвердити окремий ВНД щодо алгоритму генерації OTP-паролю/коду та порядок перевірки OTP-паролю/коду в якості ЕП.
- При перевірці OTP-паролю/коду, що отриманий від Клієнта Власником банківської системи (підрозділом Банку, що є власником відповідного бізнес процесу), останньому необхідно зробити перевірку по алгоритму генерації OTP-пароля/коду (див. п.9 Порядку) та зрівняти OTP паролі.
- В разі, коли отриманий OTP-пароль/код від Клієнта та згенерований OTP-пароль/код співпадають, вважається що ЕП вірний.
- В системах Банку, що використовують OTP-пароль/код повинен бути функціонал перевірки OTP-пароля/коду.
- Алгоритми створення та використання OTP-пароля/коду та криптоалгоритми що використовуються переглядаються щорічно з точку зору криптостійкості та наявності вразливостей. Власник інформаційної системи Банку, що використовує OTP-паролі/коди, надає службовою запискою до ДІБ опис алгоритму створення та використання OTP-пароля/коду та криптоалгоритми, що використовуються для аналізу.

12. Технічне завдання на розробку/зміну банківських систем/програмного забезпечення що використовує OTP-паролі в частині використання криптозасобів обов'язково погоджується з ДІБ.
13. Підрозділу інформаційних технологій (інформатизації, автоматизації) Банку забороняється бути власником інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності.
14. Банк запровадив такі заходи контролю доступу до інформаційних систем банку:
    - перевірку наявності у користувача дозволу керівництва та власника інформаційної системи на такий доступ;
    - заборону одноосібного ініціювання заявки, підтвердження та надання доступу;
    - перевірку відповідності рівня наданого доступу принципу мінімально необхідного рівня повноважень;
    - періодичну перевірку відповідності наданих прав доступу користувачеві тим, що діють на момент перевірки.

15. Електронна ідентифікація здійснюється за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації. Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них.
16. Рівні довіри до засобів електронної ідентифікації, якими підписуються банківські електронні документи/договори, повинні відповідати таким критеріям:
    - **Низький рівень довіри** до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності;

Використання простого ЕП, цифрового власноручного підпису або ОТР-паролю/коду (повинен відповідати вимогам п. 9 Порядку) забезпечує низький рівень довіри до схем електронної ідентифікації.

- **Середній рівень довіри** до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності;

Використання удосконалених ЕП та печаток забезпечує середній рівень довіри до схем електронної ідентифікації.

- **Високий рівень довіри** до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи.

Використання кваліфікованих ЕП та печаток забезпечує високий рівень довіри до схем електронної ідентифікації.

17. Приклад застосування рівнів довіри до засобів електронної ідентифікації при підписанні електронних документів (договорів):

Таблиця 1

№	Тип електронного документу	Рівень довіри до засобів електронної ідентифікації	Вид підпису	
			Банк	Клієнт
1	Договір поточного рахунку, Договір вкладу (депозиту)	низький рівень довіри (простий ЕП) або середній рівень довіри (УЕП) або високий рівень довіри (КЕП)	Простий ЕП або УЕП або КЕП	Простий ЕП або УЕП або КЕП
2	Договір кредиту та інші документи до кредитного договору, Договори документарних операцій (гарантії, акредитиви) та інші документи до цих договорів	високий рівень довіри (КЕП)	КЕП	КЕП
3	Договори забезпечення	високий рівень довіри (КЕП)	КЕП	КЕП

Визначення відповідного виду договору Банку та відповідного виду ЕП при його підписанні зі сторони Банку та Клієнта визначається окремим ВНД Банку, з обов'язковим дотриманням вимог даного Порядку та Положення, вимог законодавства України з питань електронних довірчих послуг, електронного документообігу, нормативно-правових актів Національного банку України.

ВНД Банку, яким буде визначатися відповідний вид договору Банку та відповідний вид ЕП в обов'язковому порядку погоджується з ДІБ

Технічне завдання (ТЗ) на розробку/зміну банківських систем/програмного забезпечення що використовує ЗЗІ в частині використання криптозасобів в обов'язковому порядку погоджується з ДІБ.

Ступінь виконання технічного завдання (ТЗ виконано, не виконане, потрібна доробка) в частині використання криптозасобів підтверджується ДІБ.

18. Відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів в Банку відбуваються згідно вимог Закону України «Про електронні документи та електронний документообіг».

Створення електронних документів, що згідно із законодавством України підлягають передаванню на архівне зберігання, здійснюється із застосуванням кваліфікованих ЕП та/або кваліфікованих електронних печаток, що забезпечують можливість перевірки відповідних кваліфікованих ЕП та/або кваліфікованих електронних печаток у довгостроковому періоді згідно з вимогами національних стандартів, визначеними в Переліку стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг, що є додатком до вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992 (зі змінами).

19. Зміст Порядку підлягає перегляду при зміні норм законодавства України, що регламентує застосування ЕП в банківській діяльності.