

РОЗДІЛ 8. СЕРВІС ЕЛЕКТРОННИХ ГАМАНЦІВ

ДО УНІВЕРСАЛЬНОГО ДОГОВОРУ БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ КЛІЄНТІВ – ФІЗИЧНИХ ОСІБ У АТ «БАНК КРЕДИТ ДНІПРО»

- 8.1. Банк до отримання від Клієнта (Держателя Платіжної картки) повідомлення про заборону токенизації, надаючи послуги за цим УДБО, виходить з того, що Клієнт (власник рахунку), не забороняє токенизацію Карток/додаткових карток, випущених за його рахунком. Клієнт може подати заяву про заборону токенизації всіх або окремих Карток/додаткових карток, випущених за його рахунком (-ми), шляхом звернення до Контакт-центру з проходженням ідентифікації. Клієнт може скасувати раніше подану ним заяву про заборону токенизації в той самий спосіб, в який заява була подана.
- 8.2. Токенизація та операції з використанням Сервісу електронних гаманців виконується лише за дійсними картками/додатковими картками платіжної МПС за наявності технічної можливості в Банку.
- 8.3. Для здійснення розрахунків за допомогою Сервісу електронних гаманців, необхідно зареєструвати в ньому картки, надавши відповідні реквізити таких карток в мобільному додатку.
- 8.4. Підключення Сервісу електронних гаманців на мобільний пристрій здійснюється з використанням підказок мобільного додатку.
- 8.5. Банк здійснює перевірку введених в мобільний додаток реквізитів Платіжної картки (номер картки, термін дії картки, код CVC2/CVV2), а також, у разі необхідності, проводить Автентифікацію Держателя картки. Картка повинна бути дійсна.
- 8.6. Автентифікація Держателя здійснюється Банком одним із способів (на вибір Держателя або у разі, якщо інший спосіб автентифікації є не вдалим):
- 8.6.1. Використанням одноразового цифрового пароля (OTP-пароля), направленою Держателю картки в SMS-повідомленні/Push-повідомленні.
- 8.6.2. Шляхом проходження Держателем картки процедури перевірки через Контакт-центр у порядку, встановленому Банком.
- 8.7. Після успішної реєстрації Картки в мобільному додатку в захищеному сховищі мобільного пристрою формується і зберігається токен. Токен дозволяє однозначно ідентифікувати Картку, що використовується при здійсненні платежів за допомогою Сервісу електронних гаманців.
- 8.8. В Сервісі електронних гаманців фіксується десять останніх операцій за кожною зареєстрованою в Сервісі електронних гаманців Карткою (історія операцій).
- 8.9. При наявності декількох Карток, зареєстрованих в Сервісі електронних гаманців, Держатель Картки може вибрати Картку, з використанням якої будуть здійснюватися платежі за умовчанням в Сервісі електронних гаманців.
- 8.10. Держатель з використанням Сервісу електронних гаманців за допомогою відповідного мобільного пристрою може:
- здійснювати платежі через POS-термінал, оснащений технологією NFC;
 - здійснювати платежі в мобільних додатках на мобільному пристрої і на сайтах, які підтримують розрахунки через Сервіс електронних гаманців.
- 8.11. Держатель Картки здійснюючи платіж за допомогою Сервісу електронних гаманців, реєстрацію Картки в мобільному додатку, використовуючи при цьому одноразовий цифровий пароль/відбиток пальця, підтверджує виникнення і використання ним аналога власноручного підпису. Держатель Картки визнає, що формування ним електронного документу для здійснення платежу за допомогою Сервісу електронних гаманців, є аналогом власноручного підпису документів на паперовому носії.
- 8.12. Видалення підключеної картки із Сервісу електронних гаманців здійснюється шляхом видалення токenu з мобільного додатку.
- 8.13. Держатель зобов'язаний видалити токен з мобільного додатку та видалити мобільний додаток з мобільного пристрою у наступних випадках:
- у випадках зламу мобільного пристрою Держателю або підозри про злам;
 - одержання третіми особами доступу до мобільного пристрою або виникнення підозри про це чи інше порушення безпеки та доступу до мобільного пристрою та/або мобільного додатку тощо;
 - перед знищенням мобільного пристрою або передачею в користування іншій особі та іншим вибуттям мобільного пристрою з володіння Держателя, яке відбувається за його волевиявленням, або без такого волевиявлення.
- 8.14. Видалення токenu може здійснюватися Банком у разі звернення Держателя до Контакт-центру, його ідентифікації та отримання повідомлення від Держателя про ознаки компрометації токenu.
- 8.15. Держатель розуміє і погоджується з тим, що:
- не всі юридичні особи та фізичні особи-підприємці, які здійснюють реалізацію товарів, виконання робіт, надання послуг, а також не всі установи, які надають фінансові послуги, можуть забезпечити можливість оплати за допомогою Сервісу електронних гаманців;
 - платіжні системи, установи, які надають фінансові послуги, можуть вводити обмеження, зокрема, за сумами операцій з використанням Сервісу електронних гаманців та встановлювати свої комісії щодо таких операцій;
 - здійснення операцій з використанням Сервісу електронних гаманців може бути обмежено функціональністю програмного забезпечення мобільного пристрою, в тому числі, мобільного додатку;
 - доступ, використання і можливість здійснення операцій з використанням Сервісу електронних гаманців належить від стану мереж бездротового зв'язку, використовуваних інтернет-провайдером;
 - з будь-яких питань, пов'язаних з технічною підтримкою мобільного пристрою, вимогами до програмного і апаратного забезпечення Держатель Картки повинен звертатися безпосередньо до сервісного центру виробника такого мобільного пристрою;
 - порядок отримання і обробки будь-якої інформації, одержуваної інтернет-провайдером в процесі використання Держателем Картки Сервісу електронних гаманців, регулюється договором між Держателем та інтернет-провайдером;
 - інтернет-провайдер, оператор мобільного зв'язку, яким користується Держатель, інші особи, задіяні в забезпеченні роботи Сервісу електронних гаманців, мають свої умови обслуговування і політики конфіденційності. Передаючи

зазначеним особам свої персональні дані, використовуючи послуги або відвідуючи сайти в мережі Інтернет зазначених осіб, Держатель приймає їх умови обслуговування і політики конфіденційності.

8.16. Держатель усвідомлює підвищений ризик та розуміє, що при використанні Сервісу електронних гаманців доступ до мобільного пристрою Держателя безпосередньо впливає на можливість несанкціонованих Держателем операцій за Карткою/додатковою Карткою, а отже Держатель самостійно несе відповідальність за:

- конфіденційність одноразових паролів, ПІН, інших засобів доступу Держателя до мобільного пристрою, мобільного додатку, картки/додаткової картки;
- наявність обмежень доступу до мобільного пристрою (систематичне блокування тощо) та надійність та достатність обраних Держателем засобів обмеження доступу до мобільного пристрою (паролів, біометричних ідентифікаторів, часових інтервалів блокування тощо), за наявності та своєчасне оновлення антивірусних програм, встановлених на ньому мобільним додатком;
- операції, здійсненні за допомогою Сервісу електронних гаманці, за наявності технічних можливостей Банку надавати таку послугу, на мобільному пристрої Держателя;
- своєчасне повідомлення Банку про необхідність блокування токєну, в тому числі, але не виключно: у випадках зламу мобільного пристрою Держателя третіми особами, втрати/викрадення або пошкодження мобільного пристрою, одержання третіми особами доступу до мобільного пристрою або виникнення підозри про те чи інше порушення безпеки та доступу до мобільного пристрою та/або мобільного додатку тощо;
- видалення токєну з мобільного додатку перед видаленням мобільного додатку з мобільного пристрою;
- видалення мобільного додатку перед передачею мобільного пристрою на переробку, перед знищенням, передачею в користування або у власність третій особі та іншим вибуттям мобільного пристрою з володіння Держателя, яке відбувається за його волевиявленням або без такого;
- виконання інструкцій та правил роботи з мобільним додатком.

8.17. Банк відповідає за:

- збереження грошових коштів на рахунку Держателя Картки та виконання операцій за рахунком за умови дотримання Держателем Картки умов цього УДБО, тарифів;
- невиконання своїх зобов'язань перед Держателем Картки відповідно до чинного законодавства.

8.18. Банк не несе відповідальності за:

- роботу Сервісу електронних гаманців;
- неможливість здійснення Держателем Картки операцій за допомогою Сервісу електронних гаманців;
- будь-яке блокування, призупинення, анулювання або припинення використання Картки/додаткової картки за допомогою Сервісу електронних гаманців;
- конфіденційність інформації, що зберігається на мобільному пристрої, в мобільному додатку;
- підтримку операційної системи мобільного пристрою;
- дії провайдера або будь-якої третьої особи, що здійснюються в межах обслуговування мобільного додатку, Сервісу електронних гаманців;
- будь-які обставини, які можуть перервати, перешкодити або іншим чином вплинути на функціонування мобільного додатку, Сервісу електронних гаманців (недопустимість мережі оператора мобільного зв'язку, обмеження зони покриття мережі мобільного зв'язку, перебої в подачі або переривання бездротового з'єднання);
- обслуговування бездротових мереж зв'язку, систему відключення/переривання бездротового з'єднання.

8.19. Банк не гарантує конфіденційність і безпеку електронної передачі даних Держателя Картки через сторонні підключення, які не перебувають під контролем Банку. Конфіденційність та безпека передачі даних забезпечуються відповідно до регламентів Компанії, які надають Сервіс електронних гаманців.