ДОГОВІР №
про надання розрахункових послуг в системі "Клієнт-Банк"

м. Київ

АКЦІОНЕРНЕ ТОВАРИСТВО «АГРОПРОСПЕРІС БАНК», надалі "Банк", в особі , який (яка) діє на підставі , з однієї сторони, і , ***надалі "Клієнт", в особі ,*** з іншої сторони, надалі разом "Сторони", уклали цей Договір про наступне:

1. Предмет Договору

1.1. Клієнт доручає, а Банк приймає на себе зобов'язання щодо виконання розрахункового обслуговування Клієнта за допомогою програмно-технічного комплексу "Клієнт-Банк" (далі – система «Клієнт-банк»).
1.2. Плата за послуги з обслуговування в системі «Клієнт-Банк» здійснюється відповідно до Тарифів банку на розрахунково-касове обслуговування.
1.3. Клієнт доручає Банку самостійно стягувати плату з його рахунків за обслуговування і надані послуги згідно з діючими Тарифами Банку на розрахунково-касове обслуговування та Договором банківського рахунку.

1.4. Терміни та визначення

Аварійний пароль - пароль, який призначається Банком Користувачу для виконання ним процедури створення нового ключа ЕЦП. Після призначення Аварійного паролю, звичайна робота Користувача у системі «Клієнт – банк» стає не можливою до завершення процедури відновлення або видалення Аварійного паролю.
Після успішного закінчення процедури відновлення, Аварійний пароль автоматично видаляється.
Блокування облікового запису - дія, внаслідок якої тимчасово унеможливлюється робота користувачів з системою «Клієнт-банк», облікові записи яких піддаються цій дії, на строк до виконання дії розблокування облікового запису.
У разі блокування облікового запису Клієнта відбувається блокування всіх облікових записів користувачів, що пов'язані з ним.
Відновлення ключа ЕЦП - Процедура, під час якої Користувач, зі свого робочого місця, має змогу відновити (генерувати новий) Ключ ЕЦП, який був зіпсований або втрачений Користувачем з різних причин, в т.ч. коли Користувач не пам'ятає пароль на секретний ключ. Розпочати процедуру відновлення можливо лише після призначення Користувачу Аварійного паролю.
Заміна відповідальної особи клієнта / створення нового користувача - процедура, що має на меті створення нового клієнта (з додатковою генерацією ключа ЕЦП при формуванні Первинного сертифікату) системи «Клієнт-банк».
ЕЦП - електронний цифровий підпис.
Інформація про відкриті ключі користувача (запит) - документ, який формується системою, під час виконання процедури генерування нового Ключа ЕЦП Користувачем. Підтверджує, що під час генерування до Банку в електронному вигляді надійшов запит на сертифікацію відкритого (публічного) ключа Користувача. Цей документ, роздрукований на паперовому носії та оформлений (дата виконання, підпис Користувача, підпис керівника підприємства, відбиток печатки (за наявності) підприємства) має бути переданий до Банку та є обов'язковою підставою для виконання Банком Сертифікації відкритого ключа (запиту на сертифікат).
Під час кожного нового генерування Ключа ЕЦП формується новий унікальний запит на сертифікацію.
Ключ ЕЦП - призначений для підписання (накладання ЕЦП) документів та повідомлень, які Клієнт надсилає засобами системи «Клієнт-банк» у Банк. Ключ складається з відкритої (публічної) та закритої частини. Відкрита частина відома Банку і зафіксована на паперовому носії у вигляді документу «Інформація про відкриті ключі користувача (запит)», закрита частина зберігається виключно на електронному носії у Клієнта. Під час накладання ЕЦП Клієнтом – використовується закрита частина Ключа ЕЦП. Відкрита частина використовується для перевірки достовірності підпису на документах та повідомленнях, під час приймання їх Банком. Даний механізм забезпечує ідентифікацію особи, що наклала особистий підпис та захист документів і повідомлень від підробки, під час передачі їх каналами зв'язку від Клієнта до Банку засобами системи «Клієнт – банк».
Користувач - посадова особа Клієнта, для якої створений Обліковий запис та надані права у системі «Клієнт – банк».
Логін - найменування Облікового запису Користувача, унікальний набір символів в межах системи «Клієнт – банк», який однозначно ідентифікує кожного Користувача.
Обліковий запис Клієнта - спеціальна одиниця інформації про Клієнта Банку у системі «Клієнт – банк».
Обліковий запис Користувача - спеціальна одиниця інформації про Користувача у системі «Клієнт – банк», яка описує права та повноваження доступу до рахунків Клієнта та ресурсів у системі «Клієнт – банк».
Сертифікація відкритого ключа (запиту на сертифікат) - дія, під час якої у системі «Клієнт-банк» виконується перевірка відкритого ключа, надісланого Користувачем у вигляді запиту на сертифікат, при генеруванні ним нового Ключа ЕЦП. При успішній перевірці системою, на основі запиту формується сертифікат з унікальним номером. Сертифікат зберігається у базі даних Банку та надсилається засобами системи «Клієнт-банк» Користувачу. Після збереження сертифікату Користувачем, вступає в дію його новий Ключ ЕЦП.
Система «Клієнт-банк» - система дистанційного банківського обслуговування «Клієнт-банк».
Первинний сертифікат - набір, що складається із сертифікату та Ключа ЕЦП, з терміном дії 30 днів. Цей набір передається кожному новому Користувачу та необхідний для виконання ним першого входу у систему «Клієнт-банк» і генерування нового (робочого) Ключа ЕЦП. Після генерування Користувачем робочого Ключа ЕЦП, Первинний сертифікат стає не дійсним.
Токен – захищений носій ключової інформації, сертифікований відповідно до державних стандартів захисту інформації. Призначений для зберігання Ключів ЕЦП Користувачів.
OTP (one time password) токен – пристрій, призначений для генерації одноразових паролів з метою додаткової авторизації Користувача в системі «Клієнт-банк».

2. Права та зобов'язання сторін

2.1. Банк має право:

2.1.1. Запроваджувати нові програмно-технічні та технологічні засоби, розроблені або придбані ним з метою вдосконалення системи "Клієнт-Банк".
2.1.2. Повертати без обробки електронні розрахункові документи, зміст яких не відповідає чинному законодавству та нормативно-правовим актам Національного банку України.
2.1.3. Припиняти обслуговування Клієнта відповідно до вимоги уповноважених органів у випадках, передбачених чинним законодавством України.
2.1.4. Відмовляти Клієнту у виконанні платіжних інструментів у разі порушення Клієнтом правил, встановлених чинним законодавством або умов цього Договору.
2.1.5. Відмовити Клієнту у виконанні електронного розрахункового документу якщо операція містить ознаки такої, що підлягає фінансовому моніторингу.
2.1.6. У разі непогашення Клієнтом заборгованості по оплаті обслуговування за системою "Клієнт-Банк":
2.1.6.1. до 14 числа (включно) місяця, що слідує за звітним місяцем призупинити обслуговування Клієнта в системі "Клієнт-Банк" із збереженням паролів для доступу до системи. У разі погашення Клієнтом заборгованості у строки, зазначені у п. 2.1.6.2. цього Договору, доступ до системи відновлюється на підставі відповідного письмового запиту, наданого до Банку;
2.1.6.2. до 25 числа (включно) місяця, що слідує за звітним місяцем, припинити обслуговування Клієнта в системі "Клієнт-Банк" із послідуючим розірванням цього Договору. Обслуговування Клієнта у системі «Клієнт-Банк» припиняється з наступного робочого дня. У такому разі для поновлення обслуговування у системі «Клієнт-Банк» Клієнтові необхідно укласти новий договір про надання розрахункових послуг в системі "Клієнт-Банк" із отриманням нових паролів для доступу до системи "Клієнт-Банк".
2.1.6.3. Здійснювати тимчасове блокування операцій Клієнта в системі «Клієнт-Банк» за рахунками на підставі усного звернення Клієнта до Банку або шляхом надсилання клієнтом повідомлення на електронну адресу Банку, у зв'язку з виникненням нештатних ситуацій в системі «Клієнт-Банк», втрати ключів ЕЦП, паролів тощо до моменту з'ясування обставин інциденту, з подальшим наданням не пізніше наступного робочого дня письмового підтвердження такого

Банк
_____
М.П.

Клієнт
_____
М.П.

звернення. Розблокування операцій Клієнта у системі «Клієнт-Банк» здійснюється на підставі відповідного письмового звернення Клієнта до Банку.

2.2. Банк бере на себе зобов'язання:

2.2.1. Надати Користувачам Клієнта Первинні сертифікати, засоби крипто захисту системи «Клієнт-Банк», документацію, регламентуючу правила та технологію використання системи «Клієнт-Банк», надати Клієнту консультацію з використання, обслуговування та супроводження системи «Клієнт-Банк» протягом 5 робочих днів з дня надання Клієнтом Заявки на підключення / внесення змін в системі «Клієнт-Банк», за формою Додатку 1 до цього Договору (надалі по тексту – **Заявка**).

2.2.2. Виконувати розрахункові операції по рахунку Клієнта у встановлені чинним законодавством та нормативно-правовими актами Національного Банку України строки за умови виконання Клієнтом положень цього Договору.

2.2.3. Приймати та виконувати електронні розрахункові документи Клієнта, що надійшли за допомогою системи «Клієнт-Банк», що відповідають вимогам діючого законодавства та нормативно-правовим актам Національного Банку України.

2.2.4. Надати можливість Клієнту щоденно отримувати інформацію про прийняті і неприйняті електронні розрахункові документи, передані за допомогою системи «Клієнт-Банк», інформацію про зарахування та списання грошових коштів з його рахунків в Банку.

2.2.5. Вести протоколи обміну інформацією та архівації документів у відповідності з прийнятою в Банку технологією і вимогами інструкцій та методичних матеріалів.

2.3. Клієнт має право:

2.3.1. Користуватися системою «Клієнт-Банк» для здійснення розрахункових операцій по поточних рахунках, визначених у Заявці.

2.3.2. Дати Банку вказівку про необхідність підписання платіжних та інших документів від імені Клієнта однією або кількома уповноваженими особами, підписи яких наведені у картці із зразками підписів та відбитка печатки.

2.3.3. Щоденно отримувати інформацію про прийняті і неприйняті електронні розрахункові документи, передані за допомогою системи «Клієнт-Банк», інформацію про зарахування та списання грошових коштів з його поточних рахунків в Банку.

2.3.4. Передавати до Банку розрахункові документи в національній та/або іноземній валюті, заяви на купівлю, продаж та конвертацію іноземної валюти, копії документів в електронній формі та інше як за допомогою системи «Клієнт-Банк» так і на паперових носіях.

2.3.5. В процесі роботи з системою «Клієнт-банк» використовувати додаткові засоби захисту (токени, тощо).

2.3.6. Призупинити обслуговування в системі «Клієнт-Банк» на строк до 30 календарних днів, надавши до Банку відповідний письмовий запит.

2.3.7. Ініціювати припинення обслуговування у системі «Клієнт-Банк» шляхом надання до Банку Заявки на припинення обслуговування в системі «Клієнт-Банк» згідно Додатку 3 Договору.

2.4. Клієнт бере на себе зобов'язання:

2.4.1. Обладнати робоче місце системи "Клієнт-Банк" власною працюючою ПЕОМ (сумісною з IBM PC), з доступом до мережі Internet.

2.4.2. Забезпечити надійне зберігання файлів системи «Клієнт-Банк» та технічного обладнання ЕЦП і засобів захисту.

2.4.3. Виключити доступ до технічних і програмних засобів системи "Клієнт-Банк" сторонніх осіб.

2.4.4. Дотримуватись Рекомендацій клієнтам щодо забезпечення інформаційної безпеки при користуванні системою «Клієнт-банк», наведених у Додатку 4 до цього Договору та розміщені на Інтернет сайті Банку.

2.4.5. Щоденно аналізувати всі повідомлення про прийняті і неприйняті Банком розрахункові документи та іншу інформацію і негайно повідомляти Банк про випадки помилкового зарахування та/або перерахування грошових коштів.

2.4.6. Передавати в Банк електронні розрахункові документи з поточною календарною датою.

2.4.7. Узгоджувати з Банком дії щодо усунення екстремальних та непередбачених ситуацій в системі "Клієнт-Банк".

2.4.8. Щомісячно, не пізніше 14-ого числа (включно) місяця, що слідує за звітним місяцем здійснювати оплату послуг за цим Договором згідно з діючими тарифами Банку на розрахунково-касове обслуговування.

2.4.9. У разі прийняття рішення про припинення обслуговування у системі «Клієнт-Банк»:

– Надати Банку Заявку на припинення обслуговування в системі «Клієнт-Банк» не пізніше ніж за 2 (два) робочих дні до кінця поточного місяця;

– сплатити заборгованість по оплаті обслуговування за системою "Клієнт-Банк" за поточний місяць у повному розмірі.

2.4.10. У разі зміни своєї юридичної, фактичної адреси або інших реквізитів, надати до Банку належним чином засвідчені копії документів протягом 5 (п'яти) робочих днів.

3. Умови встановлення та експлуатації програмно-технічного комплексу електронних платежів «Клієнт-Банк»

3.1. Супроводження системи "Клієнт-Банк" здійснюють уповноважені працівники Банку.

3.2. Для реєстрації та підключення Клієнта в системі «Клієнт – Банк» Клієнт надає до Банку Заявку.

3.3. Банк протягом 5 робочих днів з дня надання Клієнтом Заявки надає Користувачам Клієнта у спосіб, визначений у Заявці, Первинні сертифікати, засоби крипто захисту системи «Клієнт-Банк», інформацію для доступу до системи «Клієнт-Банк», засоби ЕЦП та документацію, що регламентує правила та технологію використання системи «Клієнт-Банк». Підключення Клієнта до системи «Клієнт-Банк» відбувається дистанційно, відповідно до Пам'ятки з підключення до системи «Клієнт-Банк», яка надається Клієнту після підписання цього Договору та консультацій уповноважених працівників Банку. Банк надає Клієнту консультацію по роботі з системою «Клієнт-Банк».

3.4. У разі якщо Користувачем не буде здійснено перший вхід у систему «Клієнт-банк» та генерування нового (робочого) Ключа ЕЦП протягом терміну дії Первинного сертифікату або у разі неможливості використання наданого Банком Первинного сертифікату (втрата, псування тощо) повторне надання Первинного сертифікату здійснюється за умови надання Клієнтом до банку Заявки на повторне надання Первинних сертифікатів до системи «Клієнт-банк» згідно Додатку 2 до цього Договору та сплати комісійної винагороди згідно Тарифів Банку на розрахунково – касове обслуговування.

3.5. Клієнт не має права вносити жодних змін не передбачених наданою Банком документацією до системи «Клієнт-Банк» без письмового дозволу Банку. Зараження програмними "вірусами" або порушення цілісності програмного чи апаратного забезпечення внаслідок недбалого ставлення або некомпетентності співробітників Клієнта, вважається порушенням умов цього Договору.

3.6.Сторони домовились, що передані Клієнту згідно цього Договору засоби та друковані матеріали вважаються такими, що містять конфіденційну та/або таємну інформацію, та суворе збереження їх секретності має бути забезпечене в повній мірі. В зв'язку з цим, всі співробітники Клієнта, які мають до них доступ, повинні поводитись з такою інформацією з належною увагою та не допускати її розголошення або копіювання у будь-якому вигляді.

3.7. Банк має право здійснювати перевірки робочих місць/приміщень Клієнта на предмет виконання ним вимог захисту інформації та зберігання засобів захисту і припиняти обслуговування Клієнта в разі невиконання ним вимог безпеки.

3.8. Зміна/доповнення/видалення Користувачів системи "Клієнт-Банк" та/або зміна рівня доступів Користувачів до системи «Клієнт-Банк» та/або зміни переліку рахунків Клієнта / замовлення додаткових послуг, визначених у Заявці, відбувається після подання Клієнтом до Банку нової Заявки. При цьому Клієнт сплачує Банку комісію згідно з діючими тарифами Банку на розрахунково-касове обслуговування.

3.9. Якщо Користувачем клієнта протягом одного календарного року не було здійснено входу до системи «Клієнт-Банк», Банк має право здійснити блокування Облікового запису такого Користувача в системі. Відновлення права доступу здійснюється Банком на підставі наданої Клієнтом до Банку Заявки, відповідно до пункту 3.8. цього Договору, шляхом реєстрації нового Облікового запису та повторного надання Первинних сертифікатів.

3.10. Припинення обслуговування Клієнта у системі «Клієнт-Банк» здійснюється:

3.10.1. За ініціативою Клієнта – шляхом надання до Банку Заявки на припинення обслуговування в системі «Клієнт-Банк» згідно Додатку 3 до Договору не пізніше ніж за 2 (два) робочих дні до кінця поточного місяця та сплати заборгованості по оплаті обслуговування за системою "Клієнт-Банк" за поточний місяць у повному обсязі. Обслуговування Клієнта у системі «Клієнт-Банк» припиняється протягом 1 (одного) робочого дня з моменту надання до Банку Заявки на припинення обслуговування в системі «Клієнт-Банк».

3.10.2. За ініціативою Банку – за умови непогашення Клієнтом заборгованості по оплаті обслуговування за системою "Клієнт-Банк" в строк до 25 числа (включно) місяця, що слідує за звітним місяцем, припиняється обслуговування Клієнта в системі "Клієнт-Банк" і Договір вважається таким, що припиняє чинність. Обслуговування Клієнта у системі «Клієнт-Банк» припиняється з наступного робочого дня. У такому разі для поновлення обслуговування у системі «Клієнт-Банк» Клієнтові необхідно укласти новий договір.

3.10.3. У разі закриття рахунків Клієнта за ініціативою Банку відповідно до умов Договору банківського рахунку та чинного законодавства, Договір вважається таким, що втратив чинність з дати закриття останнього рахунку Клієнта.

4. Умови використання ЕЦП та крипто захисту.

Банк

_____

М.П.

Клієнт

_____

М.П.

4.1. До виконання приймаються електронні розрахункові документи, що містять ЕЦП та зашифровані відповідно до програмного забезпечення, встановленого Банком.
4.2. Електронні розрахункові документи передані до Банку за допомогою системи “Клієнт-Банк” та підписані ЕЦП, розглядаються як такі, що мають юридичну силу нарівні з паперовими розрахунковими документами, що містять відбиток печатки (за наявності) та підписи відповідальних осіб Клієнта.
4.3. Клієнт зобов'язується забезпечити збереження технічних носіїв ЕЦП з метою уникнення їх псування, втрати, використання сторонніми особами.
4.4. Передача технічних носіїв ЕЦП (або їх заміна) здійснюється Банком лише відповідальним особам Клієнта, які вповноважені розпоряджатися рахунками Клієнта і зразки підписів яких заявлені Банку в картці із зразками підписів та відбитка печатки та уповноваженим особам Клієнта, визначеним у Заявці .
4.5. Сторона, яка втратила контроль за використанням технічних носіїв ЕЦП, незалежно від наявності чи відсутності відомостей про їх несанкціоноване використання, терміново сповіщає про це іншу Сторону.
4.6. Сторони, виходячи з вимог п. 4.3. цього Договору, встановили, що відповідальність за належне оформлення документів за допомогою ЕЦП цілком покладається на Клієнта. Сторони також домовились, що у випадку встановлення фіктивності оформленого за допомогою ЕЦП документа, збитки, заподіяні одній із Сторін Договору або третім особам в результаті здійсненої на підставі такого фіктивного документа, операції, підлягають відшкодуванню за рахунок Сторони, від імені якої було оформлено цей документ.
4.7. У разі зміни осіб, яким надано право підпису розрахункових документів, а також при зміні своєї адреси, Клієнт зобов’язаний повідомити про це Банк з наданням відповідних документів не пізніше трьох робочих днів з дня виникнення таких змін.

5. Умови та порядок розрахунків

5.1. Плата за ведення рахунку в системі “Клієнт-Банк” сплачується Клієнтом відповідно до Тарифів Банку на розрахунково-касове обслуговування, починаючи з дня підписання цього Договору і не залежить від кількості та суми виконаних операцій за рахунками Клієнта.
5.2. Оплата Клієнтом послуг в системі “Клієнт-Банк” за цим Договором здійснюється згідно з діючими тарифами Банку на розрахунково-касове обслуговування шляхом проведення договірного списання коштів з рахунків Клієнта в АТ «АП БАНК» , код банку **380548**, на свою користь в оплату послуг за цим Договором.
5.3. Якщо граничні строки сплати Клієнтом заборгованості по оплаті обслуговування за системою “Клієнт-Банк”, зазначені у п.2.1.6 цього Договору припадають на неробочий день, заборгованість по оплаті обслуговування за системою “Клієнт-Банк” в такому разі сплачується в попередній робочий день.

6. Відповідальність Сторін

6.1. Клієнт несе відповідальність за випадки помилкового формування та подання паперових та електронних розрахункових документів, що тягне за собою подвійне списання коштів з рахунку Клієнта.

6.2. Банк не несе відповідальності за:

6.2.1. Невикористання Клієнтом послуг, що обумовлюються цим Договором.
6.2.2. Несправності та дефекти обладнання Клієнта або неправильне використання чи експлуатацію цього обладнання та системи “Клієнт-Банк”.
6.2.3. Надійність функціонування мережі Internet та доступу до неї.

7. Форс-мажор

7.1. Сторони звільняються від відповідальності за повне або часткове невиконання будь-якого з положень цього Договору, якщо це невиконання сталося внаслідок причин, які знаходяться поза сферою контролю Сторін. Такі причини включають стихійні лиха, екстремальні погодні умови, пожежі, війни, страйки, воєнні дії, дії компетентних державних органів, а також перебої, затримки або відключення (часткові або повні) електричної енергії чи комп’ютера (апаратного або програмного забезпечення) або засобів зв’язку (далі “форс-мажор”). Період звільнення від відповідальності починається з моменту оголошення “форс-мажору” Стороною, яка не виконує своїх обов’язків, та закінчується після виходу з “форс-мажору” та ліквідації його наслідків. “Форс-мажор” автоматично продовжує термін виконання зобов’язань на весь період його дії та ліквідації наслідків.

8. Строк дії Договору, заключні умови

8.1. Договір укладений на невизначений строк та набуває чинності з дня його підписання уповноваженими на це особами сторін. Дія Договору припиняється за згодою сторін або у випадках, передбачених чинним законодавством України та цим Договором.
8.2. Будь-які зміни і доповнення до цього Договору оформляються шляхом укладення договорів про внесення змін та доповнень до цього Договору, які підписуються кожною із Сторін.
8.3. Банк є платником податків на загальних умовах, передбачених Податковим Кодексом України.
8.4. Клієнт зазначає, що він є платником податків _____ _____ *(вказати платником якого податку є клієнт згідно з чинним законодавством та зазначити відповідний нормативний акт).*
8.5. У всьому, що не передбачено умовами цього Договору, Сторони керуються чинним законодавством.
8.6. Спори, що виникають протягом дії Договору, вирішуються шляхом переговорів. У разі недосягнення згоди – в судовому порядку згідно з чинним законодавством України.
8.7. Цей Договір складено у двох примірниках, по одному для кожної із Сторін. При цьому обидва примірники мають однакову юридичну силу.
8.8. Клієнт підтверджує, що ознайомлений та згодний з діючими тарифами Банку на розрахунково-касове обслуговування.
8.9. Всі додатки до цього Договору є його невід’ємною частиною.
8.9.1. Додаток 1 – Заявка на підключення / внесення змін в системі «Клієнт-Банк».
8.9.2. Додаток 2 – Заявка на повторне надання Первинних сертифікатів до системи «Клієнт-Банк».
8.9.3. Додаток 3 – Заявка на припинення обслуговування в системі «Клієнт-Банк».
8.9.4 Додаток 4 **-** Рекомендації клієнтам щодо забезпечення інформаційної безпеки при користуванні системою «Клієнт-банк».

9. Юридичні адреси та реквізити сторін

Сторона 1. Банк		**Сторона 2. Клієнт**
Назва Банку:	АКЦІОНЕРНЕ ТОВАРИСТВО «АГРОПРОСПЕРІС БАНК»	**Назва:**
Юридична адреса банку:	04119 м. Київ, вул. Дегтярівська 27-Т (Літера А)	**Юридична адреса:**
код банку:	380548	**Фактична адреса:**
Код за ЄДРПОУ:	35590956	**Код за ЄДРПОУ / Реєстраційний номер облікової картки платника податків:**
К/р:	к/р 32000118501026 в Національному банку України	
Установа банку:		**Тел.:**
Адреса установи банку:		
Посада:		**Посада:**
_____ (підпис) М.П.		_____ (підпис) М.П.

Примірник Договору отримав _____( )
підпис (ПІБ)

Банк
_____
М.П.

Клієнт
_____
М.П.

Додаток 1
до Договору №
про надання розрахункових послуг в системі "Клієнт-Банк"
від

Заявка на підключення / внесення змін в системі «Клієнт-Банк»
(необхідне підкреслити)

Дата заповнення:

РЕЄСТРАЦІЙНІ ДАНІ КЛІЄНТА	
Найменування (скорочене)/П.І.Б	
Код ЄДРПОУ/Реєстраційний номер платника податків	
Фактична адреса	
Номери телефонів / e-mail	

Контактна інформація відповідальної за встановлення системи «Клієнт-банк» особи Клієнта:

П.І.Б (з розшифруванням ініціалів)	**Номери телефонів**	**Адреса e-mail**

Просимо виконати наступні налаштування у системі «Клієнт-Банк»:

☐ первинне підключення (пункти 1, 2, 3);
☐ додаткова реєстрація/зміна прав/видалення Користувачів (пункт 2);
☐ зміна/доповнення/видалення рахунків (пункт 1);
☐ зміна / доповнення переліку IP – адрес (пункт 3);

1. Надати доступ до рахунків, вказаних у переліку, з наступними правами:

№ з/п	**Аналітичний номер рахунку/ Валюта**
1	
2	
3	
4	
5	

2. Зареєструвати / видалити Користувачів / змінити права Користувачів, вказаних у переліку, з наступними правами:

№ з/п	**П.І.Б** (з розшифруванням ініціалів)	**Посада**	**Реєстрація[1]/ зміна прав/ видалення** *(вказав необхідне)*	**Рахунки** *(вказується, якщо користувач має права на окремі рахунки)*	**Адреса e-mail / моб. тел.**	**Роль[2]**	**Тип носія[3]**	**Підключення до системи генерації одноразових паролів (використання OTP токена)[4]** *(+)*
1								
2								
3								
4								

Карта прав доступу

№ з/п	**Право**	**Опис права**	**Ролі Користувачів**					
			«D+B» Директор + Бухгалтер	**«D» Директор**	**«B» Бухгалтер**	**«P» Виконавець без права підпису**	**«R» Перегляд Інформації по рахунках**	**«A» Авторизаційний підпис**
1	Право двох підписів		●					
2	Право першого підпису			●				
3	Право другого підпису				●			
4	Право третього підпису							●
5	Вхід в систему	Дозволяє входити в систему	●	●	●	●	●	●
6	Робота з гривневими документами	Дозволяє створення платіжних доручень у нац. валюті та відправку їх у банк, в т.ч. у неробочий час.	●	●	●	●		●

[1] У разі надання тимчасового права доступу, додатково зазначається період з ___ по ____.
[2] Права доступу Користувачів до ресурсів системи; визначається на основі Карти прав доступу.
[3] Носій на який відбувається запис Первинних сертифікатів: «Т» - Токен (надається Банком згідно Тарифів), «Р» - надсилання архіву з Первинним сертифікатом на електронну пошту Користувача. Пароль до архіву надсилається на номер мобільний номер телефону відповідальної за встановлення системи «Клієнт-банк» особи Клієнта, визначений у цій заявці.
[4] Видача OTP токена Користувачу здійснюється за умови сплати Клієнтом комісійної винагороди згідно Тарифів.

Банк
_____
М.П.

Клієнт
_____
М.П.

7	Робота з валютними документами	Дозволяє створення платіжних доручень у іноземній валюті, в т.ч. валютних заявок на купівлю, продаж, конверсію та відправку їх у банк, в т.ч. у неробочий час	●	●	●	●		●
8	Перегляд інформації по кредитах	Надає право на перегляд інформації по кредитних угодах	●	●	●	●		
9	Перегляд інформації по депозитах	Надає право на перегляд інформації по депозитних угодах	●	●	●	●		
10	Робота з консоллю WEB-клієнта	Дозволяє працювати з консоллю WEB- клієнта	●	●	●	●	●	●
11	Робота з Win32 інтерфейсом	Дозволяє роботу з Win32 версією системи	●	●	●	●	●	●
12	Прийом документів за майбутню дату	Дозволяє відправку платіжних доручень у банк за майбутню дату	●	●	●	●	●	●

3. Дозволити доступ Користувачів до системи «Клієнт-Банк» лише з вказаних у переліку IP-адрес[5]:

Роль	**Дозволені IP-адреси (xxx.xxx.xxx.xxx)**		
D			
B			
A			

Клієнт погоджується з тим, що розуміє всі ризики та бере на себе повну відповідальність за забезпечення безпеки рахунків (Банк звільняється від відповідальності), у разі:

- не зазначення Клієнтом у пункті 3 дозволеної IP - адреси, з якої (яких) можливий доступ Користувачів до системи «Клієнт – Банк»;
- обрання Клієнтом у пункті 2 типу носія «Р» - надсилання архіву з Первинним сертифікатом на електронну пошту Користувача;
- відмови Клієнта від використання OTP токена.

_____ / /
(Підпис) (П.І.Б.)

М.П.

_____ / /
(Підпис) (П.І.Б.)

Відмітка Банку:
Заявку прийнято до виконання
Дата: «____»._____.20___р.
Відповідальний працівник: _____ _____
(П.І.Б.) (Підпис)

[5] Статична зовнішня IP- адреса, що надана постачальником послуг Інтернет (заповнюється в разі потреби).

Банк _____ М.П.

Клієнт _____ М.П.

Додаток 2
до Договору №
про надання розрахункових послуг в системі “Клієнт-Банк”
від

Заявка

на повторне надання Первинних сертифікатів до системи «Клієнт-банк»

Дата заповнення: «____» _____ 20___ р.

РЕЄСТРАЦІЙНІ ДАНІ КЛІЄНТА	
Найменування (скорочене)/П.І.Б	
Код ЄДРПОУ/Реєстраційний номер платника податків ФОП	

Прошу повторно надати Первинні сертифікати для наступних Користувачів, що зареєстровані у системі «Клієнт-банк»:

№ з/п	**ПІБ** (з розшифруванням ініціалів)	**Посада**	**Ідентифікатор користувача**

Керівник _____ /_____/
(Підпис) (П.І.Б.)
М.П.

Відмітка Банку:
Заявку прийнято до виконання
Дата: «____».____.20___р.
Відповідальний працівник: _____ _____
(П.І.Б.) (Підпис)

Банк
_____
М.П.

Клієнт
_____
М.П.

Додаток 3
до Договору №
про надання розрахункових послуг в системі “Клієнт-Банк”
від

Заявка

на припинення обслуговування в системі «Клієнт-Банк»

Дата заповнення: «_____» _____ 20___ р.

РЕЄСТРАЦІЙНІ ДАНІ КЛІЄНТА	
Найменування (скорочене)/П.І.Б	
Код ЄДРПОУ/Реєстраційний номер платника податків ФОП	

Прошу зупинити обслуговування та відключити від системи «Клієнт-Банк», з дати:

Дата відключення від системи
«____» _____ 20___ р.

Керівник _____ /_____/
(Підпис) (П.І.Б.)

М.П.

Банк
_____
М.П.

Клієнт
_____
М.П.

Додаток 4
до Договору
про надання розрахункових послуг в системі "Клієнт-Банк"
від

Рекомендації клієнтам щодо забезпечення
інформаційної безпеки при користуванні системою «Клієнт-банк»

Терміни та визначення:

Система «Клієнт-Банк» –система дистанційного банківського «Клієнт-банк»».
Клієнтська частина системи «Клієнт-Банк» – сукупність комп'ютерного обладнання Клієнта (персональний комп'ютер, ноутбук, планшет тощо), а також спеціалізованого програмного забезпечення (далі – ПЗ), що надає можливість дистанційного обслуговування на стороні Клієнта (ПЗ, що надано Банком, а також стандартне ПЗ Клієнта (наприклад, веб-браузер).
Веб-браузер – ПЗ, що надає можливість користувачу в мережі Інтернет переглядати текстову інформацію, малюнки, посилання на інші сайти, тощо на веб-сторінках.
Відкритий ключ ЕЦП – це криптографічний ключ (дані, інформація), який отримано математичним обчисленням та який являється відкритою інформацією для перевірки ЕЦП користувача.
ЕЦП - електронний цифровий підпис.
Закритий (секретний) ключ ЕЦП – це криптографічний ключ, що зв'язаний із відкритим ключем спеціальним математичним співвідношенням, та являється таємною інформацією, за допомого якої накладається ЕЦП користувача.
Сертифікат (сертифікат ключа, сертифікат відкритого ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа особі, яка володіє відповідним особистим ключем. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документів на папері та використовуватися для ідентифікації особи власника відповідного особистого ключа.
Ключ ЕЦП - призначений для підписання (накладання ЕЦП) документів та повідомлень, які Клієнт надсилає засобами системи «Клієнт-банк» у Банк. Ключ складається з відкритої (публічної) та закритої частини. Відкрита частина відома Банку та зафіксована на паперовому носії (у вигляді геш-коду) в документі «Інформація про відкриті ключі користувача (запит)», закрита частина зберігається виключно на електронному носії у Клієнта. Під час накладання ЕЦП Клієнтом – використовується закрита частина Ключа ЕЦП. Відкрита частина використовується для перевірки достовірності підпису на документах та повідомленнях, під час приймання їх Банком. Даний механізм забезпечує ідентифікацію особи, що наклала особистий підпис та захист документів і повідомлень від підробки, під час передачі їх каналами зв'язку від Клієнта до Банку засобами системи «Клієнт – банк».
Токен - захищений носій ключової інформації, сертифікований відповідно до державних стандартів захисту інформації. Призначений для зберігання Ключів ЕЦП Користувачів.
OTP (one time password) токен – пристрій, призначений для генерації одноразових паролів з метою додаткової авторизації Користувача в системі «Клієнт-банк».
Персональний мережевий екран (файєрвол, брандмауер) – система, встановлена на комп'ютері користувача, та призначена для захисту від несанкціонованого доступу до його комп'ютера.
Веб-сервер – сервер (спеціалізоване ПЗ), що приймає специфічні запити від веб-браузерів клієнтів, видає їм відповіді, зазвичай разом із інтернет-сторінкою, зображенням, файлом, медіа-потоком або іншими даними.
Антишпигунське ПЗ – програмне забезпечення, що виявляє та знешкоджує шкідливі програми, які збирають інформацію про дії користувача та передають її зловмиснику.
Сигнатури вірусу - характерні ознаки комп'ютерного вірусу, що використовуються для його виявлення.
Сигнатури шпигунського ПЗ - характерні ознаки шпигунського програмного забезпечення, що використовуються для його виявлення.
Антивірусні бази даних – бази даних, у яких зберігаються сигнатури вірусів.
Бази сигнатур антишпигунського ПЗ – бази даних, у яких зберігаються сигнатури шпигунського програмного забезпечення.
Обліковий запис – спеціальна одиниця інформації про Клієнта Банку у системі «Клієнт – банк».
.

Базові рекомендації Клієнту щодо забезпечення захисту клієнтської частини системи «Клієнт-Банк»

- Під час роботи у системі «Клієнт-Банк» (далі Система) не залишайте комп'ютер без нагляду.

1. Для запобігання несанкціонованого доступу до конфіденційної інформації не повідомляйте свої авторизаційні дані у Системі (логін, пароль, секретний ключ ЕЦП, пароль на секретний ключ ЕЦП) третім особам (включаючи членів родини, друзів і т.д.).

- Рекомендується зберігати особистий сертифікат і секретний ключ ЕЦП на зовнішньому носії інформації (диск, накопичувачі із флеш-пам'яттю (USB-токени, флешки) та ін.), а не на комп'ютері. Зберігання даної інформації на зовнішніх носіях забезпечує додатковий захист конфіденційної інформації клієнта в Системі та забезпечує цілість сертифікатів і секретних ключів ЕЦП у разі виникнення раптових проблем, збоїв у роботі комп'ютера Клієнта.

- Для максимального захисту конфіденційної інформації (особистий сертифікат, секретний ключ ЕЦП) рекомендується використовувати зовнішній носій інформації із захищеною пам'яттю (що унеможливлює несанкціоновану модифікацію даних, збережених на носії), наприклад, спеціалізований USB-токен, тощо.

- При використанні паролів не рекомендується зберігати паролі, взагалі, в будь-якому місці (на папері, на комп'ютері, на флеш-носіях, дискетах тощо). Пароль рекомендується запам'ятати!

- При використанні зовнішнього носія інформації з особистим сертифікатом та секретним ключем ЕЦП на ньому не зберігайте даний носій інформації разом із логіном та паролями Системи (якщо клієнтом було прийнято рішення не запам'ятовувати, а зберігати паролі).

- Рекомендується завжди вилучати із комп'ютера зовнішній носій інформації по завершенню роботи в Системі.

- Підключення до Системи необхідно здійснювати тільки з надійних комп'ютерів, на яких встановлено антивірусне ПЗ та програмний персональний мережний екран.

- При вході до Системи необхідно впевнитись, що в адресному полі веб-браузера знаходиться адреса саме Системи Банку (наприклад, https://cb.ap-bank.com/ifobsClient/LoginShow.action).

- При підключенні до Системи необхідно перевірити, чи ввімкнено шифрування між клієнтським комп'ютером та веб-сервером Банка. Про ввімкнене шифрування свідчить наявність піктограми  «Замок» у вікні браузера (справа від адресного поля браузера).

- Підтвердженням того, що між веб-браузером клієнта та веб-сервером Банку встановлено безпечне з'єднання, є наявність цифрового (електронного) сертифікату Банку. Рекомендується перевірити дійсність сертифікату та термін його дії.

- Після відкриття сесії роботи в Системі у веб-браузері перевіряйте дату останнього свого входу до системи та відстежуйте історію своїх операцій в Системі.

- Після завершення роботи у Системі необхідно закрити сесію, натиснувши піктограму «Вихід», та закрити вікно веб-браузера.

- Не рекомендується переглядати інші сайти в тому ж веб-браузері, в якому запущена Система.

- Рекомендується звертати увагу на можливі повідомлення веб-браузера про будь-яку небезпеку. У разі виникнення будь-якої підозри

Банк
_____
М.П.

Клієнт
_____
М.П.

рекомендується завершити роботу із Системою та закрити сесію.

- Банк надсилає Клієнту первинні сертифікати тільки авторизованою електронною поштою cb@ap-bank.com. Не використовуйте будь-яку інформацію (ключі та сертифікати тощо) у Системі, вислану з інших електронних поштових адрес, навіть якщо вони схожі за назвою із авторизованою банківською електронною адресою (без попереднього офіційного повідомлення та погодження з боку Банку).

- Не відповідайте на запити (найчастіше запити розсилаються через SMS-повідомлення засобами мобільного зв'язку, електронною поштою тощо), які містять вимогу надати або перевірити логін, пароль, секретний ключ ЕЦП тощо.

- Банк, без попереднього офіційного повідомлення та погодження із Клієнтом, за жодних обставин не здійснює розсилку із:

○ Запитами на отримання персональних даних (паролів) Клієнта;

○ Додатковим ПЗ для Системи;

○ Посиланнями на інші сайти із необхідністю завантажити додаткове ПЗ Системи тощо.

- Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих адресатів із прикріпленими файлами, що мають розширення
*.exe, *.com, *.zip, *.rar, *.bat, *.jpeg, *.pif, *.vbs та інші файли, так як існує значна ймовірність зараження комп'ютера вірусами та/чи іншим зловмисним ПЗ.

Рекомендації щодо забезпечення захисту комп'ютера Клієнта

- Рекомендується, щоб комп'ютер (персональний комп'ютер, ноутбук, планшет тощо) Клієнта, який використовується для роботи в Системі, мав:

○ Ліцензійну операційну систему, яка отримує оновлення;

○ Встановлену останню доступну версію веб-браузера;

○ Програмне забезпечення захисту, що складається із ліцензійної антивірусної системи, антишпигунського ПЗ («antispyware») та програмного персонального мережевого екрану.

- На комп'ютері із встановленою операційною системою Windows рекомендується активувати функцію автоматичного оновлення операційної системи.

- Рекомендується постійно оновлювати антивірусні бази даних та бази сигнатур антишпигунського ПЗ.

- Рекомендується регулярно (не рідше, ніж раз на тиждень) здійснювати повне сканування комп'ютера за допомогою антивірусного, антишпигунського ПЗ для виявлення вірусів та зловмисного ПЗ (вірусів, шпигунських програм тощо).

- У разі виявлення на комп'ютері будь-якого зловмисного ПЗ рекомендується не заходити з цього комп'ютера у Систему до повного видалення даного зловмисного ПЗ із комп'ютера. Наступний вхід до Системи обов'язково виконується із гарантовано незараженого комп'ютера, при цьому необхідно якнайшвидше змінити пароль доступу до Системи, а також пароль секретного ключа ЕЦП.

- Не рекомендується встановлювати на комп'ютер будь-яке неліцензійне ПЗ.

- Не рекомендується встановлювати на комп'ютер ПЗ із ненадійних джерел (наприклад, програмне забезпечення із невідомих повідомлень електронної пошти, файлових ресурсів (наприклад, FEX.NET) із невідомих посилань на сайтах в Інтернет, що відвідуються Клієнтом тощо).

Рекомендації щодо використання безпечних паролів

- При введенні паролю на доступ до Системи або паролю до секретного ключа ЕЦП переконайтесь, що за Вами ніхто не спостерігає.

- Рекомендується обмежити доступ сторонніх осіб до мобільного телефону Клієнта, на який надходить SMS із первинним паролем доступу до Системи.

- Перед тим, як змінити пароль, перевірте сертифікат безпеки банківського веб-сервера.

- Не використовуйте функцію збереження паролів, яку може запропонувати веб-браузер.

- Для забезпечення найвищого рівня інформаційної безпеки при використанні паролів не рекомендується зберігати паролі, взагалі, в будь-якому місці (на папері, на комп'ютері, на флеш-носіях, дискетах тощо). Пароль рекомендується запам'ятати.

- За умови прийнятого рішення збоку Клієнта щодо збереження паролів, рекомендується зберігати паролі у недоступному для інших місці.

- За умови прийнятого рішення збоку Клієнта щодо збереження паролів, рекомендується зберігайте пароль на доступ до Системи та пароль до секретного ключа ЕЦП окремо.

- Паролі Системи не повинні містити словникові слова або ім'я, пов'язані з клієнтом (ім'я, прізвище, ім'я дружини, дітей, домашніх улюбленців тощо), не містити очевидних послідовностей символів (наприклад, abcdEF, Qwertyu тощо).

- Рекомендовані вимоги до створення та використання паролів:

○ мінімум 8 символів, мінімум 1 мала та 1 велика літери, мінімум 1 цифра та мінімум 1 спеціальний знак (наприклад, «*», «_» , «-», «!», «+» тощо);

○ 4-ри останні паролі не повинні співпадати;

○ термін дії паролю – 90 днів.

Ризики і відповідальність

Клієнт, що використовує Систему, погоджується з тим, що розуміє всі ризики (звільняє Банк від відповідальності), пов'язані із розголошенням конфіденційної інформації (з провини Клієнта) в рамках використання Системи (логін, пароль, секретний ключ ЕЦП, пароль на секретний ключ ЕЦП тощо), номеру його мобільного телефону (на який надсилається первинний пароль на вхід до Системи), будь-якої інформації, що є банківською таємницею (про свої рахунки, тощо), ризики при здійсненні доступу до Системи не з власного комп'ютера та несе повну відповідальність за такі випадки.
Клієнт погоджується з тим, що розуміє всі ризики та несе повну відповідальність (звільняє Банк від відповідальності), пов'язану із здійсненням доступу до Системи через комп'ютер:

- на який не встановлено актуальне ПЗ антивірусного та мережного захисту (антивірусна система, антишпигунське програмне забезпечення та програмний персональний мережний екран);

- на якому встановлено ПЗ антивірусного та мережного захисту, що не оновлюється або оновлюється нерегулярно;

- на якому встановлено неліцензійне ПЗ (включаючи операційну систему);

- на якому відсутні оновлення безпеки операційної системи;

- на якому відсутнє розмежування доступу (доступ до операційної системи комп'ютера відбувається без паролю, використовується єдиний обліковий запис (наприклад, administrator, office, user, dom тощо) для будь-яких користувачів комп'ютера);

- із якого відбувається доступ в Інтернет до сайтів неналежного змісту (порнографічного характеру, ігрові та розважальні сайти, хакерські форуми тощо), на яких досить вірогідне зараження вірусним, шпигунським та іншим зловмисним ПЗ.

Банк

_____

М.П.

Клієнт

_____

М.П.

ПОРЯДОК ДІЙ В ЕКСТРЕМАЛЬНИХ ТА НЕПЕРЕДБАЧЕНИХ СИТУАЦІЯХ

Клієнт Банку, який користується послугами системи «Клієнт-Банк», зобов'язаний припинити використання секретного ключа (ТК) та негайно інформувати адміністратора системи захисту інформації СКБ за допомогою телефона (044) 392-93-79 та електронної пошти cb@ap-bank.com в таких випадках:

- несанкціоноване зняття коштів з рахунків;
- виконання (спроби виконання) фіктивного платіжного документа;
- компрометація таємного ключа (ТК) системи «Клієнт-Банк»;
- втрата контролю над OTP токеном (за наявності).

Банк

_____

М.П.

Клієнт

_____

М.П.