Затверджено
Протокол засідання Правління
публічного акціонерного товариства
"Розрахунковий центр з обслуговування
договорів на фінансових ринках"
07.10.2013 р. №43

Викладено у новій редакції
Протокол засідання Правління
публічного акціонерного товариства
"Розрахунковий центр з обслуговування
договорів на фінансових ринках"
05.12.2017 р. №58

Положення
про Систему дистанційного обслуговування клірингових рахунків / субрахунків "Інтернет-кліринг" публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках"

1. Загальні положення

1.1. Терміни, які вживаються в Положенні про Систему дистанційного обслуговування клірингових рахунків / субрахунків "Інтернет-кліринг" публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Положення):

- **відкритий ключ** – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;
- **блокування доступу Користувача до Системи** – дії Розрахункового центру внаслідок яких унеможливлюється доступ Користувача до Системи;
- **блокування сертифіката ключа** – тимчасове зупинення чинності сертифіката ключа;
- **електронний документ (ЕД) –** документ, в якому інформація зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа;
- **електронні розпорядження –** електронний документ, який сформований та відправлений Клієнтом до Розрахункового центру за допомогою Системи дистанційного обслуговування клірингових рахунків / субрахунків "Інтернет-кліринг", який містить розпорядження Клієнта щодо здійснення операцій по кліринговим рахункам / субрахункам;
- **електронний цифровий підпис (далі – ЕЦП)** – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. ЕЦП накладається за допомогою особистого ключа і перевіряється за допомогою відкритого ключа;
- **компрометація особистого ключа** – будь-яка подія та / або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;
- **Клієнт** – юридична особа, яка уклала з Розрахунковим центром договір про обслуговування в Системі дистанційного обслуговування клірингових рахунків / субрахунків "Інтернет-кліринг";
- **Користувач (в множині Користувачі) –** фізичні особи, уповноважені Клієнтом розпоряджатися Рахунком / Рахунками Клієнта і підписувати електронні розпорядження;

- **особистий ключ –** параметр криптографічного алгоритму формування ЕЦП, доступний тільки користувачу ЕЦП. Особистий ключ працює тільки в парі з відкритим ключем;
- **поновлення сертифіката ключа** – відновлення чинності попередньо заблокованого сертифіката ключа;
- **Рахунок / Рахунки** – клірінговий рахунок або субрахунок Клієнта в Розрахунковому центрі;
- **Розрахунковий центр –** публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках";
- **Система дистанційного обслуговування клірингових рахунків / субрахунків "Інтернет-кліринг" публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках (далі – Система)** – сукупність технічних засобів та програмного забезпечення, впровадженого в Розрахунковому центрі, що дозволяють Клієнту дистанційно отримувати інформацію по Рахунках та здійснювати розрахункові операції по Рахунку / Рахунках на підставі електронних розрахункових документів Клієнта, а також отримувати інші послуги в порядку та на умовах, передбачених договором про обслуговування в системі інтернет-клірингу, укладеним між Розрахунковим центром та Клієнтом;
- **скасування сертифіката ключа** – припинення чинності сертифіката ключа.

Інші терміни, що вживаються в цьому Положенні, використовуються відповідно до законодавства України.

1.2. Положення визначає загальний порядок обігу електронних документів між Розрахунковим центром та Клієнтом при роботі за допомогою Системи, умови допуску та порядок підключення Клієнта до Системи, порядок отримання від Розрахункового центру особистих ключів, порядок дії при компрометації особистих ключів Клієнта.

2. Обіг електронних документів

2.1. Формування електронних документів Клієнтом здійснюється за допомогою програмних засобів, наданих Клієнту Розрахунковим центром.

2.2. Електронні документи, що надходять від Клієнта до Розрахункового центру, повинні містити реквізити, встановлені внутрішніми документами Розрахункового центру.

2.3. Юридична сила ЕД забезпечується накладенням ЕЦП Користувача відповідно до вимог цього Положення. Для накладення ЕЦП Користувача використовується особистий ключ.

2.4. В Розрахунковому центрі перевіряється ЕЦП ЕД і правильність заповнення реквізитів ЕД. У разі позитивного результату контролю ЕД такий ЕД виконується. У разі негативного результату контролю ЕД такий ЕД не виконується Розрахунковим центром. Розрахунковий центр повідомляє про це Клієнта засобами Системи із зазначенням причин відмови прийняти документ до виконання.

2.5. Розрахунковий центр протягом операційного дня обробляє ЕД, що надійшли від Клієнтів. У разі відмови Розрахунковим центром від виконання ЕД Клієнта, надісланого засобами Системи, Розрахунковий центр повідомляє про це Клієнта засобами Системи із зазначенням причин відмови прийняти такий ЕД до виконання.

2.6. Електронні розпорядження Клієнта повинні містити:

- один ЕЦП Користувача та
- один ЕЦП печатки Клієнта (в разі наявності відбитка печатки Клієнта в картці зі зразками підписів розпорядників клірингового рахунку (рахунків) Клієнта) або один ключ ідентифікатора Клієнта (в разі відсутності відбитка печатки Клієнта в

картці зі зразками підписів розпорядників клірингового рахунку (рахунків) Клієнта).

3. Одержання додаткової інформації

Клієнт за допомогою Системи може отримати наступну інформацію:

- поточний стан Рахунку / Рахунків;
- поточний статус ЕД;
- поточний статус ЕД в складі операції за Рахунком / Рахунками;
- виписка про стан та операції за Рахунком / Рахунками;
- відомості проведених розпоряджень та розпоряджень, що виконуються, за Рахунком / Рахунками;
- перелік записів про обмін інформаційними повідомленнями та їх зміст.

4. Підключення до Системи

4.1. Підключення до Системи можливе після виконання Клієнтом таких умов:

4.1.1. Укладення з Розрахунковим центром договору про клірингове обслуговування та договору про обслуговування в системі інтернет-клірингу;

4.1.2. У разі, якщо Клієнту необхідно отримати від Розрахункового центру в користування носій ключової інформації "Secure Token 337" – оплата Клієнтом заставної вартості носія ключової інформації відповідно до умов договору про обслуговування в системі інтернет-кліринг і його отримання від Розрахункового центру. Підтвердженням надання Клієнту носія ключової інформації є Акт прийому-передачі носія ключової інформації (Додаток 6).

4.1.3. Надання Розрахунковому центру заяви на підключення до Системи (Додаток 1);

4.1.4. Надання Розрахунковому центру заяви на засвідчення та реєстрацію відкритого ключа (Додаток 2);

4.1.5. Налаштування робочого місця Клієнта відповідно вимог до програмно-технічного забезпечення Клієнтів (Додаток 5);

4.1.6. Підписання Акту про підключення до Системи між Розрахунковим центром та Клієнтом (Додаток 4).

5. Вимоги до ЕЦП Клієнта

5.1. В Системі для генерації та зберігання ключів ЕЦП Користувача та ЕЦП печатки Клієнта/ключа ідентифікатора Клієнта застосовуються носії ключової інформації "Secure Token 318" виробництва ТОВ "Автор" (ЄДРПОУ 32248356).

При їх відсутності можливе використання програмних носіїв "Token", які записуються на флеш-накопичувач.

5.2. Для забезпечення обов’язкового шифрування каналу зв’язку між Розрахунковим центром та Клієнтом використовується ключ шифрування, який записується виключно на захищений носій ключової інформації "Secure Token 337" виробництва ТОВ "Автор" (ЄДРПОУ 32248356).

5.3. Носій ключової інформації "Secure Token 337" придбавається Клієнтом самостійно або надаються Клієнту в користування Розрахунковим центром відповідно до умов договору про обслуговування в системі інтернет-кліринг. В разі необхідності отримання в користування носія ключової інформації Клієнт зазначає про це в заявці на укладення

договору про обслуговування в системі інтернет-кліринг, розміщеній на веб-сайті http://www.settlement.com.ua.

При поверненні Клієнтом Розрахунковому центру отриманого носія ключової інформації "Secure Token 337" без пошкоджень і в робочому стані складається Акт прийому-передачі носія ключової інформації (Додаток 7).

5.4. Розрахунковий центр надає робоче місце (програмно-технічний комплекс) та допомагає виконати генерацію особистих ключів Користувача Клієнта.

5.5. Особистий ключ використовується в Системі для накладання ЕЦП, який в свою чергу використовується для ідентифікації особи, що накладає ЕЦП, і підтвердження цілісності електронного документа, що передається в Розрахунковий центр.

5.6. Відкритий ключ використовується Розрахунковим центром для перевірки ЕЦП Користувача на ЕД.

5.7. Користувач, який здійснює діяльність в Системі повинен бути вказаний в анкеті клірингового рахунку (рахунків) Клієнта як розпорядник Рахунку, та володіти чинним особистим ключем. Користувачем може бути тільки один з розпорядників Рахунку, вказаних в анкеті клірингового рахунку (рахунків) Клієнта. При зміні Користувача генеруються нові особисті ключі.

5.8. Клієнт повинен використовувати таку кількість особистих ключів, яка необхідна для накладення ЕЦП відповідно до вимог розділу 2 цього Положення.

5.9. Власник особистого ключа несе повну відповідальність за збереження особистого ключа і приймає всі заходи, що перешкоджають користуванню цим ключем сторонніми особами.

5.10. Термін дії кожного особистого ключа Клієнта становить **365** календарних днів з дня його генерації.

5.11. Для генерації особистих ключів Клієнт використовує необхідну кількість носіїв ключової інформації з дотриманням вимог, встановлених п. 5.8 цього Положення.

5.12. Крім ключів для здійснення алгоритмів ЕЦП Клієнт на робочому місці Розрахункового центру проводить генерацію ключа шифрування.

6. Порядок генерації особистих ключів ЕЦП та ключа шифрування

6.1. Клієнт надає Розрахунковому центру наступні документи для генерації особистих ключів ЕЦП Користувача, ЕЦП печатки Клієнта/ключа ідентифікатора Клієнта та ключа шифрування:

- заяву на засвідчення та реєстрацію відкритого ключа та ключа шифрування (Додаток 2);
- довіреність на виконання генерації особистих ключів та ключа шифрування (Додаток 3).

6.2. Розрахунковий центр забезпечує генерацію ключів ЕЦП Користувача, ЕЦП печатки Клієнта/ключа ідентифікатора Клієнта та ключа шифрування відповідно до заяви на засвідчення та реєстрацію відкритого ключа та ключа шифрування на робочому місці.

6.3. Для повторної генерації особистих ключів та ключа шифрування Клієнт виконує дії відповідно п. 6.1 – 6.2цього Положення.

7. Забезпечення інформаційної безпеки в Системі

7.1. Засоби забезпечення інформаційної безпеки.

7.1.1. Інформаційна безпека в Системі реалізується за допомогою програмно-технічних та організаційних засобів.

7.1.2. До програмно-технічних засобів інформаційної безпеки відносяться:

7.1.2.1. Система паролів та ідентифікаторів для розмежування доступу Користувачів до технічних і програмних засобів Системи;

7.1.2.2. Використання програмного забезпечення для підготовки даних для виконання алгоритмів ЕЦП;

7.1.2.3. Програмно-апаратні засоби захисту від несанкціонованого доступу до ЕД та іншої інформації;

7.1.2.4. Криптографічне шифрування інформації в каналах зв'язку з використанням алгоритмів шифрування відповідно до ГОСТ-28147;

7.1.2.5. Засоби захисту від програмних вірусів.

7.1.3. До організаційних заходів відносяться:

7.1.3.1. Розміщення технічних засобів в приміщеннях з контрольованим доступом;

7.1.3.2. Адміністративні обмеження доступу до технічних засобів;

7.1.3.3. Допуск до Системи тільки спеціально підготовлених та уповноважених осіб;

7.1.3.4. Підтримка програмно-технічних засобів в справному стані.

7.2. Порядок дій при компрометації особистих ключів Клієнта.

7.2.1. До подій, на підставі яких Клієнт приймає рішення про компрометацію особистого ключа, відносяться наступні:

- втрата носія ключової інформації з особистим ключем;
- виникнення підозри на витік інформації або її спотворення за рахунок несанкціонованого використання.

7.2.2. В разі компрометації особистих ключів, Клієнт негайно повідомляє про це Розрахунковий центр шляхом надіслання засобами факсимільного зв'язку письмового повідомлення про компрометацію, підписаного Клієнтом або керівником (особою, що виконує обов'язки керівника) Клієнта з подальшою відправкою оригіналу вказаного повідомлення поштою або кур'єрським зв'язком.

В разі ненадання Клієнтом такого повідомлення, особисті ключі якого скомпрометовані, для Розрахункового центру відкриті ключі вважаються чинними і Розрахунковий центр не несе відповідальності за одержання, оброблення та здійснення інших дій щодо ЕД підписаних ЕЦП Клієнта.

7.2.3.В разі отримання Розрахунковим центром факсимільного письмового повідомлення від Клієнта про компрометацію особистого ключа, Розрахунковий центр здійснює блокування сертифіката ключа та блокування доступу Користувача до Системи. Після отримання оригіналу письмового повідомлення Клієнта про компрометацію особистого ключа, Розрахунковий центр здійснює скасування сертифіката ключа Користувача та вносить відкритий ключ Клієнта в список відкликаних відкритих ключів (далі – СВВК).

7.2.4. Розрахунковий центр з моменту внесення відкритих ключів Клієнта в СВВК, припиняє обробку та виконання ЕД Клієнта, що підписані "скомпрометованими" особистими ключами Клієнта, які відповідають відкритим ключам включеним до СВВК.

8. Порядок блокування, поновлення та скасування сертифіката ключа Користувача, блокування доступу Користувача до Системи

8.1. Розрахунковий центр здійснює блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи у таких випадках:

8.1.1. Закінчення строку повноважень Користувача розпоряджатися Рахунком / Рахунками Клієнта і підписувати електронні розпорядження (в разі якщо Розрахунковому центру для відкриття чи обслуговування Рахунку / Рахунків Клієнта були надані документи, в яких вказані строки повноважень Користувача) – з дня наступного за днем закінчення строку повноважень Користувача;

8.1.2. Відсутності вклеєних в паспорт Користувача фотокарток при досягненні Користувачем 25 / 45-річного віку – з дня наступного за днем досягнення Користувачем 25 / 45-річного віку;

8.1.3. Призначення, зміни або припинення повноважень уповноваженої особи Фонду гарантування вкладів фізичних осіб на здійснення тимчасової адміністрації у Клієнті або на ліквідацію Клієнта – з дня розміщення відповідної інформації на сайті Фонду гарантування вкладів фізичних осіб;

8.1.4. Отримання Розрахунковим центром інформації з офіційних джерел (у тому числі веб-сайтів https://smida.gov.ua, https://stockmarket.gov.ua, https://usr.minjust.gov.ua, https://fg.gov.ua, https://lr.nssmc.gov.ua) щодо зміни інформації про Користувача – в день отримання Розрахунковим центром відповідної інформації;

8.1.5. Отримання факсимільного письмового повідомлення від Клієнта про компрометацію особистого ключа – в день отримання такого повідомлення від Клієнта.

8.2. Розрахунковий центр поновлює сертифікат ключа Користувача та розблоковує доступ Користувача до Системи у таких випадках:

8.2.1. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.1. цього Положення – у день внесення Розрахунковим центром змін до реквізитів Рахунку/Рахунків Клієнта, які підтверджують продовження строку повноважень Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів;

8.2.2. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.2. цього Положення – у день внесення Розрахунковим центром змін до реквізитів Рахунку/Рахунків Клієнта, які підтверджують наявність в паспорті Користувача фотокарток при досягнені Користувачем 25 / 45-річного віку;

8.2.3. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.3. цього Положення – у день отримання Розрахунковим центром документів, що підтверджують повноваження Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів;

8.2.4. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.4. цього Положення – у день отримання Розрахунковим центром документів, що підтверджують повноваження Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів, або документів, що підтверджують відсутність змін в інформації про Користувача, або у день внесення Розрахунковим центром змін до документів справи з юридичного оформлення рахунку Клієнта, які підтверджують відповідні зміни щодо Користувача (якщо для поновлення сертифіката ключа Користувача та розблокування доступу Користувача до Системи необхідне внесення змін до реквізитів Рахунку/Рахунків Клієнта).

8.3. Розрахунковий центр здійснює скасування сертифіката ключа Користувача та блокування доступу Користувача до Системи у таких випадках:

8.3.1. Зміна Користувача або зміна прізвища, імені, по батькові Користувача – у день отримання Розрахунковим центром документів, що підтверджують ці зміни;

8.3.2. Зміна найменування Клієнта-юридичної особи – у день отримання Розрахунковим центром документів, що підтверджують ці зміни;

8.3.3. Закінчення строку чинності сертифіката – у день і час закінчення строку чинності сертифіката;

8.3.4. Закриття Рахунку Клієнта – у день закриття Рахунку;

8.3.5. Розірвання /припинення дії договору про обслуговування в системі інтернет-клірингу, укладеного з Клієнтом – у день розірвання /припинення дії договору про обслуговування в системі інтернет-клірингу;

8.3.6. Призначення, зміни або припинення повноважень уповноваженої особи Фонду гарантування вкладів фізичних осіб на здійснення тимчасової адміністрації у Клієнті або на ліквідацію Клієнта – у день отримання Розрахунковим центром документів щодо припинення повноважень Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів, або у день внесення Розрахунковим центром змін до реквізитів Рахунку/ Рахунків Клієнта, які підтверджують відповідні зміни щодо Користувача (якщо клієнтом були надані документи для внесення Розрахунковим центром змін до реквізитів Рахунку / Рахунків Клієнта);

8.3.7. Отримання оригіналу письмового повідомлення Клієнта про компрометацію особистого ключа – в день отримання такого повідомлення від Клієнта.

8.4. У разі скасування сертифіката ключа Користувача з підстав, вказаних в п.8.3.1., 8.3.2., 8.3.3., 8.3.7. цього Положення, для поновлення доступу Користувача до Системи Клієнту необхідно виконати повторну генерацію особистих та відкритих ключів відповідно до розділу 6 цього Положення.

9. Порядок вирішення конфліктних ситуацій та спорів у Системі

9.1. При роботі в Системі можливе виникнення конфліктних ситуацій, пов'язаних з формуванням, доставкою, отриманням, підтвердженням отримання ЕД, а також використанням в даних документах ЕЦП. Дані конфліктні ситуації можуть виникати в наступних випадках:

9.1.1. Заперечення факту формування, підписання ЕД особистими ключами Клієнта;

9.1.2. Заперечення факту відправлення ЕД в Системі;

9.1.3. Інші випадки виникнення конфліктних ситуацій, пов'язаних з функціонуванням Системи.

9.2. Конфліктна ситуація може виникнути у випадку, якщо Розрахунковий центр висловлює недовіру до складу і формату ЕД, що відправлено Клієнтом, а також якщо Розрахунковий центр висловлює недовіру до програмного забезпечення, що функціонує на робочому місці Клієнта.

9.3. Повідомлення про конфліктну ситуацію:

9.3.1. Вразі виникнення конфліктної ситуації Клієнт повинен негайно направити повідомлення про конфліктну ситуацію в Розрахунковий центр;

9.3.2. Повідомлення про наявність конфліктної ситуації повинне містити інформацію про зміст конфліктної ситуації і обставини, які свідчать про наявність конфліктної ситуації. Незалежно від форми, в якій складено повідомлення (паперова форма або електронний документ), таке повідомлення повинне містити реквізити відповідного ЕД. Крім того, в ньому мають бути вказані прізвище, ім'я і по батькові, посада, контактні телефони, факс,

адреса електронної пошти контактної особи або контактних осіб з питань врегулювання конфліктної ситуації.

9.4. Розгляд конфліктної ситуації.

9.4.1. Конфліктна ситуація визнається вирішеною в робочому порядку у випадку, якщо Клієнт задоволений інформацією, отриманою від Розрахункового центра.

9.4.2. У випадку, якщо Клієнт не задоволений отриманою від Розрахункового центру інформацією, для розгляду конфліктної ситуації формується відповідна технічна комісія.

9.4.3. Не пізніше ніж на наступний робочий день після того, як прийнято рішення про необхідність формування технічної комісії, або не пізніше, ніж на третій робочий день після отримання повідомлення про конфліктну ситуацію, у випадку, якщо конфліктна ситуація не була врегульована в робочому порядку, технічна комісія має бути сформована.

9.4.4. До складу технічної комісії можуть входити фахівці з числа працівників підрозділів інформаційної безпеки Клієнта. Особи, що входять до складу технічної комісії, повинні володіти необхідними знаннями в галузі побудови системи криптографічного захисту інформації, роботи комп'ютерних інформаційних систем та ЕЦП.

9.4.5. Загальна кількість членів технічної комісії – 5 осіб. До складу технічної комісії можуть входити Клієнти або представники Клієнтів. Повноваження представника Клієнта для участі в технічній комісії повинні бути підтверджені згідно законодавства України.

9.4.6. Сформована технічна комісія при розгляді конфліктної ситуації встановлює на технологічному рівні наявність або відсутність фактичних обставин, що свідчать про факт і час складання та / або відправки ЕД, достовірність ЕД, а також факт підписання ЕД ЕЦП, автентичність відправленого документа отриманому та інші факти.

Технічна комісія має право розглядати будь-які інші технічні питання, необхідні для з'ясування причин і наслідків виникнення конфліктної ситуації.

9.4.7. Технічна комісія не дає правову або яку-небудь іншу оцінку професійній діяльності Клієнта або Розрахункового центру, діям, які були виконані або не виконані, або несвоєчасно виконані на підставі ЕД, у відношенні якого/яких розглядається конфліктна ситуація.

9.4.8. Всі дії, що здійснюються технічною комісією для з'ясування фактичних обставин, а також висновки, зроблені технічною комісією, заносяться в протокол засідання технічної комісії. Протокол засідання технічної комісії повинен містити наступні дані:

9.4.8.1 склад технічної комісії з вказівкою відомостей про кваліфікацію кожного з членів технічної комісії;

9.4.8.2 короткий виклад обставин конфліктної ситуації, що виникла;

9.4.8.3 заходи, що проводяться технічною комісією для встановлення підстав виникнення і наслідків конфліктної ситуації, з вказівкою дати, часу і місця проведення заходів;

9.4.8.4 висновки технічної комісії в результаті проведених дослідження конфліктної ситуації.

9.4.9. У випадку якщо думка члена технічної комісії щодо порядку, методики, мети заходів, що проводяться, не збігається з думкою більшості членів технічної комісії, про це в Протоколі засідання технічної комісії складається відповідний запис, який підписується членом (або членами технічної комісії), особливу думку якого /яких відображає відповідний запис.

9.4.10. Протокол засідання технічної комісії складається в двох примірниках на паперовому носії, який надається Клієнту.

9.5. Порядок врегулювання суперечок і розбіжностей.

9.5.1. Всі спори і розбіжності, які можуть виникнути у зв'язку із застосуванням, порушенням, тлумаченням цього Положення, визнанням недійсними цього Положення, вирішуються шляхом переговорів.

9.5.2. У випадку, якщо конфліктна ситуація не врегульована в процесі переговорів, вона може бути вирішена у судовому порядку.

10. Прикінцеві положення

10.1. Це Положення затверджується Правлінням та набуває чинності з моменту його затвердження.

10.2. Зміни та доповнення до цього Положення затверджуються Правлінням Розрахункового центру. Внесення змін та доповнень здійснюється шляхом затвердження нової редакції цього Положення.

10.3. У випадку, якщо будь-яка частина цього Положення перестає відповідати законодавству України та / або Статуту, то відповідна частина цього Положення втрачає чинність і Положення застосовується лише в тій частині, що не суперечить законодавству України та Статуту.

Голова Правління **Ю.І. Шаповал**

РОЗРОБНИК:

Начальник відділу інформаційної безпеки	_____	Ю.Ю. Желябовський

ПОГОДЖЕНО:

Начальник управління комплаєнс-контролю	_____	І.В. Гнатюк
Начальник управління інформаційних технологій	_____	К.В. М’якушко
Начальник управління забезпечення розрахунків	_____	Б.Б. Жиров

Додатки

Додаток 1

(ОФОРМЛЮЄТЬСЯ НА БЛАНКУ КЛІЄНТА)

Заява
на підключення до Системи "Інтернет-кліринг"

№_____ "___" _____ 20_ р.

1. Просимо Вас підключити до Системи "Інтернет-Кліринг"

_____
(повне найменування Клієнта)

та надати доступ для дистанційного обслуговування до клірингових рахунків/субрахунків, відкритих на підставі договору про клірингове обслуговування №_____ від _____р.
створити та зареєструвати такі відкриті ключі Клієнта.

2. Користувач (Особа, яка має право підпису)*:

Посада	
Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	

3. Користувач (Особа, яка відповідальна за підпис печатки/ ключ ідентифікатора Клієнта):

Повне найменування Клієнта	
E-Mail	
ЄДРПОУ	
Прізвище, ім'я, по батькові відповідальної особи	
Контактний тел.	

Керівник Клієнта _____ / _____ /
(підпис) (прізвище, ініціали)

* Особи зазначені в картці із зразками підписів Клієнта. Вказується необхідна кількість осіб відповідно до картки із зразками підписів

Продовження на звороті

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Адміністратор системи "Інтернет-кліринг"

_____

(дата підключення, прізвище, ініціали та підпис)

Додаток 2

(ОФОРМЛЮЄТЬСЯ НА БЛАНКУ КЛІЄНТА)

Заява
на засвідчення та реєстрацію відкритих ключів та ключа шифрування в Системі дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет-кліринг"

№_____ " ___" _____ 20_ р.

1. Просимо Вас засвідчити та зареєструвати відкриті ключі та ключ шифрування **в Системі дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет-кліринг"**
_____
(повне найменування Клієнта)

таким Користувачам:

1. Користувач (Особа, яка має право підпису)*:

Посада	
Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	
Діє на підставі (статут, довіреність, інше)	
Зразок підпису власника відкритого ключа	

Заповнюється працівником підрозділу інформаційної безпеки Розрахункового центру:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

2. Користувач (Особа, яка відповідальна за підпис печатки/ключ ідентифікатора Клієнта):

Повне найменування Клієнта	
E-Mail	
ЄДРПОУ	
Прізвище, ім'я, по батькові відповідальної особи	
Контактний тел.	
Діє на підставі (статут, довіреність, інше)	

Заповнюється працівником підрозділу інформаційної безпеки Розрахункового центру:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

3. Користувач (Особа, яка відповідальна за ключ шифрування):

Повне найменування Клієнта	
E-Mail	
ЄДРПОУ	
Прізвище, ім'я, по батькові відповідальної	

особи	
Контактний тел.	

Заповнюється працівником підрозділу інформаційної безпеки Розрахункового центру:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

Керівник Клієнта _____ / _____ /

(підпис) (прізвище, ініціали)

* Особи зазначені в картці із зразками підписів Клієнта. Вказується необхідна кількість осіб відповідно до картки із зразками підписів

Заповнюється працівниками Розрахункового центру

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Додаток 3

(ОФОРМЛЮЄТЬСЯ НА БЛАНКУ КЛІЄНТА)

Довіреність

_____ _____
(місце видачі) (дата видачі)

_____, далі – Клієнт
(повне найменування Клієнт)

в особі _____, що діє на
(посада, прізвище, ім'я, по батькові)

підставі Статуту, уповноважує _____
(посада, прізвище, ім'я, по батькові повноважного представника)

- *паспортні дані (серія, номер, орган, що видав паспорт, дата видачі) та місце проживання;*
- *телефон для зв'язку.*

Виконати генерацію особистих та відкритих ключів підпису, печатки/ключа ідентифікатора Клієнта, ключа шифрування на програмно-технічному комплексі ПАТ «Розрахунковий центр»

Ця довіреність дійсна до "_____" _____ 20__ року.

Керівник _____ _____ (_____)
(найменування посади) (підпис) (прізвище, ініціали)

Додаток 4

Акт про підключення
до Системи дистанційного обслуговування клірингових рахунків/субрахунків
"Інтернет-кліринг"

м. Київ _____ 201__ року

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Розрахунковий центр) в особі_____
_____,
який діє на підставі_____,
та _____(далі – Клієнт)
в особі _____,
який діє на підставі _____, підписали цей акт про таке:

1. Розрахунковий центр підключив Клієнта до Системи дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет-кліринг" та надав доступ для дистанційного обслуговування Рахунку клірингових рахунків/субрахунків, відкритих на підставі договору про клірингове обслуговування №_____ від _____ р.

2. Розрахунковий центр зареєстрував в Системі дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет-кліринг" відкриті ключі Клієнта:

№	*Заповнюється клієнтом:*	*Заповнюється працівником підрозділу інформаційної безпеки Розрахункового центру:*	
1.	Прізвище, ім'я, по батькові Користувача: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____
2.	Найменування Клієнта: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____

ПАТ "Розрахунковий центр" Клієнт

_____ _____ _____ _____
(підпис) (прізвище, ініціали) (підпис) (прізвище, ініціали)

Продовження на звороті

Заповнюється працівниками Розрахункового центру

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Додаток 5

Вимоги
до програмно-технічного забезпечення Клієнтів, що підключаються до Системи дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет-кліринг" ПАТ "Розрахунковий Центр"

1. Вимоги до технічного забезпечення Клієнтів, що підключаються до Системи дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет- кліринг " ПАТ "Розрахунковий центр"

Підключення до Системи дистанційного обслуговування клірингових рахунків/субрахунків "Інтернет-кліринг" ПАТ "Розрахунковий Центр" (далі - Система "Інтернет-кліринг") передбачає наступні вимоги до технічного забезпечення Клієнтів:

- наявність персонального комп’ютера, що має порт USB 2.0;
- наявність швидкісного Internet-каналу(не менше ніж 256 кб/с). Безпосереднє (без використання проксі сервера) підключення до мережі Інтернет;
- забезпечити на стороні Користувача, проходження пакетів по ftp протоколу на адресу icliring.settlement.com.ua:10122, по http протоколу на адресу icliring.settlement.com.ua:10180 (при цьому - ftp протокол, порти 10122 та 10180 не повинні бути закриті).

2. Вимоги до системного програмного забезпечення Клієнтів, що підключаються до Системи "Інтернет-кліринг"

Підключення до Системи "Інтернет-кліринг"передбачає наступні вимоги до системного програмного забезпечення Клієнта:

- наявність ліцензійної версії однієї з операційних систем родини Windows, не нижче Windows XP SP3.
- Інтернет-баузер сумісний з операційною системою з підтримкою ActiveX: Microsoft Internet Explorer 8 і вище.

Додаток 6

Акт
прийому-передачі носія ключової інформації
до Договору про обслуговування в системі інтернет-кліринг
№ _____ від _____

м. Київ _____ 20__ р.

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі - ПАТ "Розрахунковий центр") в особі _____ _____,
який діє на підставі _____,
з однієї сторони,
та _____ (далі - Клієнт) в особі _____,
який діє на підставі _____, з другої сторони, підписали цей акт про наступне:

1. ПАТ "Розрахунковий центр" передав, а Клієнт прийняв:

1.1. носій ключової інформації "Secure Token 337" №_____

2. Вказаний в п.1 цього акту носій ключової інформації, переданий в робочому стані і без пошкоджень.

ПАТ "Розрахунковий центр"		Клієнт	
_____ (підпис)	_____ (прізвище, ініціали)	_____ (підпис)	_____ (прізвище, ініціали)

Додаток 7

Акт
прийому-передачі носіїв ключової інформації
до додаткового договору до договору про обслуговування в системі інтернет-кліринг
№ _____ від _____
до Договору про обслуговування в системі інтернет-кліринг
№ _____ від _____

м. Київ _____ 20__ р.

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі - ПАТ "Розрахунковий центр") в особі _____ _____,
який діє на підставі _____,
з однієї сторони,
та _____ (далі - Клієнт) в особі _____,
який діє на підставі _____, з другої сторони, підписали цей акт про наступне:

1.Клієнт передав, а ПАТ "Розрахунковий центр" прийняв:

1. носій ключової інформації "Secure Token 337" №_____

2. Вказаний в п.1 цього акту носій ключової інформації переданий в робочому стані і без пошкоджень.

3. ПАТ "Розрахунковий центр" зобов'язується повернути Клієнту заставну вартість, вказаного в п.1 цього акту носія ключової інформації протягом 5 робочих днів з дати підписання цього акту на поточний (кореспондентський) рахунок Клієнта:

рахунок № _____
в _____ (найменування банку)

код банку _____

ПАТ "Розрахунковий центр"		Клієнт	
_____	_____	_____	_____
(підпис)	(прізвище, ініціали)	(підпис)	(прізвище, ініціали)

Друга редакція

Затверджено
Протокол засідання Правління
04.08.2015 р. №34