

«ЗАТВЕРДЖЕНО»
Рішенням учасника (одноосібного власника)
ТОВ «ФК «Форінт»
№ 292 від «12» березня 2024 р.

Директор



Васильєв О.В.

ПОРЯДОК
використання електронного підпису та електронної печатки в
ТОВАРИСТВІ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ФІНАНСОВА КОМПАНІЯ «ФОРІНТ»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Порядок використання електронного підпису та електронної печатки (далі – Порядок) в ТОВАРИСТВІ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ФІНАНСОВА КОМПАНІЯ «ФОРІНТ» (далі – Установа) є внутрішнім документом Установи, який регламентує визначення організаційно-методологічних умов застосування в Установі електронних підписів та електронної печатки, які використовуються під час створення, оброблення та зберігання електронних документів, а також встановлення порядку дій при роботі з електронними документами, зокрема, в частині виявлення будь-яких змін в електронних документах та/або в електронних підписах після їх підписання з метою забезпечення належного рівня безпеки інформації та дотримання Установою вимог чинного законодавства України.

1.2. У своїй діяльності Установа має право створювати, відправляти, передавати, одержувати, зберігати, обробляти, використовувати та знищувати документи, у тому числі електронні, інформація в яких зафіксована у вигляді даних, у тому числі електронних, а також вчиняти правочини у вигляді документів, створених як в паперовій, та і в електронній формі.

1.3. Дії з електронними документами, їх зберігання здійснюються Установою із забезпеченням можливості перевірки їх цілісності та справжності та у відповідності до вимог, визначених законодавством та внутрішніми положеннями Установи.

1.4. Порядок розроблений, впроваджується та має оновлюватись з урахуванням вимог Закону України «Про електронні документи та електронний документообіг», Закону України «Про електронну ідентифікацію та електронні довірчі послуги», Положення про використання електронного підпису та електронної печатки, затвердженого постановою Правління Національного банку України від 20.12.2023р. №172, інших нормативно-правових актів Національного банку України, нормативно-правових актів інших державних органів, прийнятих для виконання та відповідно до законів України.

1.5. Цей Порядок затверджується Рішенням учасника (одноосібного власника) Установи і є обов'язковим для виконання всіма працівниками Установи й уповноваженими представниками Установи. ТОВ «ФК «Форінт» забезпечує безперешкодний доступ до Порядку своїх клієнтів та інших фізичних і юридичних осіб шляхом розміщення Порядку на веб-сайті Установи та/або в приміщенні Установи.

2. ВИЗНАЧЕННЯ ТЕРМІНІВ

Верифікація – заходи, що вживаються установою з метою перевірки (підтвердження) належності відповідній особі отриманих установою ідентифікаційних даних;

Електронні дані – будь-яка інформація в електронній формі;

Електронний документ (ЕД) – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (стаття 5 розділ II Закону України «Про електронні документи та електронний документообіг»);

Електронний підпис (ЕП) - електронні дані, які додаються Підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис.

Ідентифікація – заходи, що вживаються установою для встановлення особи шляхом отримання її ідентифікаційних даних;

Кваліфікований електронний підпис (КЕП/ кваліфікований ЕП) – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

Кваліфікований сертифікат відкритого ключа (Кваліфікований сертифікат) – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам Законодавства;

Компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого використання Особистого ключа;

Засоби криптографічного захисту інформації – це програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації.

Клієнт установи – клієнт банку, небанківської фінансової установи або особи, що не є фінансовою установою, але має право надавати окремі фінансові послуги, користувач платіжних послуг;

Контрагент установи – будь-яка юридична чи фізична особа, фізична особа-підприємець, фізична особа, яка провадить незалежну професійну діяльність, яка має з установою відносини фінансового характеру. Контрагент може одночасно мати з установою трудові відносини або відносини іншого характеру;

Паперовий документ (ПД) – будь-який документ сформований/відображений на папері;

Перевірка цілісності – процедура, яка дає змогу виявити будь-які зміни в електронному документі та зміни ЕП після підписання електронного документа;

Підписувач - особа, яка здійснює накладання електронного підпису на електронний документ;

Суб'єкт електронної взаємодії – Національний банк, установа, клієнт установи, контрагент установи та комерційний агент установи;

Удосконалена електронна печатка, що базується на кваліфікованому сертифікаті електронної печатки (далі - електронна печатка з кваліфікованим сертифікатом), - удосконалена електронна печатка, створена з використанням кваліфікованого сертифіката електронної печатки, у якому є позначка, що цей сертифікат сформовано як кваліфікований для використання електронної печатки, та немає відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки;

Уповноважена особа установи – особа, яка не є працівником установи, якій згідно з довіреністю та/або на підставі правочинів надано повноваження на підписання з клієнтами установи, контрагентами договорів та інших документів від імені установи;

Уповноважений працівник установи – працівник установи, до повноважень якого згідно з внутрішніми документами установи чи на підставі довіреності належить підписання з клієнтами установи, контрагентами установи, комерційними агентами установи договорів та інших документів від імені установи.

3. СФЕРА ЗАСТОСУВАННЯ

3.1. Положення визначені цим Порядком застосовуються до процесів обробки та перетворення електронних документів засвідчених електронно-цифровим підписом та електронною печаткою у процесі вчинення юридичних дій.

3.2. Дії з електронними документами, їх зберігання здійснюються Установою із забезпеченням можливості перевірки їх цілісності та справжності та у відповідності до вимог, визначених законодавством та внутрішніми документами Установи. Обов'язок доведення цілісності та справжності електронних документів, створених з використанням технології, визначеної Установою, покладається на Установу.

3.3. Керівник Установи відповідає за організацію використання електронного підпису та електронної печатки в Установі, а також за використання ЕП та електронної печатки уповноваженими працівниками Установи / уповноваженими особами Установи (далі - уповноважений представник установи), комерційними агентами Установи під час їх взаємодії від імені Установи з клієнтами Установи та контрагентами Установи, якщо інше не встановлено законодавством України.

3.4. ЕП є обов'язковим реквізитом електронного документа. ЕП представляє собою електронні дані (будь-яку інформацію в електронній формі), які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис.

3.5. Особа, що підписала електронний документ ЕП, у такий спосіб засвідчує, що ознайомила з усім текстом документа, повністю зрозуміла його зміст, не має заперечень до тексту документа (або її заперечення внесені як окремий реквізит документа) і свідомо використала свій ЕП у контексті, передбаченому документом (підписала, затвердила, погодила, завізувала, засвідчила, ознайомила).

3.6. ЕП використовується в якості аналога особистого підпису.

3.7. Установа у своїй діяльності під час створення, оброблення та зберігання електронних документів використовує кваліфікований ЕП.

3.8. Вимоги цього Порядку поширюються на суб'єктів електронної взаємодії.

3.9. Вимоги цього Порядку щодо використання ЕП не можуть тлумачитися суб'єктами електронної взаємодії як такі, що обмежують права суб'єктів електронної взаємодії вчиняти правочини у вигляді паперових документів (змінювати, доповнювати або припиняти дію електронних документів паперовими документами чи в іншій не забороненій законодавством України формі і навпаки) чи в усній формі, якщо законом не встановлено обов'язок вчиняти правочин у письмовій формі.

4. ПОРЯДОК ВИКОРИСТАННЯ ЕП

4.1. Застосовані в Установі ЕП мають юридичну силу незалежно від технологій, що застосовуються для ідентифікації та автентифікації Підписувача, та відповідають таким вимогам:

- логічно пов'язуються з підписаними електронними даними із можливістю перевірити цей зв'язок протягом усього життєвого циклу електронного документа;
- електронні дані, що використовуються для створення ЕП, є унікальними та однозначно пов'язані із Підписувачем і не пов'язані з жодною іншою особою;
- дають змогу однозначно ідентифікувати Підписувача;
- технологія застосування ЕП забезпечує під час підписання контроль електронних даних, які підписуються, та електронних даних, які використовуються для створення ЕП;
- під час перевірки, здійсненої відповідно до вимог цього Порядку, не виявлено будь-яких змін в електронному документі та/або будь-яких змін ЕП після підписання електронного документа.

5. ВИДИ ЕЛЕКТРОННОГО ПІДПISУ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В УСТАНОВІ

5.1. КЕП Установи та кваліфікована електронна печатка Установи застосовується для: відправки звітності та листів в електронній формі до Національного банку України, Державної податкової служби України, Пенсійного фонду України тощо; підписання інших документів в електронній формі відповідно до повноважень, наданих працівникам Установи.

5.2. КЕП Клієнта використовується для підписання електронних документів, в програмних комплексах або WEB-сервісах електронного документообігу з метою підписання електронних документів та здійснення електронної взаємодії між Установою та Клієнтом.

5.3. КЕП Установи – КЕП працівника Установи, уповноваженого на укладення від імені Установи правочинів та підписання відповідних документів, в тому числі під час електронної взаємодії з Клієнтом.

5.4. Умови електронної взаємодії між Клієнтом та Установою зазначаються у відповідному договорі (у випадках та в обсязі, визначеному відповідно до чинного законодавства України).

5.5. ЕП НБУ застосовується для забезпечення роботи з інформаційними задачами НБУ, підписання та відправки платежів та інформаційних повідомлень Банку в системі електронних платежів НБУ.

6. ПОРЯДОК ОТРИМАННЯ ЕП

6.1. Порядок отримання ЕП визначається:

- для КЕП та кваліфікованої електронної печатки – відповідно до регламенту роботи та вимог АЦСК;
- для ЕП НБУ – відповідними нормативними документами НБУ та умовами договору, укладеного між Установою та НБУ.

7. ПОРЯДОК РОБОТИ З КЕП ТА КВАЛІФІКОВАНОЮ ЕЛЕКТРОННОЮ ПЕЧАТКОЮ

7.1. КЕП має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Укладення окремого договору щодо використання КЕП не вимагається.

7.2. Кваліфікована електронна печатка створюється, якщо:

- відповідно до законодавства України потрібно засвідчити дійсність підпису на електронних документах;

- відповідно до законодавства України проставлення печатки вимагається для засвідчення відповідності копій документів оригіналам;

- потрібно підтвердити повноваження представника юридичної особи на застосування ЕП у контексті, передбаченому документом.

7.3. Установа має право використовувати більш, ніж одну кваліфіковану електронну печатку. Юридична особа – суб'єкт електронної взаємодії має право використовувати більш, ніж одну кваліфіковану електронну печатку.

7.4. Створювачу кваліфікованої електронної печатки забороняється створювати кваліфіковану електронну печатку, якщо кваліфікований сертифікат електронної печатки є нечинним або одержати інформацію про його статус неможливо.

7.5. Проставлення КЕП Установи та створення кваліфікованої електронної печатки на електронних документах здійснюється працівниками Установи, які мають на це повноваження відповідно до розпорядчого документу Установи, або в межах, передбачених відповідною довіреністю (у разі, якщо складення довіреності вимагається згідно з законодавством України).

7.6. Уповноважені особи Установи використовують кваліфіковані електронні печатки в програмних комплексах. Відповідно до вимог чинного законодавства України, Установа здійснює приймання, реєстрацію та обробку повідомлень, що надходять до Установи із накладеними КЕП.

7.7. При надходженні вхідного електронного повідомлення, додаток до якого є електронний документ, підписаний КЕП, таке повідомлення проходить перевірку на наявність шкідливого програмного забезпечення, а також перевіряється справжність зазначеного ЕП (в т.ч. здійснюється перевірка цілісності електронних даних, що підписуються ЕП та ідентифікація Підписувача).

7.8. За відсутності шкідливого програмного забезпечення та визначення справжності ЕП (в т.ч. проходження перевірки на предмет цілісності електронних даних, що підписуються, та на предмет ідентифікації Підписувача), повідомлення реєструється в Установі та приймається до опрацювання відповідними підрозділами Установи, яких стосується вказане звернення, відповідно до встановленого порядку.

8. ПОРЯДОК СТВОРЕННЯ І ЗАСВІДЧЕННЯ ЕЛЕКТРОННОЇ КОПІЇ З ПАПЕРОВОГО ДОКУМЕНТА

8.1. Створення електронної копії з оригіналу документа на папері здійснюється шляхом його сканування та/або фотографування, та збереження документа.

8.2. Для засвідчення копії документа в електронній формі працівник Установи, уповноважений на підписання такого документа в паперовій формі або на засвідчення копій документів, накладає на документ свій ЕП.

8.3. У разі необхідності додаткового підтвердження повноважень особи, що накладає Кваліфікований ЕП, на електронній копії документа, допускається застосування Кваліфікованої електронної печатки.

8.4. Установа на вимогу Клієнта надає йому документ, оформлений в паперовій формі, та/або копію оригіналу електронного документа в паперовій формі,

та/або примірник оригіналу електронного документа (копію файла електронного документа).

8.5. Електронна копія документу у паперовій формі, засвідчена ЕП уповноваженого працівника Установи, є електронним документом, статус якого прирівнюється до завіреної електронної копії оригіналу документу у паперовій формі.

8.6. Завірений документ може бути перевірений на цілісність та достовірність з використанням інструментів АЦСК органів юстиції України або інших АЦСК.

8.7. Установа залишає за собою право не приймати завірений електронний документ, якщо він не відповідає вищеперерахованим вимогам.

9. ПОРЯДОК СТВОРЕННЯ І ЗАСВІДЧЕННЯ ПАПЕРОВОЇ КОПІЇ ЕЛЕКТРОННОГО ДОКУМЕНТА

9.1. У разі створення копії на папері з електронного документу працівник Установи, який створює таку копію, проводить обов'язкову перевірку цілісності електронного документу засобами перевірки ЕП, вбудованих в програмні комплекси (WEB-сервіси в мережі Інтернет) електронного документообігу або WEB-сервіси в мережі Інтернет на офіційному сайті кваліфікованого надавача електронних довірчих послуг «АЦСК органів юстиції України». Електронний документ вважається справжнім у разі одержання позитивного результату перевірки його цілісності.

9.2. Створення копії на папері з електронного документа виконується шляхом роздрукування електронного документа.

9.3. Оригінал ЕД повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством України та у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у вигляді копії на папері.

9.4. Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене особистим підписом Власника документа.

9.5. Для засвідчення копії на папері працівник Установи, уповноважений на підписання такого документа в паперовій формі або на засвідчення копій документів, накладає на документ свій власноручний підпис та відмітку «Згідно з оригіналом».

9.6. У разі необхідності додаткового підтвердження повноважень особи, що накладає власноручний підпис на документ, допускається застосування печатки (за вимогою).

9.7. На паперову копію наноситься інформація про те, що даний документ – копія з електронного документа і що електронний документ підписаний ЕП, П.І.Б. підписанта, дата та час накладання підпису.

9.8. У разі отримання відомостей з «Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань про суб'єкта господарювання» (у тому числі установчі документи юридичних осіб), у вигляді безоплатного доступу через портал електронних сервісів уповноважений працівник Установи засвідчує роздруковані документи на папері власним підписом із зазначенням дати формування документу, посади, ПІБ.

9.9. У випадку нанесення на друковану копію електронного документу будь-яких поміток та коригувань, або вчинення його пошкодження він вважається не дійсним у зв'язку з порушенням цілісності.

10. ВИЯВЛЕННЯ БУДЬ-ЯКИХ ЗМІН В ЕЛЕКТРОННОМУ ДОКУМЕНТІ, В ЕЛЕКТРОННІЙ КОПІЇ З ПАПЕРОВОГО ДОКУМЕНТА

10.1. ЕП є обов'язковим реквізитом електронного документа. Накладанням ЕП завершується створення електронного документа.

10.2. Електронний документ вважається створеним, якщо ЕП додається до підписаних електронних даних та пов'язується логічно з ними. В цьому випадку є можливість перевірити цей зв'язок протягом усього життєвого циклу електронного документу: від його створення до знищення, або під час постійного зберігання.

10.3. Підписувач, який здійснює накладення ЕП на електронний документ, цим самим засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, не має заперечень до тексту документа і свідомо застосував свій підпис у контексті, передбаченому документом (підписав, погодив, засвідчив, підтвердив тощо).

10.4. Виявлення будь-яких змін в електронному документі здійснюється шляхом перевірки цілісності ЕП, наявності та актуальності ЕП на момент підписання або логічного додавання до електронного документа.

10.5. Для перевірки цілісності електронного документа можуть бути використані державні он-лайн ресурси, які використовують криптографічні алгоритми та протоколи, що відповідають чинному законодавству України, такі як сайт АЦСК органів юстиції України.

10.6. За наявності будь-яких чинників, що ставлять під сумнів достовірність електронного документа та чинність ЕП, яким засвідчувався електронний документ, Установа відмовляє в його прийомі та повертає з коротким описом причин відхилення.

10.7. Відповідальність за виявлення будь-яких змін в електронних документах покладається на працівників Установи, які у своїй діяльності та/або процесах створюють, супроводжують електронні документи.

11. ВИЯВЛЕННЯ БУДЬ-ЯКИХ ЗМІН ЕЛЕКТРОННОГО ПІДПISУ ПІСЛЯ ПІДПISАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТА

11.1. Перевірка цілісності електронного документа та виявлення будь-яких змін ЕП та електронної печатки після підписання електронного документа забезпечується:

– для КЕП та кваліфікованої електронної печатки - порядок виявлення будь-яких змін ЕП визначається та здійснюється у відповідності до регламенту роботи, настанов та інструкцій АЦСК, який здійснив випуск відповідних КЕП. Результатом перевірки КЕП та кваліфікованої електронної печатки є висновок (відповідь), отримана від відповідного сервісу АЦСК.

– для ЕП НБУ – в автоматичному режимі при обробці даних в інформаційних задачах НБУ. Порядок виявлення будь-яких змін в ЕП НБУ визначається нормативними документами НБУ.

11.2. Результати автоматизованого накладання/додавання ЕП відображаються у базах даних відповідних інформаційних систем .

11.3. Перевірка на предмет виявлення будь-яких змін в електронному документі, ЕП та електронної печатки після підписання електронного документа, в т.ч. на предмет забезпечення їх цілісності, може бути здійснена незалежною третьою стороною.

11.4. Відповідальність за виявлення будь-яких змін ЕП, електронної печатки після підписання електронного документа покладається на працівників Установи, які у своїй діяльності та/або процесах створюють, супроводжують та підписують ЕП та електронною печаткою електронні документи.

12. ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПISУ УСТАНОВИ

12.1. Кваліфікований ЕП має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

12.2. Установа зобов'язана після створення електронного документа надати можливість клієнтові / контрагенту Установи отримати примірник цього електронного документа з усіма потрібними реквізитами на адресу електронної пошти, зазначену клієнтом / контрагентом Установи або надати електронний документ в інший спосіб, узгоджений із клієнтом / контрагентом Установи.

12.3. Установа зобов'язана надати клієнтові / контрагенту Установи на його вимогу засвідчену паперову копію електронного документа.

12.4. Установа у своїй діяльності під час створення, оброблення та зберігання електронних документів використовує кваліфікований ЕП.

12.5. Під час використання кваліфікованого ЕП Установа забезпечує приймання, реєстрацію, підтвердження про отримання електронних документів із створеними кваліфікованими ЕП з дотриманням вимог законодавства України у сфері електронного документообігу.

12.6. Перевірка та підтвердження кваліфікованого ЕП, кваліфікованих сертифікатів відкритих ключів здійснюється відповідно до вимог Закону про електронні довірчі послуги.

12.7. Кваліфікований сертифікат ЕП, який приймається Установою, має відповідати вимогам Закону про електронні довірчі послуги. Підписувач зобов'язаний під час створення кваліфікованого ЕП перевірити чинність свого кваліфікованого сертифіката відкритого ключа підписувача.

12.8. Підписувачу забороняється створювати кваліфікований ЕП, якщо кваліфікований сертифікат відкритого ключа підписувача є нечинним або одержати інформацію про його статус неможливо.

12.9. Отримання сертифікату відкритого ключа, скасування кваліфікованих сертифікатів відкритих ключів здійснюється в порядку, встановленому чинним законодавством.

12.10. Порядок генерації кваліфікованого ЕП передбачає генерацію кваліфікованого сертифіката відкритого ключа у спеціальному сервісі АЦСК.

12.11. Уповноважений представник Установи під час взаємодії з клієнтом / контрагентом Установи в разі створення електронних копій з паперових документів використовує КЕП уповноваженого представника Установи з кваліфікованою електронною позначкою часу та/або з кваліфікованою електронною печаткою Установи з кваліфікованою електронною позначкою часу.

12.12. Створення електронних документів постійного і тривалого (понад 10 років) зберігання здійснюється із використанням КЕП уповноваженої відповідно до статутних документів Установи особи / уповноваженого представника Установи, що забезпечують можливість перевірки відповідних КЕП в довгостроковому періоді згідно з вимогами стандартів, що визначають вимоги до створення кваліфікованих електронних підписів та кваліфікованих електронних печаток у разі створення електронних документів, які згідно із законодавством України підлягають передаванню на архівне зберігання, наведених у додатку до Порядку.

12.13. Уповноважена відповідно до статутних документів Установи особа / уповноважений представник Установи - юридичної особи для створення КЕП та УЕП з кваліфікованим сертифікатом зобов'язана(ий) використовувати кваліфікований сертифікат відкритого ключа, який містить код за Єдиним державним реєстром юридичних осіб, фізичних осіб-підприємців та громадських формувань (далі - Реєстр) юридичної особи, представником якої вона / він є.

12.14. Фізична особа, яка діє від імені юридичної особи - клієнта / контрагента Установи (далі - представник клієнта / контрагента установи), для створення КЕП та УЕП з кваліфікованим сертифікатом має право використовувати кваліфікований сертифікат відкритого ключа, що відповідає одній із таких вимог:

- кваліфікований сертифікат відкритого ключа представника клієнта / контрагента Установи містить код за Реєстром юридичної особи;
- у кваліфікованому сертифікаті відкритого ключа представника клієнта / контрагента Установи немає коду за Реєстром юридичної особи та створений представником клієнта / контрагента Установи КЕП/УЕП з кваліфікованим сертифікатом засвідчено кваліфікованою електронною печаткою юридичної особи - клієнта / контрагента Установи;
- у кваліфікованому сертифікаті відкритого ключа представника клієнта / контрагента установи немає коду за Реєстром юридичної особи та в установи є наявності всі потрібні документи, що підтверджують повноваження представника клієнта / контрагента установи щодо підписання відповідного документа від імені юридичної особи - клієнта / контрагента установи.

12.15. Суб'єкт електронної взаємодії - юридична особа, представник якої використовує кваліфікований сертифікат відкритого ключа, що містить код за Реєстром цієї юридичної особи, зобов'язаний забезпечити подання заяви про скасування кваліфікованого сертифіката відкритого ключа представника юридичної особи кваліфікованому надавачу електронних довірчих послуг у разі настання однієї з таких подій:

- зміни даних, внесених у кваліфікований сертифікат відкритого ключа представника юридичної особи;
- звільнення працівника юридичної особи;
- припинення представництва юридичної особи.

12.16. Установа не має права використовувати для інших цілей або передавати іншим особам інформацію, отриману Установою з метою документування та контролю за процесом підписання документа клієнтом з використанням ЕП, якщо не отримав окремої згоди на це від клієнта або якщо інше не передбачено законом. Банк здійснює оброблення електронних документів з використанням ЕП та інформації щодо документування процесу підписання таких документів з дотриманням вимог законодавства України про захист персональних даних та таємниці фінансової послуги. Установа, у спосіб, визначений з клієнтом умовами Договору, надсилає клієнту примірник підписаного в електронній формі документа, що дає змогу встановити дату і час його підписання та дату відправлення на адресу електронної пошти, зазначеної клієнтом, або надати документ в інший спосіб, узгоджений з клієнтом.

12.17. Установа має право застосовувати процедури фото- та/або відео-фіксації, інші

процедури з метою документування та контролю за процесом підписання документа клієнтом з використанням ЦВП. Застосування зазначених процедур здійснюється за умови попередньо отриманої згоди клієнта.

12.18. Записи виконання підпису на екрані комп'ютерного пристрою саме клієнтом, що підтверджуються фото- та/або відео- фіксацією клієнта, зберігаються Установою і можуть бути використані Установою під час вирішення спорів, у тому числі судових, як доказ.

12.19. Установа несе відповідальність за шкоду, заподіяну клієнту під час використання запровадженої Установою технології ЕП.

12.20. Спірні питання стосовно документів, підписаних ЕП, вирішуються між Установою та клієнтом в порядку, установленому законодавством України.

12.21. Установа забезпечує доведення цілісності електронного документа та авторство ЕП клієнта в разі заперечення клієнтом факту вчинення правочину або оспорювання окремих його частин.

13. ВИМОГИ ДО ЗБЕРІГАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ

13.1. Відповідальність за:

- збереження ключів та конфіденційність;
- контроль строку дії ключів;
- використання ключів

несе особисто фізична особа – власник ключа.

13.2. У випадку отримання інформації про підозру в компрометації ключів Установа має право здійснити блокування ключів.

13.3. Зберігання ключів повинно виконуватися згідно з такими вимогами:

– для зберігання особистих ключів мають використовуватися захищені носії ключової інформації;

– відкриті ключі можуть зберігатися у відкритому вигляді з забезпеченням контролю їх цілісності;

– у випадку використання криптографічних засобів інформації, архітектура яких вимагає зберігання особистих ключів у вигляді файлів, Установа забезпечує

обмеження доступу до цих ключів на рівні файлової системи, доступ до якої у відповідній частині мають виключно власники ключів;

– паролі для особистих ключів повинні знати тільки власники особистих ключів. Передача паролів – третім особам - заборонена.

13.4. Підписувач, який здійснює накладення ЕП будь-якого виду, відповідальний за безпеку зберігання та використання особистого ключа ЕП або іншого компоненту ЕП, володіння яким носить виключний характер і є невід'ємною частиною ЕП.

13.5. Підписувачу, що є володільцем особистого ключа ЕП або іншого компонента ЕП заборонено передавати його будь-яким третім особам.

14. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ

14.1. Підписувач, який здійснює накладання ЕП та електронної печатки на електронний документ, цим самим засвідчує те, що:

- ознайомлений з текстом документа;
- розуміє його зміст;
- не має заперечень до тексту документу;
- свідомо застосував свій підпис у контексті, передбаченому документом (підписав, погодив, засвідчив тощо).

14.2. Підписувач, як власник особистого ключа, несе повну відповідальність за забезпечення конфіденційності та контроль строку дії ключа.

14.3. Контроль за виконанням Порядку працівниками Установи покладається на директора Установи.

14.4. Використання ЕП НБУ учасниками (суб'єктами) електронної взаємодії дозволяється тільки у випадках, прямо передбачених нормативно-правовими актами Національного банку України, і з обов'язковим використанням засобів захисту інформації Національного банку України. Підписувач, який здійснює накладення ЕП НБУ на електронний документ, несе особисту відповідальність за достовірність та повноту інформації, що міститься в реквізитах електронного документа.

14.5. Контроль за актуалізацію та своєчасним внесенням змін до Порядку покладається на директора Установи.

15. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

15.1. Порядок набуває чинності з дня його затвердження Рішенням учасника (одноосібного власника) Установи. Зміни до Порядку затверджуються Рішенням учасника (одноосібного власника) Установи шляхом викладення Порядку у новій редакції.

15.2. У разі невідповідності будь-якої частини Порядку чинному законодавству України або іншим нормативним документам, на підставі яких розроблено Порядок, зокрема, у зв'язку із внесенням до них змін / введенням в дію нових законодавчих / нормативних документів, цей Порядок буде діяти лише в тій частині, яка не суперечитиме останнім.

15.3. Установа забезпечує безперешкодний доступ клієнтів/потенційних клієнтів до Порядку шляхом розміщення його на офіційному сайті Установи.

Додаток
до Порядку використання електронного
підпису та електронної печатки в
ТОВАРИСТВІ З ОБМЕЖЕНОЮ
ВІДПОВІДАЛЬНІСТЮ «ФІНАНСОВА
КОМПАНІЯ «ФОРІНТ»

Стандарти, що визначають вимоги до створення
кваліфікованих електронних підписів та кваліфікованих
електронних печаток у разі створення електронних документів,
які згідно із законодавством України підлягають
передаванню на архівне зберігання

1. ДСТУ ETSI TS 102 778-2:2015 "Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 2. Базовий PAdES – профілі, що базуються на ISO 32000-1 (ETSI TS 102 778-2:2009, IDT)", затверджений наказом державного підприємства "Український науково- дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193 (зі змінами).

2. ДСТУ ETSI TS 102 778-3:2015 "Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 3. Посилений PAdES – профілі PAdES-BES і PAdES-EPES (ETSI TS 102 778-3:2010, IDT)", затверджений наказом державного підприємства "Український науково- дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193 (зі змінами).

3. ДСТУ ETSI TS 102 778-4:2015 "Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 4. Довгостроковий PAdES – профіль PAdES LTV (ETSI TS 102 778-4:2009, IDT)", затверджений наказом державного підприємства "Український науково- дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193 (зі змінами).

4. ДСТУ ETSI TS 102 778-5:2015 "Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 5. PAdES для XML контенту – профілі для підписів XAdES (ETSI TS 102 778-5:2009, IDT)", затверджений наказом державного підприємства "Український науково- дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193 (зі змінами).

5. ДСТУ ETSI EN 319 142-1:2016 (ETSI EN 319 142-1:2016, IDT)
"Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 1. Структурні елементи та базові PAdES підписи", затверджений наказом державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 23 вересня 2016 року № 279.

6. ДСТУ ETSI EN 319 142-2:2016 (ETSI EN 319 142-2:2016, IDT)
"Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 2. Додаткові профілі підписів PAdES", затверджений наказом державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 23 вересня 2016 року № 279.

7. ДСТУ ETSI EN 319 132-1:2021 (ETSI EN 319 132-1 V1.1.1 (2016-04), IDT)
"Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 1. Структурні блоки та базові підписи XAdES", затверджений наказом державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 15 грудня 2021 року № 508.

8. ДСТУ ETSI EN 319 132-2:2021 (ETSI EN 319 132-2 V1.1.1 (2016-04), IDT)
"Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES", затверджений наказом державного підприємства

“Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 15 грудня 2021 року № 508.

9. ДСТУ ETSI EN 319 122-1:2021 (ETSI EN 319 122-1 V1.2.1 (2021-10), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES”, затверджений наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 21 грудня 2021 року № 523 (зі змінами).

10. ДСТУ ETSI EN 319 122-2:2021 (ETSI EN 319 122-2 V1.2.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES”, затверджений наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 21 грудня 2021 року № 523 (зі змінами).

11. ДСТУ ETSI EN 319 162-1:2021 (ETSI EN 319 162-1 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Контейнери пов’язаних підписів (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC”, затверджений наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 21 грудня 2021 року № 523.

12. ДСТУ ETSI EN 319 162-2:2021 (ETSI EN 319 162-2 V.1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Контейнери пов’язаних підписів (ASiC). Частина 2. Додаткові контейнери ASiC”, затверджений наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 21 грудня 2021 року № 523.

13. ДСТУ ETSI TS 119 132-3:2022 (ETSI TS 119 132-3 V1.1.1 (2021-01), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 3. Уведення механізмів синтаксису запису доказів (ERS) у XAdES”, затверджений наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 29 листопада 2022 року № 232.

14. ДСТУ ETSI TS 119 182-1:2022 (ETSI TS 119 182-1 V1.1.1 (2021-03), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи JAdES. Частина 1. Структурні блоки та базові підписи JAdES”, затверджений наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 29 листопада 2022 року № 232.

Всього прошито і скріплено печат
12 (двадцять) аркущ

Директор ТОВ «ФК «Форінт»

О.В. Васильєв

