Затверджено

Рішенням правління ПрАТ «Велта»

(Протокол № 1/2024 від 15.03.2024 року)

Порядок

створення і засвідчення електронної копії з паперового документа, паперової копії електронного документа; виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа, будь-яких змін електронного підпису після підписання електронного документа; використання електронного підпису та електронних печаток Страховика; виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа після використання електронної печатки, будь-яких змін електронної печатки після її використання для засвідчення електронного документа, електронної копії з паперового документа в Страховику

(внутрішній документ)

м. Київ - 2024 рік

1. Загальні положення

1.1. Цей Порядок створення і засвідчення електронної копії з паперового документа, паперової копії електронного документа; виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа, будь-яких змін електронного підпису після підписання електронного документа; використання електронного підпису та електронних печаток Страховика; виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа після використання електронної печатки, будь-яких змін електронної печатки після її використання для засвідчення електронного документа, електронної копії з паперового документа в Страховику є внутрішнім документом, розробленим з урахуванням вимог законодавства України Приватним акціонерним товариством «Велта» (далі - Страховик) і затверджений на виконання вимог Законів України «Про фінансові послуги та фінансові компанії», «Про страхування», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги», «Про електронну комерцію» та інших законів України у відповідності до вимог Положення про використання електронного підпису та електронної печатки (Постанова Правління Національного банку України від 20.12.2023р. №172), інших нормативно-правових актів Національного банку (далі - Регулятор) з питань регулювання ринків фінансових послуг та платіжних послуг і врегульовує питання визначені законодавством та вказаними нормативно-правовими актами Регулятора.

1.2. Терміни, що вживаються в цьому Порядку мають значення, визначені відповідними законами та нормативно-правовими актами Регулятора.

1.3. Процедури, зазначені в цьому Порядку описують використання тих видів електронного підпису та електронних печаток, які використовуються в Страховику.

1.4. Цей Порядок є обов’язковим для виконання всіма працівниками Страховика, його уповноваженими представниками та оформлений у вигляді одного документа.

1.5. До документів, зазначених у пункті 10 розділу І Положення про використання електронного підпису та електронної печатки (Постанова Правління Національного банку України від 20.12.2023р. №172), забезпечений безперешкодний доступ клієнтів Страховика та потенційних клієнтів Страховика шляхом розміщення цього порядку на власному офіційному вебсайті Страховика, включаючи його мобільну версію.

1.6. Відповідно до частини четвертої статті 20 Закону «Про електронну ідентифікацію та електронні довірчі послуги», якою врегульовано порядок надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, Наказом Міністерства цифрової трансформації України від 18 січня 2024 року №12 затверджені Особливості надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката шифрування, які визначають вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів, призначених виключно для використання в протоколі узгодження ключа шифрування, вимоги до процедур формування, зберігання, скасування, блокування, поновлення, надання інформації про статус кваліфікованих сертифікатів шифрування, надання доступу до сформованих кваліфікованих сертифікатів шифрування, а також вимоги до засобів криптографічного захисту інформації, що використовуються під час надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката шифрування, які забезпечують використання кваліфікованих сертифікатів шифрування.

2. Порядок створення і засвідчення електронної копії з паперового документа

2.1. Електронні копії з паперових документів створюються шляхом сканування оригіналів документів у паперовій формі з урахуванням таких вимог:

1) документ зберігається у файл формату pdf;
2) сканована копія кожного окремого документа зберігається як окремий файл;
3) документи, що містять більше однієї сторінки, зберігаються в один файл;
4) роздільна здатність сканування повинна бути не нижче ніж 300 dpi.

2.2. Оформлення електронної копії з паперового документа завершується накладанням кваліфікованого електронного підпису, що засвідчує відповідність оригіналу та накладається на документ з дотриманням вимог законодавства України у сфері електронних довірчих послуг та електронного документообігу (крім випадків, коли таке засвідчення не вимагається законодавством).

3. Порядок створення і засвідчення паперової копії електронного документа

3.1. Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому цим розділом.

3.2. Створення копій електронних документів та їх зберігання здійснюються у відповідності до Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затвердженому Наказом Міністерства юстиції України від 11.11.2014р. №1886/5 та Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затверджених наказом Міністерства юстиції України від 18 червня 2015 року № 1000/5.

3.3. Після перевірки цілісності та справжності електронний документ засобами периферійних пристроїв (багатофункціональні пристрої, принтери) роздруковується на папері з характеристиками електронного підпису/печатки.

3.4. Копія набуває юридичної сили лише у разі її засвідчення в установленому порядку.

3.5. Напис про засвідчення копії документа складається зі слів «Згідно з оригіналом», найменування посади, особистого підпису особи, яка засвідчує копію, її власного імені та прізвища, дати засвідчення копії та проставляється нижче реквізиту документа «Підпис», наприклад:

Згідно з оригіналом

Фахівець відділу страхування

Підпис	Власне ім’я ПРІЗВИЩЕ

Дата

Напис про засвідчення копії скріплюється печаткою Страховика або печаткою структурного підрозділу Страховика (за наявності).

Сторінки копії документів (за винятком тих, що мають один аркуш) нумеруються і відмітка про засвідчення копії може доповнюватися відміткою «Всього в копії _____ арк.». За рішенням Страховика або на вимогу особи, якій надається копія документа, допускається засвідчувати копії документів поаркушно.

3.6. Працівники Страховика мають право створювати та/або засвідчувати копії на папері з електронних документів у відповідності до наданих їм повноважень.

3.7. Під час створення засвідченої паперової копії електронного документа постійного та тривалого (понад 10 років) зберігання кожний реквізит, який оформлюється окремо від цього електронного документа, роздруковується на окремому аркуші разом з усією інформацію, визначеною в цьому пункті, для подальшого відтворення реквізиту, та засвідчується в порядку, визначеному для засвідчення електронного документа.

3.8. Одразу після завершення виконання/проведення експертизи цінності електронних документів постійного та тривалого (понад 10 років) зберігання створюються їх засвідчені паперові копії для формування їх у справи в паперовій формі та передавання на архівне зберігання. Переліки документів постійного та тривалого (понад 10 років), а також уповноважених засвідчувачів служби діловодства та структурних підрозділів, які здійснюють засвідчення копій документів постійного та тривалого (понад 10 років) зберігання, що створюються в електронній формі, затверджуються розпорядчим документом Страховика.

4. Порядок виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа та в електронному підпису після підписання електронного документа

4.1. У відповідності до статті 12 Закону «Про електронні документи та електронний документообіг» перевірка цілісності електронного документа проводиться шляхом підтвердження удосконаленого або кваліфікованого електронного підпису чи печатки, а в разі накладання на електронний документ електронного підпису чи печатки іншого виду - із застосуванням інших засобів і методів захисту інформації з дотриманням вимог законодавства у сфері захисту інформації.

4.2. Перевірка цілісності здійснюється як процедура, що дає змогу виявити будь-які зміни в електронному документі та зміни електронного підпису після підписання електронного документа.

4.3. Перевірка правового статусу електронного підпису здійснюється шляхом встановлення чинності сертифіката ключа підписувача на час підписання електронного документа та відповідності особистого ключа підписувача відкритому ключу, зазначеному у сертифікаті.

4.4. Сертифікат свідчить про справжність електронного підпису та гарантує запобігання його змінам, включаючи підробки та злом.

4.5. При використанні ключів будь-якого акредитованого центру сертифікації ключів перевірка електронного підпису здійснюється на сайті Центрального засвідчувального органу Міністерства цифрової трансформації України за допомогою державного он-лайн сервісу перевірки https://czo.gov.ua/verify

4.6. Також для перевірки Страховик може використовувати спеціальні захищені довідники сертифікатів відкритих ключів, які ведуться кваліфікованими надавачами електронних довірчих послуг, як то АЦСК Органів Юстиції України, АЦСК «Україна», АЦСК ІДД ДФС, АЦСК ПАТ «НДУ» тощо, та здійснює перевірку з використанням он-лайн сервісу або спеціалізованого програмного забезпечення/застосунку відповідного надавача.

4.7. Якщо електронний документ/електронна копія паперового документу були модифіковані, то перевірка їх цілісності виявить невідповідність накладеному електронному підпису, що буде свідчить про негативний результат – такий електронний документ буде вважатися недійсним. Позитивний результат перевірки цілісності електронного документу буде підтвердженням відсутності будь-яких змін у створеному і підписаному (за допомогою електронного підпису) електронному документі та дозволить зберегти оригінальний файл без підпису, файл з підписом та протокол створення та перевірки електронного підпису.

4.8. При роботі з електронними документами/електронними копіями паперових документів, якими обмінюються через сервіси електронного документообігу або за допомогою відповідного програмного забезпечення, відповідальні працівники Страховика за допомогою певних налаштувань перевіряють, чи дійсно електронний підпис відповідає документу та відкритому ключу, зазначеному у сертифікаті. Позитивний результат підтверджує цілісність даних. За наявності будь-яких змін в електронному підписі результати перевірки вважаються негативними і такий електронний документ визначається Страховиком недійсним.

4.9. Позначка часу при перевірці є важливим параметром для електронного документа/електронної копії паперового документу, адже вона дозволяє підтвердити достовірність підпису навіть після того, як строк чинності сертифіката завершився або його було анульовано чи відкликано.

4.10. Під час перевірки електронний підпис, незалежно від технологій, що застосовуються для створення електронного підпису, повинний відповідати таким умовам:

1) електронні дані, що використовуються для створення електронного підпису, є унікальними та однозначно пов’язані з підписувачем і не пов’язані з жодною іншою особою;

2) електронний підпис дає змогу однозначно ідентифікувати підписувача;

3) технологія використання електронного підпису забезпечує підписувачу під час підписання контроль електронних даних, які підписуються, та електронних даних, які використовуються для створення електронного підпису;

4) під час перевірки не виявлено будь-яких змін в електронному документі;

5) під час перевірки не виявлено будь-яких змін електронного підпису після підписання електронного документа.

5. Порядок використання електронних підписів та електронних печаток Страховика

5.1. Під час створення, оброблення та зберігання електронних документів Страховиком використовуються:

1) кваліфікований електронний підпис (далі - КЕП);

2) кваліфікована електронна печатка;

3) удосконалений електронний підпис (далі – УЕП) з кваліфікованим сертифікатом;

4) електронна печатка з кваліфікованим сертифікатом.

5.2. Використання клієнтом Страховика електронного підпису одноразовим ідентифікатором не передбачено. Використання клієнтом Страховика аналога власноручного підпису у сфері електронної комерції регулюється Законом «Про електронну комерцію» з дотриманням положень нормативно-правових актів Національного банку з питань укладення договорів в електронній формі.

5.3. Вимоги розділу VIII Положення про використання електронного підпису та електронної печатки (Постанова Правління Національного банку України від 20.12.2023р. №172) не поширюються на використання клієнтом аналога власноручного підпису у сфері електронної комерції.

5.4. Використання УЕП, удосконаленої електронної печатки та простого електронного підпису здійснюється на підставі договору між Страховиком і клієнтом / контрагентом або Страховиком і особою, що має намір стати клієнтом / контрагентом Страховика. Договір укладається в письмовій формі після проведення ідентифікації та верифікації відповідно до вимог законодавства України.

5.5. Страховик самостійно приймає рішення про використання того чи іншого виду електронного підпису та електронної печатки з дотриманням вимог законодавства України з питань електронних довірчих послуг, електронного документообігу, Положення про використання електронного підпису та електронної печатки (Постанова Правління Національного банку України від 20.12.2023р. №172), нормативно-правових актів Регулятора.

5.6. Страховик здійснює приймання, оброблення, зберігання, надсилання електронних документів та інформації, потрібної для створення електронних документів, з дотриманням вимог законодавства України щодо захисту персональних даних, таємниці страхування, таємниці фінансової послуги, комерційної таємниці, таємниці фінансового моніторингу.

5.7. Уповноважений представник Страховика під час взаємодії з клієнтом / контрагентом в разі створення електронних копій з паперових документів використовує КЕП уповноваженого представника з кваліфікованою електронною позначкою часу та/або кваліфіковану електронну печатку Страховика з кваліфікованою електронною позначкою часу.

5.8. Уповноважена відповідно до статутних документів Страховика особа / уповноважений представник Страховика для створення КЕП та УЕП з кваліфікованим сертифікатом використовує 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.

5.9. 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:

1) кваліфікований сертифікат відкритого ключа представника клієнта / контрагента установи містить код за Реєстром юридичної особи;

2) 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;

3) у кваліфікованому сертифікаті відкритого ключа представника клієнта / контрагента установи немає коду за Реєстром юридичної особи та в установи є в наявності всі потрібні документи, що підтверджують повноваження представника клієнта / контрагента установи щодо підписання відповідного документа від імені юридичної особи – клієнта / контрагента установи.

6. Порядок використання КЕП

6.1. Страховик забезпечує:

1) приймання, реєстрацію, підтвердження про отримання електронних документів із створеними КЕП з дотриманням вимог законодавства України у сфері електронного документообігу;

2) функціонування електронної поштової скриньки для приймання, реєстрації, підтвердження про отримання електронних документів із створеними КЕП клієнтів / контрагентів.

Страховик має право визначити додаткові канали електронної взаємодії, через які він забезпечує приймання, реєстрацію, підтвердження про отримання електронних документів із створеними КЕП, та забезпечити вільний доступ клієнтів / контрагентів та потенційних клієнтів / контрагентів до інформації про зазначені канали електронної взаємодії.

6.2. Підписувач не має права подавати один і той самий відкритий ключ кільком кваліфікованим надавачам електронних довірчих послуг для формування кваліфікованого сертифіката відкритого ключа.

6.3. Перевірка та підтвердження КЕП здійснюється відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

6.4. Кваліфікований сертифікат відкритого ключа повинен відповідати вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

6.5. Підписувач зобов’язаний використовувати кваліфіковану електронну позначку часу в разі підписування електронного документа КЕП.

6.6. Підписувач зобов’язаний під час створення КЕП перевірити чинність свого кваліфікованого сер тифіката відкритого ключа підписувача.

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

7. Порядок використання кваліфікованої електронної печатки

7.1. Створювач електронної печатки – суб’єкт електронної взаємодії не має права подавати один і той самий відкритий ключ кільком кваліфікованим надавачам електронних довірчих послуг для засвідчення його чинності.

7.2. Створювач електронної печатки – суб’єкт електронної взаємодії зобов’язаний використовувати кваліфіковану електронну печатку у випадках, визначених законодавством України.

7.3. Кваліфікована електронна печатка створюється, якщо:

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

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

3) потрібно підтвердити повноваження представника юридичної особи на використання електронного підпису у контексті, передбаченому документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення).

7.4. Створення кваліфікованих електронних печаток для електронних документів здійснює працівник суб’єкта електронної взаємодії, який має на це повноваження.

Страховик затверджує розпорядчим документом перелік працівників, яким надається право використання кваліфікованих електронних печаток для електронних документів.

7.5. Створювач електронної печатки – суб'єкт електронної взаємодії має право використовувати кваліфіковану електронну печатку в разі надання або отримання послуг в електронній формі або під час здійснення інформаційного обміну з іншими суб'єктами електронної взаємодії.

Створювач електронної печатки – суб'єкт електронної взаємодії, установчими документами якого не передбачена наявність печатки, має право використовувати кваліфіковану електронну печатку з метою підтвердження цілісності та походження інформації під час інформаційної взаємодії.

7.6. Кваліфікований сертифікат електронної печатки повинен відповідати вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та мати позначку, що цей сертифікат сформовано як кваліфікований для використання електронної печатки.

7.7. Перевірка та підтвердження кваліфікованої електронної печатки здійснюються відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

7.8. Створювач електронної печатки – суб'єкт електронної взаємодії має право використовувати більше ніж одну кваліфіковану електронну печатку.

7.9. Створювач електронної печатки – суб'єкт електронної взаємодії зобов'язаний забезпечити використання кваліфікованої електронної позначки часу у випадках створення кваліфікованої електронної печатки, визначених у пункті 63 розділу IX Положення про використання електронного підпису та електронної печатки (Постанова Правління Національного банку України від 20.12.2023р. №172).

7.10. Створювач електронної печатки зобов'язаний під час створення кваліфікованої електронної печатки здійснити перевірку чинності кваліфікованого сертифіката електронної печатки.

7.11. Перевірка чинності кваліфікованого сертифіката електронної печатки здійснюється відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

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

8. Порядок використання УЕП з кваліфікованим сертифікатом

8.1. Суб'єкти електронної взаємодії мають право використовувати УЕП з кваліфікованим сертифікатом у випадках, коли таке право встановлено законами України або нормативно-правовими актами Національного банку.

8.2. Суб'єкти електронної взаємодії не мають права використовувати УЕП з кваліфікованим сертифікатом у разі виконання хоча б однієї з таких умов:

1) УЕП з кваліфікованим сертифікатом не включений до переліку електронних підписів, які можуть використовуватися для підписання електронних документів згідно з вимогами нормативно-правових актів Національного банку;

2) аналоги електронних документів на паперових носіях повинні містити власноручний підпис відповідно до вимог законодавства України.

8.3. Суб'єкти електронної взаємодії для використання УЕП з кваліфікованим сертифікатом зобов'язані отримувати в кваліфікованого надавача електронних довірчих послуг кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

8.4. Страховик визначає можливість використання УЕП з кваліфікованим сертифікатом за результатами оцінки ризиків від використання такого виду ЕП, крім випадків, коли законодавством України встановлено обов'язок для суб'єктів електронної взаємодії використовувати УЕП з кваліфікованим сертифікатом.

8.5. Страховик при використанні УЕП з кваліфікованим сертифікатом забезпечує:

1) повідомлення клієнта, контрагента про можливість використання ними УЕП з кваліфікованим сертифікатом;

2) приймання, реєстрацію, підтвердження про отримання електронних документів із створеними УЕП з кваліфікованим сертифікатом з дотриманням вимог законодавства України у сфері електронного документообігу;

3) функціонування електронної поштової скриньки для приймання, реєстрації, підтвердження про отримання електронних документів із створеними УЕП з кваліфікованим сертифікатом клієнтів / контрагентів установи.

Страховик має право визначити додаткові канали електронної взаємодії, через які він забезпечує приймання, реєстрацію, підтвердження про отримання електронних документів із створеними УЕП з кваліфікованим сертифікатом, та забезпечити вільний доступ клієнтів / контрагентів та потенційних клієнтів / контрагентів до інформації про зазначені канали електронної взаємодії.

8.6. Підписувач не має права подавати один і той самий відкритий ключ кільком кваліфікованим надавачам електронних довірчих послуг для формування кваліфікованого сертифіката електронного підпису, що використовується для створення УЕП з кваліфікованим сертифікатом.

8.7. Перевірка та підтвердження УЕП з кваліфікованим сертифікатом здійснюються у межах отримання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки. У процесі підтвердження УЕП з кваліфікованим сертифікатом дійсність такого підпису підтверджується у разі виконання всіх таких умов:

1) використання для створення УЕП з кваліфікованим сертифікатом кваліфікованого сертифіката відкритого ключа підписувача, який відповідає вимогам, установленим Законом України «Про електронну ідентифікацію та електронні довірчі послуги»;

2) видачі кваліфікованого сертифіката відкритого ключа підписувача кваліфікованим надавачем електронних довірчих послуг та його чинності на момент створення УЕП з кваліфікованим сертифікатом;

3) відповідності значення відкритого ключа його значенню, яке міститься в кваліфікованому сертифікаті відкритого ключа підписувача;

4) правильного внесення унікального набору даних, які визначають підписувача, до кваліфікованого сертифіката відкритого ключа підписувача;

5) зазначення в кваліфікованому сертифікаті відкритого ключа підписувача про використання в ньому псевдоніма (у разі його використання особою на момент створення УЕП з кваліфікованим сертифікатом);

6) не порушено цілісності електронних даних, з якими пов’язаний цей УЕП з кваліфікованим сертифікатом;

7) дотримання вимог, установлених Законом України «Про електронну ідентифікацію та електронні довірчі послуги».

8.8. Кваліфікований сертифікат відкритого ключа, що використовується для створення УЕП з кваліфікованим сертифікатом, повинен відповідати вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

8.9. Підписувач зобов’язаний використовувати кваліфіковану електронну позначку часу в разі підписування електронного документа УЕП з кваліфікованим сертифікатом.

8.10. Підписувач зобов’язаний під час створення УЕП з кваліфікованим сертифікатом перевірити чинність свого кваліфікованого сертифіката відкритого ключа підписувача.

8.11. Перевірка чинності кваліфікованого сертифіката відкритого ключа здійснюється відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

8.12. Підписувачу забороняється створювати УЕП з кваліфікованим сертифікатом, якщо кваліфікований сертифікат відкритого ключа підписувача є нечинним або одержати інформацію про його статус неможливо.

9. Порядок використання електронної печатки з кваліфікованим сертифікатом

9.1. Суб’єкти електронної взаємодії мають право використовувати електронну печатку з кваліфікованим сертифікатом у випадках, коли законодавством України не передбачено обов’язку для суб’єктів електронної взаємодії використовувати виключно кваліфіковану електронну печатку. Суб’єкти електронної взаємодії використовують електронну печатку з кваліфікованим сертифікатом у випадках, коли законодавством України для суб’єктів електронної взаємодії встановлено обов’язок використовувати електронну печатку з кваліфікованим сертифікатом.

9.2. Суб’єкти електронної взаємодії для використання електронної печатки з кваліфікованим сертифікатом зобов’язані отримувати в кваліфікованого надавача електронних довірчих послуг кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

9.3. Створювач електронної печатки – суб’єкт електронної взаємодії не має права подавати один і той самий відкритий ключ кільком кваліфікованим надавачам електронних довірчих послуг для формування кваліфікованого сертифіката електронної печатки, що використовується для створення електронної печатки з кваліфікованим сертифікатом.

9.4. Електронна печатка з кваліфікованим сертифікатом створюється, якщо законодавством України передбачено:

1) засвідчення дійсності підпису на електронних документах електронною печаткою з кваліфікованим сертифікатом;

2) проставлення печатки для засвідчення відповідності копій документів оригіналам електронною печаткою з кваліфікованим сертифікатом;

3) використання електронної печатки з кваліфікованим сертифікатом для підтвердження повноваження представника юридичної особи на використання ЕП у контексті, визначеному документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення).

9.5. Створення електронних печаток з кваліфікованим сертифікатом для електронних документів здійснює працівник суб’єкта електронної взаємодії, який має на це повноваження.

Страховик затверджує внутрішнім документом перелік працівників, яким надається право використання електронних печаток з кваліфікованим сертифікатом для електронних документів.

9.6. Створювач електронної печатки – суб’єкт електронної взаємодії має право використовувати електронну печатку з кваліфікованим сертифікатом у разі надання або отримання послуг в електронній формі або під час здійснення інформаційного обміну з іншими суб’єктами електронної взаємодії.

Створювач електронної печатки – суб’єкт електронної взаємодії, установчими документами якого не передбачена наявність печатки, має право використовувати електронну печатку з кваліфікованим сертифікатом з метою підтвердження цілісності та походження інформації під час інформаційної взаємодії.

9.7. Перевірка та підтвердження електронної печатки з кваліфікованим сертифікатом здійснюється у межах отримання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки.

9.8. Дійсність електронної печатки з кваліфікованим сертифікатом підтверджується у разі виконання всіх таких умов:

1) використання для створення електронної печатки з кваліфікованим сертифікатом кваліфікованого сертифіката відкритого ключа створювача електронної печатки, який відповідає вимогам, установленим Законом;

2) видачі кваліфікованого сертифіката відкритого ключа створювача електронної печатки кваліфікованим надавачем електронних довірчих послуг та його чинності на момент створення електронної печатки з кваліфікованим сертифікатом;

3) відповідності значення відкритого ключа його значенню, яке міститься в кваліфікованому сертифікаті відкритого ключа створювача електронної печатки;

4) правильного внесення унікального набору даних, які визначають створювача електронної печатки, до кваліфікованого сертифіката відкритого ключа створювача електронної печатки;

5) не порушено цілісності електронних даних, з якими пов’язана ця електронна печатка з кваліфікованим сертифікатом;

6) дотримання вимог, установлених Законом України «Про електронну ідентифікацію та електронні довірчі послуги».

9.9. Створювач електронної печатки – суб’єкт електронної взаємодії має право використовувати більше ніж одну електронну печатку з кваліфікованим сертифікатом.

9.10. Створювач електронної печатки – суб’єкт електронної взаємодії зобов’язаний забезпечити використання електронної позначки часу у випадках створення електронної печатки з кваліфікованим сертифікатом, визначених у пункті 73 розділу X Положення про використання електронного підпису та електронної печатки (Постанова Правління Національного банку України від 20.12.2023р. №172).

9.11. Створювач електронної печатки зобов’язаний під час створення електронної печатки з кваліфікованим сертифікатом здійснити перевірку чинності відповідного кваліфікованого сертифіката електронної печатки.

9.12. Перевірка чинності кваліфікованого сертифіката електронної печатки здійснюється в межах отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

9.13. Створювачу електронної печатки забороняється створювати електронну печатку з кваліфікованим сертифікатом, якщо кваліфікований сертифікат електронної печатки є нечинним або одержати інформацію про його статус неможливо.

10. Порядок виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа після використання електронної печатки та в електронній печатці після її використання для засвідчення електронного документа, електронної копії з паперового документа

10.1. У відповідності до статті 12 Закону «Про електронні документи та електронний документообіг» перевірка цілісності електронного документа проводиться шляхом підтвердження удосконаленого або кваліфікованого електронного підпису чи печатки, а в разі накладання на електронний документ електронного підпису чи печатки іншого виду - із застосуванням інших засобів і методів захисту інформації з дотриманням вимог законодавства у сфері захисту інформації.

10.2. Перевірка цілісності здійснюється як процедура, що дає змогу виявити будь-які зміни в електронному документі та зміни електронної печатки після її накладання на електронний документ.

10.3. Перевірка правового статусу електронної печатки здійснюється шляхом встановлення чинності сертифіката ключа печатки на час її накладання на електронний документ та відповідності особистого ключа печатки відкритому ключу, зазначеному у сертифікаті.

10.4. Сертифікат свідчить про справжність електронної печатки та гарантує запобігання її змінам, включаючи підробки та злом.

10.5. При використанні ключів будь-якого акредитованого центру сертифікації ключів перевірка електронної печатки здійснюється на сайті Центрального засвідчувального органу Міністерства цифрової трансформації України за допомогою державного он-лайн сервісу перевірки https://czo.gov.ua/verify

10.6. Також для перевірки Страховик може використовувати спеціальні захищені довідники сертифікатів відкритих ключів, які ведуться кваліфікованими надавачами електронних довірчих послуг, як то АЦСК Органів Юстиції України, АЦСК «Україна», АЦСК ІДД ДФС, АЦСК ПАТ «НДУ» тощо, та здійснює перевірку з використанням он-лайн сервісу або спеціалізованого програмного забезпечення/застосунку відповідного надавача.

10.7. Якщо електронний документ/електронна копія паперового документу були модифіковані, то перевірка їх цілісності виявить невідповідність накладеній електронній печатці, що буде свідчить

про негативний результат – такий електронний документ буде вважатися недійсним. Позитивний результат перевірки цілісності електронного документу буде підтвердженням відсутності будь-яких змін у створеному і завіреному (за допомогою електронної печатки) електронному документі та дозволить зберегти оригінальний файл без підпису, файл з підписом та протокол створення та перевірки електронної печатки.

10.8. При роботі з електронними документами/електронними копіями паперових документів, якими обмінюються через сервіси електронного документообігу або за допомогою відповідного програмного забезпечення, відповідальні працівники Страховика за допомогою певних налаштувань перевіряють, чи дійсно електронна печатка відповідає документу та відкритому ключу, зазначеному у сертифікаті. Позитивний результат підтверджує цілісність даних. За наявності будь-яких змін в електронній печатці результати перевірки вважаються негативними і такий електронний документ визначається Страховиком недійсним.

10.9. Позначка часу при перевірці є важливим параметром для електронного документа/електронної копії паперового документу, адже вона дозволяє підтвердити достовірність печатки навіть після того, як строк чинності сертифіката завершився або його було анульовано чи відкликано.