Офіційно опубліковано 22.12.2023

Правління Національного банку України

П О С Т А Н О В А

20 грудня 2023 року Київ № 172

Про затвердження Положення про використання електронного підпису та електронної печатки

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статті 6 Закону України “Про електронні документи та електронний документообіг”, з метою визначення порядку використання електронного підпису та електронної печатки в банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк України, а також при наданні платіжних послуг Правління Національного банку України **постановляє:**

1. Затвердити Положення про використання електронного підпису та електронної печатки (далі – Положення), що додається.

2. Банк, небанківська фінансова установа, особа, яка не є фінансовою установою, але має право надавати окремі фінансові послуги, державне регулювання та нагляд за діяльністю якої здійснює Національний банк України, небанківський надавач платіжних послуг, оператор платіжної системи, технологічний оператор платіжних послуг (далі – установа) зобов’язані протягом трьох місяців з дня набрання чинності Положенням розробити та затвердити документацію для інформаційних систем установи, які використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів з обов’язковим описом реалізованих у цих інформаційних системах організаційних та технічних заходів безпеки інформації, якщо така документація не надана розробниками таких інформаційних систем.

3. Уповноважена відповідно до статутних документів установи особа / уповноважений колегіальний орган установи затверджує внутрішні документи, зазначені в пунктах 10, 11 розділу I Положення, протягом трьох місяців із дня набрання чинності Положенням.

4. На період воєнного стану на території України та протягом шести місяців з дня його припинення чи скасування дозволяється використання електронних підписів чи печаток, що базуються на сертифікатах відкритих ключів, виданих

кваліфікованими надавачами електронних довірчих послуг без відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки, користувачами електронних довірчих послуг для здійснення електронної взаємодії, електронної ідентифікації та автентифікації фізичних, юридичних осіб і представників юридичних осіб у випадках, коли законодавством України передбачено використання виключно кваліфікованих електронних підписів чи печаток (засобів кваліфікованого електронного підпису чи печатки, кваліфікованих електронних довірчих послуг) або засобів електронної ідентифікації з високим рівнем довіри, крім вчинення в електронній формі правочинів, що підлягають нотаріальному посвідченню та/або державній реєстрації у випадках, установлених законами України, та випадках, пов'язаних із високим ризиком для інформаційної безпеки, що визначається власниками відповідних інформаційних та інформаційно-комунікаційних систем з урахуванням обмежень, установлених абзацом другим частини другої статті 17 Закону України "Про електронні довірчі послуги".

5. Визнати такими, що втратили чинність:

1) постанову Правління Національного банку України від 14 серпня 2017 року № 78 "Про затвердження Положення про застосування електронного підпису та електронної печатки";

2) постанову Правління Національного банку України від 25 лютого 2019 року № 42 "Про внесення змін до Положення про застосування електронного підпису в банківській системі України";

3) постанову Правління Національного банку України від 13 грудня 2019 року № 151 "Про затвердження Положення про застосування цифрового власноручного підпису в банківській системі України";

4) постанову Правління Національного банку України від 30 липня 2020 року № 110 "Про внесення змін до Положення про застосування цифрового власноручного підпису в банківській системі України";

5) постанову Правління Національного банку України від 18 травня 2022 року № 100 "Про внесення змін до деяких нормативно-правових актів Національного банку України".

6. Департаменту безпеки (Олександр Паламарчук) після офіційного опублікування довести до відома банків України, учасників платіжного ринку, осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, інформацію про прийняття цієї постанови.

7. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Андрія Пишного.

8. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування, крім пунктів 1–3, 5 цієї постанови, які набирають чинності з 31 грудня 2023 року.

Голова Андрій ПИШНИЙ

Інд. 56

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
20 грудня 2023 року № 172

Положення про використання електронного підпису та електронної печатки

І. Загальні положення

1. Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про електронні документи та електронний документообіг", Закону України "Про електронну ідентифікацію та електронні довірчі послуги" (далі – Закон) і визначає порядок використання електронного підпису (далі – ЕП) та електронної печатки під час створення, оброблення та зберігання електронних документів у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк України (далі – Національний банк), а також при наданні платіжних послуг.

2. Терміни в цьому Положенні вживаються в такому значенні:

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

2) відкритий мережевий сервіс – мобільний застосунок, вебсервіс або інше програмне забезпечення, що дає змогу здійснювати обмін повідомленнями між електронними пристроями установ та користувачів через електронні комунікаційні мережі загального користування;

3) електронний підпис Національного банку (далі – ЕП Національного банку) – удосконалений електронний підпис (далі – УЕП) або удосконалена електронна печатка, що використовується в створених Національним банком платіжних системах, облікових системах, інформаційних системах;

4) електронний сенсорний пристрій – електронний пристрій із сенсорним екраном, на якому особа може створити цифровий власноручний підпис;

5) ідентифікація – заходи, що вживаються установою для встановлення особи шляхом отримання її ідентифікаційних даних;

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

7) 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;

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

9) простий електронний підпис (далі – простий ЕП) – будь-який вид ЕП, крім кваліфікованого ЕП, цифрового власноручного підпису (далі – ЦВП), УЕП з кваліфікованим сертифікатом, УЕП, ЕП Національного банку;

10) суб’єкт електронної взаємодії – Національний банк, установа, клієнт установи, контрагент установи та комерційний агент установи;

11) 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;

12) УЕП, що базується на кваліфікованому сертифікаті електронного підпису (далі – УЕП з кваліфікованим сертифікатом), – УЕП, створений з використанням кваліфікованого сертифіката електронного підпису, у якому немає відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки;

13) 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;

14) 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;

15) установа – банк, небанківська фінансова установа, особа, яка не є фінансовою установою, але має право надавати окремі фінансові послуги, державне регулювання та нагляд за діяльністю якої здійснює Національний банк, небанківський надавач платіжних послуг, оператор платіжної системи, технологічний оператор платіжних послуг;

16) цифровий власноручний підпис (далі – ЦВП) – електронний підпис, що є власноручним підписом фізичної особи, створеним на екрані електронного сенсорного пристрою.

Інші терміни в цьому Положенні використовуються в значеннях, наведених у Законі, Законах України “Про банки і банківську діяльність”, “Про електронні документи та електронний документообіг”, “Про платіжні послуги”, “Про фінансові послуги та фінансові компанії”, “Про електронну комерцію” та інших законах України і нормативно-правових актах Національного банку з питань регулювання ринків фінансових послуг та платіжних послуг.

3. Керівник установи відповідає за організацію використання ЕП та електронних печаток в установі, а також за використання ЕП та електронних печаток 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.

4. Вимоги цього Положення поширюються на суб’єктів електронної взаємодії.

5. ЕП є обов’язковим реквізитом електронного документа.

6. Вимоги цього Положення 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.

7. Установа зобов’язана забезпечити можливість перевірки цілісності та справжності електронних документів, створених з використанням технології, визначеної установою. Обов’язок доведення цілісності та справжності електронних документів, створених з використанням технології, визначеної

установою, покладається на установу (незалежно від технологічних можливостей і компетенцій персоналу установи).

8. Особа, що підписала електронний документ ЕП, у такий спосіб засвідчує, що ознайомилася 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, ознайомилася).

9. ЕП створюються в послідовності, визначеній застосованою технологією оброблення інформації, якщо електронний документ підписується двома або більше особами. Технологія оброблення інформації розробляється з урахуванням законодавства України та може визначатись у внутрішніх документах установи та/або в договорі, укладеному між установою та її клієнтом, контрагентом, комерційним агентом.

Створення електронного документа завершується створенням останнього ЕП відповідно до технології створення такого електронного документа.

10. Установа зобов’язана розробити з урахуванням вимог законодавства України внутрішні документи, у яких має встановлюватися порядок:

1) створення і засвідчення електронної копії з паперового документа;

2) створення і засвідчення паперової копії електронного документа;

3) виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа;

4) виявлення будь-яких змін ЕП після підписання електронного документа;

5) використання ЕП та електронних печаток установи;

6) виявлення будь-яких змін в електронному документі, в електронній копії з паперового документа після використання електронної печатки;

7) виявлення будь-яких змін електронної печатки після її використання для засвідчення електронного документа, електронної копії з паперового документа.

Процедури, зазначені в підпунктах 1–7 пункту 10 розділу І цього Положення, мають описувати використання тих видів ЕП та електронних печаток, які використовуються в установі.

Внутрішні документи, зазначені в пункті 10 розділу І цього Положення, є обов’язковими для виконання всіма працівниками установи й уповноваженими

представниками установи та можуть оформлятися у вигляді окремих документів, одного документа або бути частиною / частинами іншого / інших документа / документів.

Установа зобов'язана забезпечити до документів, зазначених у пункті 10 розділу I цього Положення, безперешкодний доступ клієнтів установи та потенційних клієнтів установи шляхом розміщення цих документів або витягів із них на всіх власних офіційних вебсайтах установи, включаючи їх мобільні версії, у мобільному (платіжному) застосунку та/або в приміщеннях установи / відокремлених підрозділах установи.

11. Установа зобов'язана з урахуванням вимог законодавства України у сфері захисту інформації, інформаційної безпеки та кіберзахисту розробити внутрішні документи, які встановлюють вимоги щодо надання, скасування та контролю доступу до інформаційних систем установи, що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів, і мають містити:

1) вимоги до ідентифікації, автентифікації, авторизації клієнтів установи;

2) послідовність дій під час управління доступом, послідовність дій під час управління віддаленим доступом (реєстрація, надання повноважень, перегляд та скасування доступу);

3) перелік типових функцій та прав доступу до інформаційних систем установи;

4) вимоги щодо здійснення заходів контролю доступу;

5) періодичність контролю наданих прав доступу;

6) вимоги до протоколювання дій під час управління доступом.

Установа зобов'язана забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем установи, що використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів.

Внутрішні документи, зазначені в пункті 11 розділу I цього Положення, є обов'язковими для виконання всіма працівниками установи й уповноваженими представниками установи та можуть оформлятися у вигляді окремих документів, одного документа або бути частиною / частинами іншого / інших документа / документів.

12. Банк додатково до вимог, установлених внутрішніми документами, перелік яких зазначено в підпунктах 1–6 пункту 11 розділу I цього Положення,

зобов’язаний забезпечити виконання вимог щодо забезпечення інформаційної безпеки в інформаційних системах, які використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів, визначених Положенням про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженим постановою Правління Національного банку України від 28 вересня 2017 року № 95, а також вимог інших нормативно-правових актів Національного банку у сфері захисту інформації, інформаційної безпеки та кіберзахисту.

Оператор платіжних систем, технологічний оператор платіжних послуг додатково до вимог, установлених внутрішніми документами, перелік яких зазначено в підпунктах 1–6 пункту 11 розділу I цього Положення, зобов’язаний забезпечити виконання вимог щодо забезпечення інформаційної безпеки в інформаційних системах, які використовуються для приймання, реєстрації, оброблення, зберігання, надсилання електронних документів, визначених Положенням про захист інформації та кіберзахист учасниками платіжного ринку, затвердженим постановою Правління Національного банку України від 19 травня 2021 року № 43 (зі змінами), а також вимог інших нормативно-правових актів Національного банку у сфері захисту інформації, інформаційної безпеки та кіберзахисту.

13. ЕП має юридичну силу незалежно від технологій, що застосовуються для створення ЕП, якщо відповідає таким умовам:

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

2) ЕП дає змогу однозначно ідентифікувати підписувача;

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

4) під час перевірки відповідно до затвердженого в установі порядку не виявлено будь-яких змін в електронному документі;

5) під час перевірки відповідно до затвердженого в установі порядку не виявлено будь-яких змін ЕП після підписання електронного документа.

14. Національний банк має право перевіряти дотримання установою вимог цього Положення, а також здійснювати перевірки інформаційно-комунікаційних систем, що використовуються установами для доведення цілісності та справжності електронних документів.

ІІ. Види електронного підпису та електронної печатки

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

1) кваліфікований ЕП (далі – КЕП);

2) ЦВП;

3) УЕП з кваліфікованим сертифікатом;

4) УЕП;

5) ЕП Національного банку;

6) простий ЕП;

7) кваліфікована електронна печатка;

8) електронна печатка з кваліфікованим сертифікатом;

9) удосконалена електронна печатка.

16. Використання клієнтом установи електронного підпису одноразовим ідентифікатором та аналога власноручного підпису у сфері електронної комерції регулюється Законом України “Про електронну комерцію” з дотриманням положень нормативно-правових актів Національного банку з питань укладення договорів в електронній формі. Вимоги розділу VIII цього Положення не поширюються на використання клієнтом установи електронного підпису одноразовим ідентифікатором та аналога власноручного підпису у сфері електронної комерції.

17. Використання УЕП, удосконаленої електронної печатки та простого ЕП здійснюється на підставі договору між установою і клієнтом / контрагентом установи або установою і особою, що має намір стати клієнтом / контрагентом установи. Договір укладається в письмовій формі після проведення ідентифікації та верифікації відповідно до вимог законодавства України клієнта / контрагента установи чи особи, що має намір стати клієнтом / контрагентом установи:

1) у формі паперового документа з власноручними підписами сторін або

2) як електронний документ із КЕП сторін, або

3) як електронний документ з УЕП із кваліфікованим сертифікатом клієнта / контрагента установи та КЕП уповноваженого представника установи, або

4) як електронний документ із ЦВП фізичної особи, визначеної в абзацах першому, третьому пункту 33 розділу IV цього Положення, та КЕП уповноваженого представника установи, з дотриманням вимог розділу IV цього Положення щодо використання ЦВП, або

5) як електронний документ із використанням будь-яких видів ЕП, щодо яких між клієнтом / контрагентом установи та установою вже укладено договір відповідно до вимог одного з підпунктів 1–4 пункту 17 розділу II цього Положення.

Договір про використання УЕП, удосконаленої електронної печатки та простого ЕП має містити умови та порядок (процедуру) визнання установою і клієнтом / контрагентом установи правочинів у вигляді електронних документів із використанням УЕП, удосконаленої електронної печатки або простого ЕП відповідно.

Договір має також містити умови щодо розподілу ризиків збитків, що можуть бути заподіяні підписувачам і третім особам у разі використання простого ЕП, УЕП або удосконаленої електронної печатки відповідно.

Укладення окремого договору щодо використання клієнтом установи КЕП, ЦВП, УЕП з кваліфікованим сертифікатом, кваліфікованої електронної печатки, електронної печатки з кваліфікованим сертифікатом не вимагається за умови дотримання вимог цього Положення.

18. 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.

Установа зобов’язана надати клієнтові / контрагенту установи на його вимогу засвідчену паперову копію електронного документа.

19. Установа самостійно приймає рішення про використання того чи іншого виду ЕП та електронної печатки з дотриманням вимог законодавства України з питань електронних довірчих послуг, електронного документообігу, цього Положення, нормативно-правових актів Національного банку.

20. Установа здійснює приймання, оброблення, зберігання, надсилання електронних документів та інформації, потрібної для створення електронних документів, з дотриманням вимог законодавства України щодо захисту персональних даних, банківської таємниці, таємниці страхування, таємниці

фінансової послуги, комерційної таємниці, таємниці надавача платіжних послуг, таємниці фінансового моніторингу.

21. Установа / комерційний агент установи має право використовувати відкриті мережеві сервіси для отримання інформації з обмеженим доступом, визначеної в пункті 20 розділу ІІ цього Положення, якщо:

1) електронна взаємодія здійснюється виключно між установою та клієнтом / контрагентом установи або між комерційним агентом установи та клієнтом установи;

2) установа / комерційний агент установи попередньо отримала / отримав письмовий дозвіл від клієнта / контрагента установи на здійснення таких дій;

3) установа / комерційний агент установи забезпечує виконання вимог законодавства України у сфері захисту інформації, інформаційної безпеки та кіберзахисту.

Установа визначає технологію використання відкритих мережевих сервісів для отримання інформації з обмеженим доступом, визначеної в пункті 20 розділу ІІ цього Положення, та в разі порушення вимог законодавства України несе відповідальність за шкоду, заподіяну клієнтові / контрагенту установи під час використання запровадженої установою технології.

Установа доводить факт добровільного передавання клієнтом / контрагентом установи інформації з обмеженим доступом, визначеної в пункті 20 розділу ІІ цього Положення, у разі заперечення ним факту добровільного передавання такої інформації.

22. 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 кваліфіковану електронну печатку установи з кваліфікованою електронною позначкою часу.

23. Створення електронних документів постійного і тривалого (понад 10 років) зберігання здійснюється із використанням КЕП уповноваженої відповідно до статутних документів установи особи / уповноваженого представника установи та/або кваліфікованої електронної печатки установи, що забезпечують можливість перевірки відповідних КЕП та/або кваліфікованої електронної печатки 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 цього Положення.

24. 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.

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.

25. 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:

1) зміни даних, внесених у кваліфікований сертифікат відкритого ключа представника юридичної особи;

2) звільнення працівника юридичної особи;

3) припинення представництва юридичної особи.

III. Використання КЕП

26. Установа зобов’язана забезпечити:

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 установи.

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

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

28. Перевірка та підтвердження КЕП здійснюється відповідно до вимог Закону.

29. Кваліфікований сертифікат відкритого ключа повинен відповідати вимогам Закону.

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

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

Перевірка чинності кваліфікованого сертифіката відкритого ключа підписувача здійснюється відповідно до вимог Закону.

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

IV. Використання ЦВП

31. Вимоги розділу IV цього Положення поширюються на банки та їхніх клієнтів для підписання електронних документів.

32. Вимоги розділу IV цього Положення поширюються на:

1) страховиків;

2) ломбарди;

3) кредитні спілки;

4) лізингові компанії;

5) фінансові установи (крім тих, які надають послуги з надання гарантій та з факторингу);

6) небанківських надавачів фінансових платіжних послуг:
платіжні установи (включаючи малі платіжні установи);
філії іноземних платіжних установ;
установи електронних грошей;
філії іноземних установ електронних грошей;
фінансові установи, що мають право на надання платіжних послуг;
операторів поштового зв'язку, що мають право надавати фінансові платіжні послуги.

Для установ, визначених у підпунктах 1–6 пункту 32 розділу IV цього Положення, та установ, що діють від їхнього імені, вимоги розділу IV цього Положення поширюються виключно в разі фізичної присутності їхніх клієнтів у приміщеннях зазначених установ чи установ, що діють від імені зазначених установ, для укладання / підписання договорів, підписання касових документів, які оформляються для здійснення касових операцій.

33. Фізична особа, що є клієнтом установи або має намір стати клієнтом установи, та не є фізичною особою-підприємцем, суб'єктом, який провадить незалежну професійну діяльність або уповноваженим представником юридичної особи, фізичної особи-підприємця, суб'єкта, який провадить незалежну професійну діяльність, має право використовувати ЦВП для підписання електронних документів під час електронної взаємодії виключно з установою / комерційним агентом установи з дотриманням вимог цього Положення.

Фізична особа-підприємець, що є клієнтом установи, суб'єкт, який провадить незалежну професійну діяльність, що є клієнтом установи, фізична особа, що є представником клієнта установи (представником юридичної особи, фізичної особи-підприємця, суб'єкта, який провадить незалежну професійну діяльність), має право використовувати ЦВП для підписання електронних документів під час електронної взаємодії виключно з установою / комерційним агентом установи з дотриманням вимог цього Положення та виключно у

випадках, установлених нормативно-правовими актами Національного банку.

Фізична особа, яка є представником фізичної особи, що є клієнтом установи або має намір стати клієнтом установи, має право використовувати ЦВП для підписання електронних документів під час електронної взаємодії виключно з установою / комерційним агентом установи з дотриманням вимог цього Положення та виключно у випадках, установлених нормативно-правовими актами Національного банку.

34. Установа самостійно визначає технологію створення електронних документів з ЦВП та забезпечує дотримання вимог цього Положення.

Установа зобов'язана забезпечити дотримання таких вимог під час створення електронного документа з ЦВП підписувача:

1) проведення ідентифікації та верифікації підписувача відповідно до вимог законодавства України;

2) ознайомлення підписувача з текстом документа перед його підписанням ЦВП;

3) підписання ЦВП саме того документа, з яким ознайомився підписувач;

4) нерозривне поєднання ЦВП з електронним документом, підписаним цим ЦВП;

5) автоматичне створення кваліфікованої електронної позначки часу для електронного документа відразу після його підписання ЦВП;

6) здійснення перевірки ЦВП підписувача на його відповідність зразку власноручного підпису в паспорті підписувача або в іншому документі, що містить підпис особи / відцифрований підпис особи і посвідчує особу підписувача та відповідно до законодавства України може бути використаним на території України для укладення правочинів, або в картці зразків підписів – у випадках, визначених нормативно-правовими актами Національного банку. Якщо ЦВП підписувача не відповідає зразку власноручного підпису в паспорті підписувача або в іншому документі, що містить підпис особи / відцифрований підпис особи, і посвідчує особу підписувача та відповідно до законодавства України може бути використаним на території України для укладення правочинів, уповноважений представник установи зобов'язаний припинити процедуру створення електронного документа з ЦВП підписувача;

7) підписання електронного документа уповноваженим представником установи з використанням КЕП з кваліфікованою електронною позначкою часу та/або засвідчення електронного документа кваліфікованою електронною

печаткою установи з кваліфікованою електронною позначкою часу;

8) фіксування дій підписувача та уповноважених представників установи, пов'язаних зі створенням електронних документів з ЦВП, в електронному журналі подій, захищеному від модифікації та знищення;

9) конфіденційність усіх даних, що передаються між електронним сенсорним пристроєм та інформаційною системою установи.

Установа має право не застосовувати вимог підпунктів 1, 6 пункту 34 розділу IV цього Положення, якщо нормативно-правовим актом Національного банку не встановлено обов'язку ідентифікувати / верифікувати підписувача.

35. Установа після створення електронного документа з ЦВП зобов'язана забезпечити захист цього ЦВП від подальшого знищення, копіювання, розповсюдження, модифікації.

36. Установа зобов'язана забезпечити застосовування антивірусного захисту в інформаційній системі установи та на електронному сенсорному пристрої установи, який використовується для створення ЦВП.

37. Перелік подій, що фіксуються в електронному журналі подій, визначається установою з урахуванням можливості надалі:

1) підтвердити факт, дату і час підписання документа ЦВП особою, визначеною в пункті 33 розділу IV цього Положення, та уповноваженим представником установи;

2) підтвердити факт попереднього ознайомлення підписувача з текстом документа, що підписувався;

3) надавати інформацію щодо процесу підписання конкретного документа та доведення достовірності такої інформації на запит уповноважених державних органів у випадках, установлених законами України, або за рішенням суду.

38. Установа має право застосовувати процедури фото та/або відеофіксації, інші процедури з метою документування та контролю за процесом підписання документа клієнтом установи з використанням ЦВП. Застосування зазначених процедур повинно здійснюватися за умови попередньо отриманої згоди клієнта.

Установа не має права без згоди клієнта використовувати для інших цілей або передавати іншим особам інформацію, отриману установою під час процедури документування процесу підписання підписувачем документа ЦВП, крім випадків, передбачених законами України.

39. Установа зобов’язана зберігати інформацію, зафіксовану під час процесу створення електронного документа з ЦВП, до завершення строку зберігання електронного документа, з яким пов’язана зазначена інформація, відповідно до вимог законодавства України.

40. Установа забезпечує доведення цілісності електронного документа та авторство ЦВП підписувача в разі заперечення підписувачем факту підписання електронного документа або оспорювання окремих частин електронного документа.

41. Установа несе відповідальність за шкоду, заподіяну підписувачу внаслідок порушення нею вимог законодавства України щодо технології створення електронного документа з ЦВП.

42. Спірні питання стосовно документів, підписаних ЦВП, вирішуються між установою та підписувачем у порядку, установленому законодавством України.

43. Уповноважений представник установи не має права використовувати ЦВП для підписання електронних документів від імені установи.

V. Використання УЕП з кваліфікованим сертифікатом

44. 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.

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 ЕП, 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.

45. 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.

46. Установа 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.

Установа, яка використовує УЕП з кваліфікованим сертифікатом, зобов'язана забезпечити:

1) повідомлення клієнта установи, контрагента установи 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.

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

47. 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.

48. 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;

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.

49. Кваліфікований сертифікат відкритого ключа, що використовується для створення УЕП з кваліфікованим сертифікатом, повинен відповідати вимогам Закону.

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

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

Перевірка чинності кваліфікованого сертифіката відкритого ключа здійснюється відповідно до вимог Закону.

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

VI. Використання УЕП

51. Установи та їх клієнти під час вчинення правочинів у вигляді електронних документів мають право використовувати УЕП на підставі договору з урахуванням вимог пункту 17 розділу II цього Положення.

52. Установа визначає технологію використання УЕП та засоби удосконаленого електронного підпису чи печатки, що використовуються під час взаємодії установи з клієнтом установи.

53. Суб’єкти електронної взаємодії використовують УЕП без сертифіката відкритого ключа або чинність відкритого ключа підписувача засвідчується сертифікатом відкритого ключа на договірних засадах, або чинність відкритого ключа підписувача засвідчується надавачем електронних довірчих послуг згідно з вимогами нормативно-правових актів Національного банку у сфері електронних довірчих послуг.

54. УЕП є таким, що пройшов перевірку, якщо виконуються всі такі вимоги:

1) перевірку УЕП здійснено згідно з процедурою, зазначеною в договорі, укладеному між суб’єктами електронної взаємодії;

2) УЕП відповідає вимогам, визначеним Законом.

VII. Використання ЕП Національного банку

55. Використання ЕП Національного банку суб’єктами електронної взаємодії дозволяється тільки у створених Національним банком платіжних системах, облікових системах, інформаційних системах і з обов’язковим використанням засобів криптографічного захисту інформації Національного банку.

56. ЕП Національного банку є таким, що пройшов перевірку та отримав підтвердження, якщо:

1) перевірку ЕП Національного банку проведено засобом захисту інформації, визначеним Національним банком;

2) засіб захисту інформації, визначений Національним банком, надав повідомлення про позитивний результат перевірки ЕП Національного банку.

VIII. Використання простого ЕП

57. Клієнт установи, контрагент установи має право використовувати простий ЕП у разі дотримання таких вимог:

1) електронна взаємодія здійснюється виключно з цією установою та з використанням технології, визначеної установою;

2) використання простого ЕП здійснюється на підставі договору відповідно до вимог пункту 17 розділу II цього Положення.

58. Простий ЕП має забезпечувати однозначну ідентифікацію особи підписувача.

59. Доведення цілісності електронних документів із створеним простим ЕП може забезпечуватися засобами інформаційної системи, у якій здійснюється створення, оброблення, зберігання електронних документів.

60. Установа забезпечує доведення цілісності, достовірності та авторства електронного документа зі створеним простим ЕП.

Установа в разі недотримання зазначеної вимоги несе відповідальність за шкоду, заподіяну клієнтові установи.

IX. Використання кваліфікованої електронної печатки

61. 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.

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

63. 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 ЕП у контексті, передбаченому документом (підписання, затвердження, погодження, візування, засвідчення, ознайомлення).

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

Установа зобов'язана затвердити розпорядчим документом перелік працівників установи, яким надається право використання кваліфікованих електронних печаток для електронних документів.

65. 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.

66. Кваліфікований сертифікат електронної печатки повинен відповідати вимогам Закону та мати позначку, що цей сертифікат сформовано як кваліфікований для використання електронної печатки.

67. Перевірка та підтвердження кваліфікованої електронної печатки здійснюються відповідно до вимог Закону.

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

69. 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 цього Положення.

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

Перевірка чинності кваліфікованого сертифіката електронної печатки здійснюється відповідно до вимог Закону.

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

X. Використання електронної печатки з кваліфікованим сертифікатом

70. 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.

71. 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.

72. 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.

73. 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).

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

Установа зобов'язана затвердити внутрішнім документом перелік працівників установи, яким надається право використання електронних печаток з кваліфікованим сертифікатом для електронних документів.

75. 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.

76. 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.

77. 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.

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

79. 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 цього Положення.

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

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.

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

XI. Використання удосконаленої електронної печатки

80. Установа має право використовувати удосконалену електронну печатку для внутрішнього документообігу на підставі свого внутрішнього документа.

81. Створювач електронної печатки – суб'єкт електронної взаємодії має право використовувати удосконалену електронну печатку в разі надання або отримання послуг в електронній формі або під час здійснення інформаційного обміну з іншими суб'єктами електронної взаємодії на підставі договору з урахуванням вимог пункту 17 розділу II цього Положення.

82. Установа визначає технологію використання удосконаленої електронної печатки та засоби удосконаленого електронного підпису чи печатки, що використовуються під час взаємодії установи з клієнтом установи, контрагентом установи.

83. Удосконалена електронна печатка створюється, якщо відповідно до умов договору потрібно:

1) засвідчити дійсність підпису на електронних документах;

2) проставити печатку для засвідчення відповідності копій документів оригіналам;

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

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

Додаток
до Положення про використання
електронного підпису та
електронної печатки
(пункт 23 розділу II)

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.