

ЗАТВЕРДЖЕНО  
постановою Кабінету Міністрів України  
від 2018 р. №

## **ВИМОГИ** **у сфері електронних довірчих послуг**

### **Розділ I. Загальні положення**

#### **1. Сфера дії**

1. Вимоги до надання кваліфікованих електронних довірчих послуг визначають організаційно-методологічні технічні та технологічні умови, яких повинен дотримуватись кваліфікований надавач електронних довірчих послуг (далі – надавач), його відокремлені пункти реєстрації під час надання кваліфікованих електронних довірчих послуг їх користувачам.

2. Центральний засвідчувальний орган надає кваліфіковані електронні довірчі послуги відповідно до цих Вимог з урахуванням особливостей, передбачених Законом України «Про електронні довірчі послуги».

3. Дія цих Вимог не поширюється на надавачів електронних довірчих послуг, що не мають наміру надавати кваліфіковані електронні довірчі послуги, а також на надавачів, внесених до Довірчого списку за поданням засвідчувального центру, та програмно-технічні комплекси, що використовуються ними під час надання кваліфікованих електронних довірчих послуг у банківській системі України та при здійсненні переказу коштів.

#### **2. Визначення термінів**

4. Терміни, що вживаються в цих Вимогах, мають таке значення:

власник веб-сайту – користувач кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

геш-значення – фіксовані за обсягом електронні дані, утворені шляхом перетворення електронних даних із застосуванням криптографічного алгоритму;

гешування – перетворення будь-якого обсягу електронних даних в електронні дані фіксованого обсягу шляхом застосування криптографічного алгоритму;

заявник – фізична особа або представник юридичної особи, що звернулась до надавача для отримання кваліфікованих електронних довірчих послуг;

інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем надавача або центрального засвідчувального органу, які у процесі обробки інформації діють як єдине ціле та об'єднують програмно-технічний комплекс, що використовується під час надання кваліфікованих електронних довірчих послуг (далі – програмно-технічний комплекс), фізичне середовище, інформацію, що обробляється в цих системах, а також найманих працівників надавача або центрального засвідчувального органу, які безпосередньо задіяні у наданні кваліфікованих електронних довірчих послуг або обслуговують програмно-технічний комплекс (далі – наймані працівники);

кваліфікована електронна довірча послуга – електронна довірча послуга, надання якої забезпечує надавач, його відокремлені пункти реєстрації або центральний засвідчувальний орган за допомогою засобу кваліфікованого електронного підпису чи печатки та базується на кваліфікованому сертифікаті відкритого ключа;

користувач – особа, яка на підставі договору або іншого документа отримує у надавача кваліфіковану електронну довірчу послугу;

об'єктний ідентифікатор – унікальний буквено-числовий чи числовий ідентифікатор, зареєстрований у відповідному стандарті Міжнародної організації із стандартизації для певного класу об'єктів або об'єктів;

он-лайн операція – будь-яка дія, технологічна схема якої передбачає наявність безперервного телекомунікаційного зв'язку в режимі реального часу під час її виконання;

політика сертифіката (certificate policy) – перелік усіх правил, що застосовуються надавачем у процесі надання кваліфікованих електронних довірчих послуг з обслуговування кваліфікованих сертифікатів відкритих ключів, включаючи положення цих Вимог;

положення сертифікаційних практик (certification practice statement) – перелік усіх практичних дій та процедур, які застосовуються для реалізації політики сертифіката надавача;

публікація кваліфікованого сертифіката відкритого ключа – надання кваліфікованого сертифіката відкритого ключа користувачу та у разі його згоди іншим особам шляхом розміщення на офіційному веб-сайті надавача;

регламент роботи – нормативний документ надавача або центрального засвідчувального органу, що визначає організаційно-методологічні, технічні та технологічні умови діяльності надавача або центрального засвідчувального органу під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик;

розповсюдження інформації про статус кваліфікованого сертифіката відкритого ключа – надання вільного доступу до інформації про статус кваліфікованого сертифіката відкритого ключа;

список відкликаних сертифікатів – сформований та опублікований надавачем перелік кваліфікованих сертифікатів відкритих ключів, статус яких змінено на блокований, поновлений або скасований;

статус кваліфікованого сертифіката відкритого ключа – стан кваліфікованого сертифіката відкритого ключа (чинний, блокований, скасований) на певний момент часу;

управління статусом сертифіката – зміна статусу кваліфікованого сертифіката відкритого ключа надавачем.

5. Інші терміни вживаються у значеннях, наведених у законах України «Про електронні довірчі послуги», «Про електронні документи та електронний документообіг», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України».

## **Розділ II. Вимоги до надавачів**

### **1. Вимоги до найманих працівників надавача**

1. До посад найманих працівників надавача, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, належать:

- 1) адміністратор реєстрації;
- 2) адміністратор сертифікації;
- 3) адміністратор безпеки;
- 4) системний адміністратор;
- 5) адміністратор аудиту.

Забороняється суміщення посади адміністратора безпеки та адміністратора аудиту з іншими посадами найманих працівників надавача, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг.

2. Наймані працівники надавача повинні мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію.

На посаду адміністратора сертифікації, адміністратора безпеки, системного адміністратора та адміністратора аудиту може бути призначена особа, яка має вищу освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом в зазначених сферах не менше 3 років.

3. Організаційно-правовий статус керівника та найманих працівників надавача, їх функції та завдання, права та обов'язки, відповідальність в межах організації, а також професійні знання, досвід та кваліфікацію визначають посадові інструкції.

Посадові інструкції повинні містити вимоги інформаційної безпеки та методи її забезпечення.

4. Керівник та наймані працівники надавача повинні бути ознайомлені з положеннями їх посадових інструкцій та діяти відповідно до своїх посадових функцій та завдань.

5. Адміністратор реєстрації відповідає за перевірку документів, наданих заявниками, їх заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

6. Основними обов'язками адміністратора реєстрації є:

- 1) ідентифікація та автентифікація заявників;
- 2) перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;
- 3) встановлення належності відкритого ключа та відповідного йому особистого ключа заявнику;
- 4) ведення обліку користувачів.

7. Адміністратор сертифікації відповідає за формування кваліфікованих сертифікатів відкритих ключів, ведення електронного реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, збереження та використання особистих ключів надавача, а також створення їх резервних копій.

8. Основними обов'язками адміністратора сертифікації є:

- 1) участь у генерації пар ключів надавача та створенні резервних копій особистих ключів надавача;
- 2) зберігання особистих ключів надавача та їх резервних копій;
- 3) забезпечення використання особистих ключів надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів надавача та користувачів;

4) перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів надавача вимогам регламенту роботи центрального засвідчувального органу;

5) участь у знищенні особистих ключів надавача;

6) забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів користувачів;

7) забезпечення публікації кваліфікованих сертифікатів відкритих ключів користувачів та списків відкликаних сертифікатів на офіційному веб-сайті надавача;

8) створення резервних копій кваліфікованих сертифікатів відкритих ключів користувачів;

9) зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів інформаційно-телекомунікаційної системи надавача.

9. Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою.

10. Основними обов'язками адміністратора безпеки є:

1) участь у генерації пар ключів надавача та створенні резервних копій особистих ключів надавача;

2) контроль за формуванням, обслуговуванням та створенням резервних копій кваліфікованих сертифікатів відкритих ключів надавача, користувачів та списків відкликаних сертифікатів;

3) контроль за зберіганням особистих ключів надавача та їх резервних копій, особистих ключів адміністраторів;

4) участь у знищенні особистих ключів надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;

5) організація розмежування доступу до ресурсів інформаційно-телекомунікаційної системи надавача;

6) забезпечення спостереження за функціонуванням комплексної системи захисту інформації або системи управління інформаційною безпекою (реєстрація подій в інформаційно-телекомунікаційній системі надавача, моніторинг подій тощо);

7) забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою після збоїв, відмов, аварій інформаційно-телекомунікаційної системи надавача;

8) забезпечення режиму доступу до приміщень надавача, в яких розміщена інформаційно-телекомунікаційна система надавача;

9) ведення журналів обліку адміністратора безпеки, передбачених документацією на комплексну систему захисту інформації або звітності, що передбачена системою управління інформаційною безпекою.

11. Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу (далі – технічні засоби) інформаційно-телекомунікаційної системи надавача.

12. Основними обов'язками системного адміністратора є:

1) організація експлуатації та технічного обслуговування інформаційно-телекомунікаційної системи надавача і адміністрування її технічних засобів;

2) забезпечення функціонування офіційного веб-сайту надавача;

3) участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою;

4) ведення журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;

5) встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення інформаційно-телекомунікаційної системи надавача;

6) встановлення та налагодження штатної підсистеми резервного копіювання бази даних інформаційно-телекомунікаційної системи надавача;

7) забезпечення актуалізації баз даних, створюваних та оброблюваних в інформаційно-телекомунікаційній системі надавача, внаслідок збоїв.

13. Адміністратор аудиту відповідає за здійснення перевірок дотримання найманими працівниками надавача вимог внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою. Надавач встановлює періодичність (у днях, тижнях або місяцях) проведення таких внутрішніх перевірок, але не рідше ніж один раз на 6 місяців.

14. Обов'язки адміністратора аудиту:

1) здійснення перевірок журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;

2) здійснення перевірок відповідності внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою;

3) контроль за дотриманням найманими працівниками надавача внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою;

4) контроль за веденням баз даних надавача;

5) контроль за веденням архіву надавача.

15. Наймані працівники надавача повинні бути повідомлені про зміни в організації процесів надавача, що стосуються їх посадових обов'язків.

16. Керівник надавача зобов'язаний створити умови для безперервної особистої освіти та забезпечити постійне підвищення кваліфікації найманих працівників надавача у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних.

17. Керівником надавача має бути встановлена чітка система дисциплінарних стягнень за недотримання найманими працівниками надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою.

## **2. Вимоги до використання особистих ключів надавача**

18. Генерація пари ключів надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

Генерація пари ключів надавача здійснюється виключно за допомогою засобу кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм.

19. Всі події, пов'язані із генерацією, використанням та знищенням пари ключів надавача, повинні протоколюватися.

20. Особисті ключі надавача повинні розміщуватися у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів.

Технологія зберігання особистих ключів надавача повинна забезпечити неможливість доступу до них ззовні у відношенні до засобу кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм.

21. У разі здійснення резервного копіювання особисті ключі надавача повинні бути перенесені на зовнішній носій (пристрій) у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

Резервне копіювання та відновлення особистих ключів надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

22. Умови забезпечення захисту резервних копій особистих ключів надавача під час їх зберігання повинні бути не нижче, ніж умови забезпечення захисту особистих ключів, що знаходяться у використанні.

23. Особисті ключі надавача можуть використовуватися виключно для формування кваліфікованих сертифікатів відкритих ключів (накладання кваліфікованого електронного підпису чи печатки на кваліфікований сертифікат відкритого ключа) та інформації про статус кваліфікованого сертифіката відкритого ключа.

24. Особисті ключі надавача можуть використовуватися виключно у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, розташованим в окремому, спеціально призначеному для цього, приміщенні.

25. Після закінчення терміну дії кваліфікованого сертифіката відкритого ключа надавача особистий ключ надавача та всі його резервні копії знищуються способом, що не дозволяє їх відновлення.

### **3. Вимоги щодо страхування від збитків, які можуть бути завдані надавачем внаслідок неналежного виконання зобов'язань**

26. Діяльність надавачів здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування збитків, які можуть бути завдані користувачам чи третім особам внаслідок неналежного виконання надавачем своїх зобов'язань.

27. Розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми визначено частиною третьою статті 16 Закону України «Про електронні довірчі послуги».

28. Надавач зобов'язаний підтримувати розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми в актуальному стані відповідно до розміру мінімальної заробітної плати, встановленого законом про Державний бюджет України на відповідний рік.

29. У разі відшкодування збитків, завданих користувачам чи третім особам внаслідок неналежного виконання своїх зобов'язань, надавач вживає вичерпних заходів для найшвидшого відновлення розміру внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми.

### **4. Вимоги до регламенту роботи надавача**



30. Надавач надає кваліфіковані електронні довірчі послуги відповідно до вимог законодавства у сфері електронних довірчих послуг та регламенту роботи надавача.

31. Регламент роботи надавача розробляється та затверджується до початку роботи надавача.

32. У регламенті роботи надавача повинно бути визначено:

1) загальні відомості про надавача (найменування або прізвище, ім'я, по батькові надавача; код за Єдиним державним реєстром підприємств та організацій України; місцезнаходження, номери телефонів, електронна адреса веб-сайту);

2) перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує надавач;

3) посадовий склад надавача та функції найманих працівників надавача;

4) політика сертифіката та положення сертифікаційних практик;

5) опис процедур та процесів, які виконуються під час надання кваліфікованих електронних довірчих послуг, що не передбачають формування та обслуговування кваліфікованих сертифікатів відкритих ключів.

33. Політика сертифіката може описувати кожен кваліфікований електронний довірчий сервіс, що передбачає формування та обслуговування надавачем кваліфікованих сертифікатів відкритих ключів, окремо або у сукупності.

Положення сертифікаційних практик описують практичні та процедурні засади реалізації всіх політик сертифіката у сукупності.

34. У політиці сертифіката визначається:

1) сфера використання кваліфікованих сертифікатів відкритих ключів:

а) перелік сфер, у яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;

б) обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;

2) порядок розповсюдження інформації надавачем:

а) перелік інформації, що розміщується надавачем на своєму офіційному веб-сайті;

б) час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів;

3) порядок ідентифікації та автентифікації заявників:

а) механізми підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа;

б) умови встановлення заявника (інформація, що надається заявником під час ідентифікації особи, види документів, на підставі яких встановлюється заявник, вимоги щодо особистої присутності);

в) механізми автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем;

г) механізми автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа;

4) управління та операційний контроль:

а) фізичне середовище (опис приміщень надавача, в яких розміщена інформаційно-телекомунікаційна система надавача, механізми контролю доступу до них);

б) процедурний контроль (система дисциплінарних стягнень за недотримання найманими працівниками надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою в межах організації з урахуванням режиму роботи надавача);

в) ведення журналів аудиту подій (типи подій, що фіксуються у журналі аудиту подій, частота перегляду, строки зберігання журналів аудиту подій, захист та резервне копіювання журналів аудиту подій, перелік найманих працівників надавача, що можуть здійснювати перегляд журналів аудиту подій);

г) ведення архівів надавача (типи документів та даних, що підлягають архівуванню, строки зберігання архівів, механізми та порядок зберігання і захисту архівів);

5) управління парами ключів:

а) генерація пар ключів (процес, порядок та умови генерації пар ключів надавача та користувачів);

б) процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги їй надавачем;

в) механізм надання відкритого ключа користувача надавачу для формування кваліфікованого сертифіката відкритого ключа;

6) забезпечення захисту особистого ключа надавача:

а) порядок захисту та доступу до особистого ключа надавача;

б) резервне копіювання особистого ключа надавача, порядок та умови збереження, доступу та використання резервної копії.

35. У положеннях сертифікаційних практик має бути зазначено умови, процедури та механізми, пов'язані з формуванням, блокуванням, скасуванням та використанням кваліфікованого сертифіката відкритого ключа:

1) процес подання запиту на формування кваліфікованого сертифіката відкритого ключа (перелік суб'єктів, уповноважених здійснювати запит на формування кваліфікованого сертифіката відкритого ключа, порядок подачі та оброблення такого запиту, строки оброблення запиту на формування кваліфікованого сертифіката відкритого ключа);

2) надання сформованого кваліфікованого сертифіката відкритого ключа користувачу;

3) публікація сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті надавача;

4) умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа (попередження про можливі наслідки неправильного використання кваліфікованого сертифіката відкритого ключа та особистого ключа);

5) процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований цим надавачем;

6) обставини скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; перелік суб'єктів, уповноважених здійснювати запит на скасування (блокування та поновлення) кваліфікованого сертифіката відкритого ключа; процедура подання запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; час оброблення запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; частота формування списку відкликаних сертифікатів та строки його дії; можливість та умови надання інформації про статус кваліфікованого сертифіката відкритого ключа у режимі реального часу);

7) закінчення строку чинності кваліфікованого сертифіката відкритого ключа користувача.

36. Проект регламенту роботи надавача підлягає обов'язковому погодженню з контролюючим органом.

Після погодження з контролюючим органом регламент роботи надавача затверджується його керівником у двох примірниках.

Один примірник погодженого з контролюючим органом та затвердженого керівником надавача регламенту роботи надавача передається до контролюючого органу.

37. Погодження та затвердження змін до регламенту роботи надавача здійснюється відповідно до вимог, передбачених для погодження та затвердження регламенту роботи надавача.

Для погодження змін до регламенту роботи надавача до контролюючого органу надається текст відповідних змін та порівняльна таблиця.

38. Надавач самостійно визначає обсяг положень регламенту його роботи та інших документів, що підлягають розміщенню на офіційному веб-сайті надавача для ознайомлення.

## **5. Вимоги до початку роботи надавача**

39. Для набуття статусу надавача юридична особа або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, подає до центрального засвідчувального органу заяву про внесення відомостей про неї до Довірчого списку та інші документи, визначені частиною другою статті 30 Закону України «Про електронні довірчі послуги».

Форма заяви про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку встановлюється у регламенті роботи центрального засвідчувального органу.

40. Заява про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що до неї додаються, можуть бути подані представником юридичної особи або фізичною особою – підприємцем, що має намір надавати кваліфіковані електронні довірчі послуги, в електронній формі через Єдиний державний портал адміністративних послуг, у тому числі через інтегровану з ним інформаційну систему центрального засвідчувального органу.

Забезпечення цілісності та конфіденційності інформації, у тому числі персональних даних, під час подання заяви повинно здійснюватись з дотриманням вимог законодавства у сфері захисту інформації із застосуванням кваліфікованого електронного підпису представника юридичної особи або фізичної особи – підприємця та з використання засобів шифрування, що мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

У разі подання документів для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку в електронній формі копії документів, які існують виключно в паперовій формі, додаються до заяви про внесення до Довірчого списку у форматі PDF.

Відповідність оригіналам копій документів засвідчується шляхом накладення кваліфікованого електронного підпису керівника юридичної особи або фізичної особи – підприємця, що має намір надавати кваліфіковані електронні довірчі послуги.

Представник юридичної особи або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, відповідає за достовірність інформації наданої в документах для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку.

У разі подання заяви про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документів, що до неї додаються, в електронній формі документи на паперових носіях не подаються.

Уповноважена особа центрального засвідчувального органу перевіряє надходження електронних документів не рідше двох разів на день (у першій та другій половині робочого дня).

Документи для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку, подані в електронній формі, реєструються в інформаційній системі центрального засвідчувального органу після їх надходження, про що автоматично через персональний кабінет на Єдиному державному порталі адміністративних послуг інформується представник юридичної особи або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги.

41. Після вжиття вичерпних заходів для забезпечення ідентифікації та перевірки обсягу цивільної правоздатності та дієздатності представника юридичної особи або фізичної особи – підприємця, що має намір надавати кваліфіковані електронні довірчі послуги, центральний засвідчувальний орган здійснює розгляд заяви про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документів, що до неї додаються, і за результатами їх розгляду приймає рішення в порядку та у строки, встановлені Законом України «Про електронні довірчі послуги».

42. На підставі прийнятого центральним засвідчувальним органом рішення про внесення до Довірчого списку юридична особа або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, засвідчує чинність одного або декількох своїх відкритих ключів (окремо для кожної кваліфікованої електронної довірчої послуги) у центральному засвідчувальному органі відповідно до вимог регламенту роботи центрального засвідчувального органу.

Засвідчення чинності відкритого ключа юридичної особи або фізичної особи – підприємця є умовою внесення до Довірчого списку інформації про кваліфіковані електронні довірчі послуги, які має намір надавати юридична особа або фізична особа – підприємець.

Для засвідчення чинності відкритого ключа юридична особа або фізична особа – підприємець подає до центрального засвідчувального органу:

- 1) заяву про формування кваліфікованого сертифіката відкритого ключа та відповідний їй електронний запит, що формується після генерації пари ключів;
- 2) підписаний примірник договору про надання центральним засвідчувальним органом кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

43. Юридична особа або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, набуває статус надавача з дня внесення відомостей про неї до Довірчого списку.

44. Рішення центрального засвідчувального органу про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку оприлюднюється на офіційному веб-сайті центрального засвідчувального органу, а представник юридичної особи або фізична особа – підприємець, що має намір надавати кваліфіковані електронні довірчі послуги, повідомляється центральним засвідчувальним органом про прийняте рішення шляхом надсилання листа поштою або в електронній формі через персональний кабінет на Єдиному державному порталі адміністративних послуг.

45. Зміна відомостей про надавача, що містяться в Довірчому списку, є підставою для внесення змін до Довірчого списку, яке здійснюється в порядку та у строки, встановлені Законом України «Про електронні довірчі послуги».

У разі виникнення змін у відомостях, внесених до Довірчого списку, надавач зобов'язаний протягом п'яти робочих днів з дня настання таких змін подати до центрального засвідчувального органу заяву про внесення змін до Довірчого списку разом з документами, що підтверджують відповідні зміни.

## **6. Вимоги до припинення діяльності з надання кваліфікованих електронних довірчих послуг**

46. Надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг з підстав та в порядку, що визначені статтею 31 Закону України «Про електронні довірчі послуги».

47. У разі припинення надання кваліфікованих електронних довірчих послуг надавач зобов'язаний передати центральному засвідчувальному органу документовану інформацію (документи, на підставі яких користувачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати відкритих ключів, усі сформовані кваліфіковані сертифікати відкритих ключів, а також реєстри сформованих кваліфікованих сертифікатів відкритих ключів) у порядку, визначеному Кабінетом Міністрів України.

48. Передавання документованої інформації здійснюється надавачем не пізніше дня, визначеного ним як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, чи дня набрання законної сили відповідним рішенням суду.

49. Центральний засвідчувальний орган скасовує виданий ним кваліфікований сертифікат відкритого ключа надавача у день, визначений надавачем як дата припинення діяльності з надання кваліфікованих

електронних довірчих послуг, чи у день набрання законної сили відповідним рішенням суду.

### **III. Вимоги до надання кваліфікованих електронних довірчих послуг**

#### **1. Загальні вимоги до надавача під час надання кваліфікованих електронних довірчих послуг**

1. Кваліфіковані електронні довірчі послуги користувачам надають виключно надавачі.

2. Надавач може надавати окремо або в сукупності:

1) кваліфіковану електронну довірчу послугу створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

2) кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

3) кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

4) кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження кваліфікованої електронної позначки часу;

5) кваліфіковану електронну довірчу послугу реєстрованої електронної доставки;

6) кваліфіковану електронну довірчу послугу зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами.

3. Приміщення, у яких здійснюється обслуговування користувачів, повинні бути доступними для осіб з обмеженими фізичними можливостями відповідно до державних будівельних норм, правил і стандартів.

Інформація про умови доступності спеціальних приміщень для осіб з обмеженими фізичними можливостями розміщується у місці, доступному для візуального сприйняття користувачів.

4. Для надання кваліфікованої електронної довірчої послуги надавач здійснює ідентифікацію заявника шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних одержаних з інформаційних систем органів державної влади.

5. Ідентифікація заявника та перевірка обсягу його цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону України «Про електронні довірчі послуги».

6. Ідентифікаційні дані особи, що надаються заявником для отримання кваліфікованої електронної довірчої послуги, повинні бути перевірені надавачем:

- 1) за особистої присутності заявника;
- 2) шляхом використання засобу електронної ідентифікації заявника, який було особисто отримано заявником та який має високий рівень довіри відповідно до схеми електронної ідентифікації, визначеної Кабінетом Міністрів України;

- 3) шляхом використання ідентифікаційних даних особи – заявника з чинного кваліфікованого сертифіката відкритого ключа, сформованого тим самим надавачем.

7. Заявник повинен надати інформацію, що дозволяє зв'язатися з ним та визначена регламентом роботи надавача.

8. Реєстрація користувачів може здійснюватися через відокремлені пункти реєстрації, які виконують свої функції згідно з регламентом роботи надавача.

9. Центральний засвідчувальний орган здійснює надання кваліфікованих електронних довірчих послуг надавачам відповідно до регламенту роботи центрального засвідчувального органу з дотриманням цих Вимог.

10. Надавач повинен забезпечити можливість ознайомлення заявників з інформацією про умови отримання кваліфікованої електронної довірчої послуги.

11. До інформації, вільний доступ до якої повинен забезпечити надавач, відносяться:

- 1) відомості про надавача;
- 2) інформація про внесення відомостей про надавача до Довірчого списку;
- 3) кваліфіковані сертифікати відкритих ключів надавача;
- 4) перелік кваліфікованих електронних довірчих послуг, які надає надавач;
- 5) інформація про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;
- 6) форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- 7) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;
- 8) відомості про обмеження при використанні кваліфікованих сертифікатів відкритих ключів користувачами;



9) інформація щодо порядку перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;

10) законодавство в сфері електронних довірчих послуг.

12. Надавач забезпечує інформування користувачів щодо умов отримання кваліфікованих електронних довірчих послуг, у тому числі шляхом розміщення відповідної інформації на офіційному веб-сайті надавача.

Інформація на офіційному веб-сайті надавача повинна бути доступною для осіб з обмеженими фізичними можливостями.

13. Кваліфіковані електронні довірчі послуги надаються на підставі договору надавача із заявником про надання кваліфікованої електронної довірчої послуги.

Підставою надання кваліфікованих електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності може бути відповідне рішення керівника.

14. Надавач обліковує та зберігає протягом строків, визначених законодавством, договори про надання кваліфікованих електронних довірчих послуг, а також документи (засвідчені в установленому порядку копії документів), що використовуються під час ідентифікації та перевірки достатності обсягу цивільної правоздатності та дієздатності заявника.

15. Істотними умовами договору про надання кваліфікованих електронних довірчих послуг є:

- 1) права та обов'язки сторін;
- 2) умови використання засобів кваліфікованого електронного підпису чи печатки (у разі якщо кваліфікована електронна довірча послуга передбачає використання засобів кваліфікованого електронного підпису чи печатки);
- 3) умови використання заявником особистого ключа (у разі якщо кваліфікована електронна довірча послуга передбачає використання особистого ключа);
- 4) умови публікації кваліфікованого сертифіката відкритого ключа заявника (у разі якщо кваліфікована електронна довірча послуга передбачає формування кваліфікованого сертифіката відкритого ключа);
- 5) строк дії договору;
- 6) умови оплати;
- 7) порядок внесення змін до договору;
- 8) порядок розірвання договору.

16. Договір про надання кваліфікованої електронної довірчої послуги може бути змінено виключно за взаємною згодою сторін.

17. У разі зміни відомостей, що містяться у договорі про надання кваліфікованої електронної довірчої послуги, заявник у триденний строк з дня настання таких змін повідомляє про це надавача та надає документи, що підтверджують відповідні зміни.

18. Підставами для розірвання договору про надання кваліфікованої електронної довірчої послуги є:

- 1) згода сторін;
- 2) рішення суду про розірвання договору;
- 3) виключення надавача з Довірчого списку.

19. У разі якщо договір про надання кваліфікованої електронної довірчої послуги передбачав формування кваліфікованого сертифіката відкритого ключа, розірвання такого договору є підставою для скасування надавачем кваліфікованого сертифіката відкритого ключа, сформованого відповідно до такого договору.

20. Надавач має право самостійно обирати, які саме стандарти будуть ним застосовуватися при наданні кваліфікованих електронних довірчих послуг з Переліку, що додається до цих Вимог.

21. Контроль за наданням кваліфікованих електронних довірчих послуг надавачами здійснює контролюючий орган.

## **2. Вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток**

22. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток включає вчинення дій, передбачених частиною першою статті 18 Закону України «Про електронні довірчі послуги».

23. Під час надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток надавачем забезпечується:

1) використання підписувачем або створювачем електронної печатки виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката електронного підпису чи печатки;

2) захист обміну інформацією між підписувачем або створювачем електронної печатки та надавачем засобами телекомунікаційних мереж загального користування;

3) створення умов для генерації пари ключів підписувача або створювача електронної печатки;

4) допомога під час генерації пари ключів підписувача або створювача електронної печатки у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

5) унікальності пари ключів підписувача або створювача електронної печатки;

6) зберігання особистого ключа підписувача або створювача електронної печатки;

7) захист від доступу сторонніх осіб до параметрів особистого ключа підписувача або створювача електронної печатки під час використання засобу кваліфікованого електронного підпису чи печатки.

24. У разі якщо пара ключів була згенерована заявником поза приміщенням надавача та/або за відсутності відповідного персоналу, ідентифікація такого заявника, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката відкритого ключа здійснюється надавачем після перевірки володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа.

Перевірка володіння заявником особистим ключем виконується без розкриття його особистого ключа.

25. Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно надавач.

26. Надавач, який здійснює управління парою ключів підписувача або створювача електронної печатки, може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання за умови дотримання таких вимог:

1) рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;

2) кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

27. Кваліфікований електронний підпис чи печатка повинні відповідати таким вимогам:

1) встановлювати однозначний зв'язок з підписувачем або створювачем електронної печатки;

2) надавати можливість здійснити електронну ідентифікацію підписувача або створювача електронної печатки;

3) забезпечувати одноосібний контроль підписувача або створювача електронної печатки за відповідним особистим ключем;

4) виявляти будь-які зміни пов'язаних електронних даних, на які накладено кваліфікований електронний підпис чи печатку.

28. Процес перевірки кваліфікованого електронного підпису чи печатки повинен підтвердити справжність кваліфікованого електронного підпису чи печатки за таких умов:

- 1) дотримання вимог, визначених у частині другій статті 18 Закону України «Про електронні довірчі послуги»;
- 2) правильності внесення ідентифікаційних даних особи до відповідного кваліфікованого сертифіката електронного підпису чи печатки підписувача або створювача електронної печатки;
- 3) під час перевірки встановлено, що кваліфікований електронний підпис або печатку створено за допомогою засобу кваліфікованого електронного підпису чи печатки;
- 4) дотримання вимог, визначених у пункті 26 цього підрозділу, на момент накладення на пов'язані електронні дані.

29. Перевірка кваліфікованого електронного підпису чи печатки може здійснюватися будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого електронного підпису чи печатки.

30. Надання кваліфікованої електронної довірчої послуги перевірки та підтвердження кваліфікованих електронних підписів чи печаток передбачає, що:

- 1) послуга надається виключно надавачем;
- 2) послуга відповідає всім вимогам до перевірки кваліфікованих електронних підписів чи печаток, визначеним у пункті 26 цього підрозділу;
- 3) дозволяє отримувати результати перевірки із застосуванням кваліфікованого електронного підпису чи печатки надавача автоматизованим способом, який є надійним, ефективним та захищеним.

### **3. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки**

31. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає вчинення дій, передбачених частиною першою статті 20 Закону України «Про електронні довірчі послуги».

32. Формування кваліфікованого сертифіката електронного підпису чи печатки заявника здійснюється надавачем на основі ідентифікаційних даних особи, одержаних від заявника під час його ідентифікації та перевірки достатності обсягу його цивільної правоздатності і дієздатності.

33. Надавач зобов'язаний забезпечити унікальність серійного номера кваліфікованого сертифіката електронного підпису чи печатки заявника серед

інших кваліфікованих сертифікатів електронного підпису чи печатки, сформованих цим самим надавачем.

34. Надавач зобов'язаний резервувати всі сформовані ним кваліфіковані сертифікати електронного підпису чи печатки.

35. Під час повторного формування кваліфікованого сертифіката електронного підпису чи печатки користувача надавач повинен перевірити актуальність інформації, що надавалась для попереднього формування кваліфікованого сертифіката електронного підпису чи печатки цього заявника.

36. Кваліфікований сертифікат електронного підпису чи печатки користувача після його формування надавачем повинен бути доступний користувачу, для якого цей кваліфікований сертифікат електронного підпису чи печатки був сформований.

37. Доступ інших осіб до сформованого кваліфікованого сертифіката електронного підпису чи печатки користувача надається у разі його згоди на публікацію кваліфікованого сертифіката електронного підпису чи печатки.

38. У разі зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, користувач у триденний строк з дня настання таких змін повідомляє про це надавача та надає документи, що підтверджують відповідні зміни.

На підставі наданих користувачем документів, що підтверджують зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, надавач здійснює повторне формування кваліфікованого сертифіката електронного підпису чи печатки користувача та його публікацію у разі згоди користувача.

Повторне формування кваліфікованого сертифіката електронного підпису чи печатки користувача не продовжує строку дії його кваліфікованого сертифіката електронного підпису чи печатки.

39. Сформований кваліфікований сертифікат електронного підпису чи печатки користувача скасовується або блокується надавачем у разі настання підстав передбачених статтею 25 Закону України «Про електронні довірчі послуги».

40. Заява про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки подається користувачем надавачу в будь-який спосіб, що забезпечує підтвердження особи-користувача.

Під час опрацювання заяви про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки надавачем здійснюється ідентифікація та перевірка достатності обсягу цивільної правоздатності і дієздатності користувача з дотриманням вимог щодо підтвердження особи, встановлених у регламенті роботи надавача.

41. Кваліфікований сертифікат електронного підпису чи печатки користувача вважається скасованим або блокованим з моменту зміни надавачем

статусу кваліфікованого сертифіката електронного підпису чи печатки користувача на скасований або блокований.

42. Користувач, статус кваліфікованого сертифіката електронного підпису чи печатки якого було змінено на скасований чи блокований, повинен невідкладно бути поінформований про відповідну зміну статусу.

43. Скасований кваліфікований сертифікат електронного підпису чи печатки поновленню не підлягає.

44. Відомості про кваліфіковані сертифікати електронного підпису чи печатки, сформовані надавачем, їх статус та списки відкликаних сертифікатів містяться у реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів.

45. Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів здійснюється за допомогою публікації повного та часткового списків відкликаних сертифікатів на офіційному веб-сайті надавача та забезпечення можливості перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки користувача в режимі реального часу через телекомунікаційні мережі загального користування.

До списку відкликаних сертифікатів надавача висуваються такі вимоги:

1) у кожному списку відкликаних сертифікатів зазначається граничний термін його дії до видання наступного списку, якщо інше не передбачено регламентом роботи надавача;

2) новий список відкликаних сертифікатів може бути опублікований до настання граничного терміну його дії до видання наступного списку;

3) на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис чи печатка надавача.

46. Управління статусом кваліфікованого сертифіката електронного підпису чи печатки та розповсюдження інформації про статус кваліфікованого сертифіката електронного підпису чи печатки повинні бути доступні користувачу цілодобово.

47. Заяви про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки фіксуються та зберігаються надавачем протягом строків, визначених законодавством.

48. Надавач повинен забезпечити цілісність та походження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки.

49. Час, що використовується надавачем в процесі обслуговування кваліфікованих сертифікатів електронного підпису чи печатки користувачів, повинен бути синхронізований з Всесвітнім координованим часом (UTC) з точністю до секунди.

50. Формування кваліфікованого сертифіката електронного підпису чи печатки здійснюється надавачем за запитом користувача.

51. Надавачі отримують кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки від центрального засвідчувального органу.

#### **4. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту**

52. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту включає вчинення дій, передбачених частиною першою статті 21 Закону України «Про електронні довірчі послуги».

53. Формування кваліфікованого сертифіката автентифікації веб-сайту здійснюється надавачем за запитом користувача.

54. Кваліфікований сертифікат автентифікації веб-сайту повинен забезпечувати:

1) автентифікацію власника веб-сайту;

2) гарантування:

шифрування інформації, обмін якою здійснюють через Інтернет учасник он-лайн операції та веб-сайт;

належного рівня довіри до власника веб-сайту щодо захисту від шахрайства в Інтернеті;

захисту особистої інформації та персональних даних учасника он-лайн операції під час вчинення такої операцій.

55. Перевірка кваліфікованого сертифіката автентифікації веб-сайту може здійснюватися будь-якою особою з метою отримання інформації про власника веб-сайту та чинність кваліфікованого сертифіката автентифікації веб-сайту.

56. Під час перевірки кваліфікованого сертифіката автентифікації веб-сайту особа, що здійснює перевірку, виконує такі дії:

1) отримує з кваліфікованого сертифіката автентифікації веб-сайту інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити власника веб-сайту та надавача;

2) перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфікований сертифікат автентифікації веб-сайту за допомогою чинного (на момент формування кваліфікованого сертифіката автентифікації веб-сайту) кваліфікованого сертифіката відкритого ключа надавача.

57. Кваліфікований сертифікат автентифікації веб-сайту вважається нечинним у разі:

- 1) закінчення строку дії кваліфікованого сертифіката автентифікації веб-сайту або зміни його статусу на блокований чи скасований;
- 2) використання скасованого або блокованого кваліфікованого сертифіката відкритого ключа надавача на момент формування кваліфікованого сертифіката автентифікації веб-сайту.

58. Надавачі отримують кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту від центрального засвідчувального органу.

## **5. Вимоги до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу**

59. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає вчинення дій, передбачених частиною першою статті 26 Закону України «Про електронні довірчі послуги».

60. Формування кваліфікованої електронної позначки часу здійснюється надавачем за запитом користувача.

61. Під час формування кваліфікованої електронної позначки часу користувач та надавач за допомогою засобів кваліфікованого електронного підпису чи печатки виконують такі дії:

- 1) користувач обчислює геш-значення електронних даних, на які необхідно сформувати кваліфіковану електронну позначку часу;

- 2) користувач формує запит на формування кваліфікованої електронної позначки часу, який містить:

обчислене геш-значення;

об'єктний ідентифікатор політики формування позначки часу (необов'язково);

ідентифікатор алгоритму гешування, що використовувався;

унікальний ідентифікатор запиту (необов'язково);

необов'язкові розширення;

- 3) користувач передає сформований запит до надавача;

- 4) надавач перевіряє правильність формату запиту та виконує його обробку, формує кваліфіковану електронну позначку часу та відповідь, що



містить кваліфіковану електронну позначку часу, чи відповідь з інформацією про відмову у формуванні кваліфікованої електронної позначки часу;

5) надавач пересилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, яка містить такі дані:

об'єктний ідентифікатор політики формування кваліфікованої електронної позначки часу, що була використана;

геш-значення електронних даних, для яких було сформовано кваліфіковану електронну позначку часу;

серійний номер кваліфікованої електронної позначки часу;

час формування кваліфікованої електронної позначки часу;

додаткову інформацію про кваліфіковану електронну позначку часу;

кваліфікований електронний підпис чи печатку надавача, накладений на кваліфіковану електронну позначку часу;

б) користувач після отримання відповіді від надавача виконує такі дії:

перевіряє результат обробки у відповіді;

перевіряє відповідність імені чи найменування суб'єкта, що наклав кваліфікований електронний підпис чи печатку на кваліфіковану електронну позначку часу, імені чи найменуванню надавача;

перевіряє відповідність призначення кваліфікованого сертифіката відкритого ключа надавача (для формування позначки часу);

перевіряє чинність кваліфікованого сертифіката відкритого ключа надавача;

перевіряє кваліфікований електронний підпис чи печатку, що був накладений на кваліфіковану електронну позначку часу;

перевіряє відповідність електронних даних та даних, для яких була сформована кваліфікована електронна позначка часу (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу);

додає кваліфіковану електронну позначку часу до електронних даних.

62. Кваліфікована електронна позначка часу повинна забезпечувати:

1) зв'язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;

2) точність часу в програмно-технічному комплексі надавача, що синхронізується із Всесвітнім координованим часом (UTC) з точністю до секунди.

63. Перевірка кваліфікованої електронної позначки часу може здійснюватися будь-якою особою з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

64. Під час перевірки та підтвердження кваліфікованої електронної позначки часу особа, що здійснює перевірку, виконує такі дії:

1) отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити надавача;

2) перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката відкритого ключа надавача;

3) перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу).

65. Кваліфікована електронна позначка часу вважається недійсною у разі:

1) недотримання вимоги щодо точності часу в програмно-технічному комплексі надавача;

2) використання скасованого або блокованого кваліфікованого сертифіката відкритого ключа надавача на момент формування кваліфікованої електронної позначки часу.

66. Правильність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в засобі кваліфікованого електронного підпису чи печатки забезпечує протокол фіксування часу.

67. Надавачі отримують кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження кваліфікованої електронної позначки часу від центрального засвідчувального органу.

68. Механізм синхронізації часу із Всесвітнім координованим часом (UTC) в програмно-технічному комплексі надавача та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із Всесвітнім координованим часом (UTC).

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) розробляється надавачем та погоджується з центральним засвідчувальним органом.

## **6. Вимоги до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки**

69. Кваліфікована електронна довірча послуга реєстрованої електронної доставки повинна відповідати вимогам, передбаченим частиною першою

статті 27 Закону України «Про електронні довірчі послуги», та включати вчинення таких дій:

- 1) відправку електронних даних із забезпеченням доказів відправки;
- 2) отримання електронних даних із забезпеченням доказів отримання.

70. Реєстрована електронна доставка здійснюється надавачем за запитом користувача (відправника та/або отримувача електронних даних).

71. Реєстрована електронна доставка повинна забезпечувати:

- 1) передачу електронних даних між користувачами (відправником та отримувачем електронних даних);
- 2) автентифікацію відправника та отримувача електронних даних;
- 3) конфіденційність електронних даних, що доставляються, та персональних даних відправника та отримувача електронних даних;
- 4) захист цілісності електронних даних, що доставляються;
- 5) забезпечення точності дати та часу відправки та отримання електронних даних;
- 6) можливість доказування відправки та отримання електронних даних.

72. Перевірка електронних даних, що передаються в процесі реєстрованої електронної доставки, здійснюється отримувачем електронних даних.

**7. Вимоги до надання кваліфікованої електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами**

73. Кваліфікована електронна довірча послуга зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, включає вчинення таких дій:

- 1) передачу кваліфікованих електронних підписів чи печаток, позначок часу та сформованих сертифікатів, пов'язаних з цими послугами;
- 2) зберігання кваліфікованих електронних підписів чи печаток, позначок часу та сформованих сертифікатів, пов'язаних з цими послугами.

74. Зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, здійснюється надавачем за запитом користувача.

75. При наданні електронної довірчої послуги зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів повинно забезпечуватися:

- 1) цілісність всіх збережених об'єктів даних;

- 2) протоколювання подій на предмет зміни, видалення або додавання об'єктів даних;
- 3) покладання відповідальності за збереження на одну чи декількох конкретних посадових осіб;
- 4) проведення регулярних перевірок дотримання цих Вимог.

### **III. Вимоги до засобів кваліфікованого електронного підпису чи печатки**

1. Засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг, повинні відповідати вимогам, встановленим частинами першою та другою статті 19 Закону України «Про електронні довірчі послуги».

2. Для надання кваліфікованих електронних довірчих послуг використовуються засоби кваліфікованого електронного підпису чи печатки, які повинні мати документи про відповідність або позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

3. Надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, що підтверджують його право власності та/або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються для надання кваліфікованих електронних довірчих послуг, забороняється.

4. Технічні специфікації форматів, які реалізуються у засобах кваліфікованого електронного підпису чи печатки, встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг, спільно з спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

5. Контроль за дотриманням вимог до засобів кваліфікованого електронного підпису чи печатки здійснює контролюючий орган.

### **IV. Вимоги до кваліфікованих сертифікатів відкритих ключів**

1. Кваліфіковані сертифікати відкритих ключів, що формуються надавачами або центральним засвідчувальним органом під час надання кваліфікованих електронних довірчих послуг, повинні відповідати вимогам, встановленим частинами першою, другою та третьою статті 23 Закону України «Про електронні довірчі послуги».

2. Надавач або центральний засвідчувальний орган, який видав кваліфікований сертифікат відкритого ключа, повинен забезпечити доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа.

3. Контроль за дотриманням вимог до кваліфікованих сертифікатів відкритих ключів здійснює контролюючий орган.

---