Офіційно опубліковано 29.11.2019

Правління Національного банку України

П О С Т А Н О В А

21 листопада 2019 року м. Київ № 138

Про затвердження Регламенту роботи засвідчувального центру

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статті 9 Закону України “Про електронні довірчі послуги”, з метою встановлення організаційно-методологічних, технічних і технологічних умов діяльності засвідчувального центру під час надання ним кваліфікованих електронних довірчих послуг, порядку взаємодії кваліфікованих надавачів електронних довірчих послуг із засвідчувальним центром у процесі надання ним кваліфікованих електронних довірчих послуг Правління Національного банку України **постановляє**:

1. Затвердити Регламент роботи засвідчувального центру, що додається.

2. Департаменту безпеки (Олександр Скомаровський) після офіційного опублікування надіслати копію цієї постанови до Адміністрації Державної служби спеціального зв’язку та захисту інформації України, довести до відома банків України інформацію про прийняття цієї постанови.

3. Контроль за виконанням цієї постанови покласти на Голову Національного банку України Якова Смолія.

4. Постанова набирає чинності з дня, наступного за днем її офіційного опублікування.

Голова Яків СМОЛІЙ

Інд. 56

Аркуш погодження додається.

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
21 листопада 2019 року № 138

Регламент роботи засвідчувального центру

І. Загальні положення

1. Цей Регламент розроблено відповідно до статті 7 Закону України “Про Національний банк України”, статей 9, 30 Закону України “Про електронні довірчі послуги” (далі – Закон), Положення про кваліфікованих надавачів електронних довірчих послуг, унесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116.

2. У цьому Регламенті терміни вживаються в такому значенні:

1) заявник – надавач електронних довірчих послуг, який звертається до засвідчувального центру з метою набуття статусу кваліфікованого надавача електронних довірчих послуг або кваліфікований надавач електронних довірчих послуг (далі – кваліфікований надавач), який звертається до засвідчувального центру для отримання кваліфікованих електронних довірчих послуг, зміни відомостей, що містяться в Довірчому списку, передавання документованої інформації;

2) інформаційно-телекомунікаційна система засвідчувального центру – сукупність інформаційних і телекомунікаційних систем Національного банку України (далі – Національний банк), яка об’єднує програмно-технічний комплекс засвідчувального центру, що використовується ним для надання електронних довірчих послуг, фізичне середовище, інформацію, котра обробляється в інформаційних і телекомунікаційних системах Національного банку, а також працівників Національного банку, які забезпечують виконання функцій засвідчувального центру;

3) комплексна система захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру – сукупність організаційних заходів, інженерно-технічних та програмно-апаратних засобів, які забезпечують технічний та криптографічний захист інформації в інформаційно-телекомунікаційній системі засвідчувального центру;

4) програмно-технічний комплекс засвідчувального центру, що використовується ним для надання електронних довірчих послуг (далі – програмно-технічний комплекс засвідчувального центру) – сукупність апаратних, апаратно-програмних та програмних засобів, що використовується Національним банком для забезпечення виконання функцій, пов’язаних із наданням засвідчувальним центром кваліфікованих електронних довірчих послуг;

5) реєстр засвідчувального центру – електронна база даних, яка ведеться засвідчувальним центром та містить відомості про кваліфікованих надавачів і реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

6) список відкликаних сертифікатів ключів засвідчувального центру (далі – СВС) – перелік блокованих і скасованих кваліфікованих сертифікатів відкритих ключів (далі – сертифікати ключів), що формується засвідчувальним центром;

7) уповноважений представник заявника – керівник заявника або інший представник заявника, уповноважений підписувати документи, передбачені цим Регламентом та Законом, які заявник подає до засвідчувального центру.

Інші терміни в цьому Регламенті вживаються в значеннях, наведених у Законі, нормативно-правових актах Національного банку у сфері електронних довірчих послуг.

3. Дія Регламенту поширюється на засвідчувальний центр, кваліфікованих надавачів, унесених до Довірчого списку за поданням засвідчувального центру та надавачів електронних довірчих послуг, які мають намір набути статус кваліфікованих надавачів.

4. Цей Регламент визначає:

1) організаційно-методологічні, технічні і технологічні умови діяльності засвідчувального центру під час надання ним кваліфікованих електронних довірчих послуг;

2) порядок взаємодії кваліфікованих надавачів із засвідчувальним центром у процесі надання ним кваліфікованих електронних довірчих послуг;

3) умови внесення до Довірчого списку відомостей про надавачів електронних довірчих послуг, які мають намір набути статусу кваліфікованих надавачів;

4) умови внесення змін до Довірчого списку.

5. Підставою для оброблення персональних даних у засвідчувальному центрі є згода суб'єктів персональних даних на оброблення їхніх персональних даних. Така згода оформляється у вигляді письмового дозволу на оброблення персональних даних, у якому задокументовано добровільне волевиявлення фізичних осіб щодо надання дозволу на оброблення їхніх персональних даних.

Форма дозволу суб'єктів персональних даних на оброблення їхніх персональних даних у засвідчувальному центрі розміщується на вебсайті засвідчувального центру. Дозвіл на оброблення персональних даних надають ті суб'єкти персональних даних, чиї персональні дані вперше передаються до засвідчувального центру. Заявник забезпечує подання до засвідчувального центру дозволу на оброблення персональних даних разом із відповідною заявою.

6. Кваліфікований надавач зобов'язаний щороку до 15 січня подавати до засвідчувального центру звіт про роботу кваліфікованого надавача електронних довірчих послуг за попередній рік. Форма звіту розміщується на вебсайті засвідчувального центру.

7. Кваліфікований надавач зобов'язаний передати засвідчувальному центру документовану інформацію в разі припинення діяльності з надання кваліфікованих електронних довірчих послуг у порядку, визначеному Національним банком.

8. Ідентифікаційні дані засвідчувального центру:

1) місцезнаходження: 01601, м. Київ, вул. Інститутська, 9;

2) адреси розміщення Засвідчувального центру:
01601, м. Київ, вул. Інститутська, 9;
03028, м. Київ, просп. Науки, 7;
79000, м. Львів, вул. Коперника, 4 (віддалений резервний пункт);

3) телефони: (044) 527–31–55, (044) 527–31–08;

4) факс: (044) 524–39–63;

5) код за ЄДРПОУ: 00032106;

6) адреса вебсайта засвідчувального центру: https://zc.bank.gov.ua;

7) електронна пошта засвідчувального центру: zc_nbu@bank.gov.ua.

9. Заявник зобов’язаний подавати документи, передбачені цим Регламентом і Законом, у паперовій формі або у формі електронних документів.

10. Заявник зобов’язаний подавати у формі електронних документів із кваліфікованим електронним підписом уповноваженого представника заявника:

1) заяви про отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

2) заяви про скасування сертифіката ключа кваліфікованого надавача;

3) заяви про блокування сертифіката ключа кваліфікованого надавача;

4) заяви про поновлення сертифіката ключа кваліфікованого надавача;

5) звіт про роботу кваліфікованого надавача електронних довірчих послуг;

6) заяву про виключення відомостей про кваліфікованого надавача з Довірчого списку.

11. Заявник має право подавати у паперовій формі із власноручним підписом уповноваженого представника заявника або у формі електронних документів із кваліфікованим електронним підписом уповноваженого представника заявника:

1) заяву про внесення до Довірчого списку та документи, передбачені цим Регламентом і Законом для набуття статусу кваліфікованого надавача;

2) заяви про внесення змін до Довірчого списку та документи, передбачені цим Регламентом і Законом для внесення змін до Довірчого списку;

3) дозволи суб’єктів персональних даних на оброблення їхніх персональних даних у засвідчувальному центрі.

12. Форми документів, зазначених у пунктах 10, 11 розділу I цього Регламенту, розміщуються на вебсайті засвідчувального центру.

Заявник має право засвідчити власноручний підпис/кваліфікований електронний підпис на документах, зазначених у пунктах 10, 11 розділу I цього Регламенту, печаткою/електронною печаткою.

13. Заявник подає документи, передбачені цим Регламентом і Законом, у паперовій формі за адресою 01601, м. Київ, вул. Інститутська, 9.

Заявник подає документи, передбачені цим Регламентом і Законом, у формі електронних документів на електронну поштову скриньку Національного банку nbu@bank.gov.ua або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку.

14. Засвідчувальний центр не приймає до розгляду документи, копії документів, які мають виправлення або дописки чи пошкодження, що не дають змоги однозначно тлумачити зміст таких документів.

15. На вебсайті засвідчувального центру розміщується така інформація:

1) відомості про засвідчувальний центр (ідентифікаційні дані);

2) сертифікати ключів засвідчувального центру;

3) перелік кваліфікованих електронних довірчих послуг, які надає засвідчувальний центр;

4) інформація про графік роботи засвідчувального центру;

5) регламент роботи засвідчувального центру;

6) форми заяв;

7) перелік нормативно-правових актів у сфері електронних довірчих послуг;

8) відомості про кваліфікованих надавачів;

9) реєстр чинних, блокованих та скасованих сертифікатів ключів;

10) відомості про обмеження під час використання сертифікатів ключів, сформованих засвідчувальним центром;

11) інформація про порядок перевірки чинності сертифіката ключа;

12) СВС;

13) інформація про рішення засвідчувального центру щодо внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача;

14) повідомлення про припинення надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем;

15) відомості про прийняття від кваліфікованих надавачів на зберігання

документованої інформації в разі припинення їхньої діяльності.

ІІ. Перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує засвідчувальний центр

16. Засвідчувальний центр надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки кваліфікованим надавачам із використанням самопідписаних кваліфікованих сертифікатів відкритих ключів електронної печатки засвідчувального центру (далі – самопідписаний сертифікат ключа засвідчувального центру).

17. Засвідчувальний центр надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки кваліфікованим надавачам на договірних засадах у рамках Публічної пропозиції Національного банку України на укладення Єдиного договору банківського обслуговування та надання інших послуг Національним банком України, розміщеної на сторінці офіційного Інтернет-представництва Національного банку.

ІІІ. Організаційна структура засвідчувального центру

18. Національний банк для забезпечення виконання організаційних, технічних і технологічних функцій засвідчувального центру призначає працівників, що виконують функції:

1) керівника засвідчувального центру;

2) заступника керівника засвідчувального центру;

3) адміністратора реєстрації;

4) адміністратора сертифікації;

5) системного адміністратора;

6) адміністратора безпеки.

19. Керівник засвідчувального центру, заступник керівника засвідчувального центру, адміністратор реєстрації, адміністратор сертифікації, системний адміністратор, адміністратор безпеки перед початком виконання своїх функціональних обов’язків зобов’язані ознайомитися зі змістом цього Регламенту.

20. Керівник засвідчувального центру та заступник керівника

засвідчувального центру здійснюють загальне керівництво діяльністю засвідчувального центру і контроль за його діяльністю.

21. Керівник засвідчувального центру:

1) дає доручення, обов’язкові для заступника керівника засвідчувального центру, адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки;

2) підписує розпорядчі акти, інструкції, проектну й експлуатаційну документацію, інші документи, що визначають організаційні, технічні і технологічні умови діяльності засвідчувального центру;

3) підписує документи, які засвідчувальний центр подає до центрального засвідчувального органу.

22. Заступник керівника засвідчувального центру виконує функції керівника засвідчувального центру в разі його відсутності або за його письмовим дорученням.

23. Адміністратор реєстрації відповідає за:

1) ідентифікацію, автентифікацію, верифікацію заявників;

2) опрацювання поданих заявниками документів і запитів.

24. Основними обов’язками адміністратора реєстрації є:

1) ідентифікація, автентифікація, верифікація заявників та представників заявників;

2) опрацювання документів і запитів, які подаються заявником до засвідчувального центру:
для набуття статусу кваліфікованого надавача;
для внесення змін про кваліфікованого надавача до Довірчого списку;
для отримання послуг, передбачених розділом ІІ цього Регламенту;
у разі припинення надання кваліфікованих електронних довірчих послуг;
під час передавання на зберігання документованої інформації в разі припинення їхньої діяльності;

3) публікація на вебсайті засвідчувального центру інформації про рішення засвідчувального центру щодо внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача;

4) публікація на вебсайті засвідчувального центру повідомлення про

припинення надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем;

5) публікація на вебсайті засвідчувального центру відомостей про прийняття від кваліфікованих надавачів на зберігання документованої інформації в разі припинення їхньої діяльності.

25. Адміністратор сертифікації відповідає за:

1) формування сертифікатів ключів;

2) ведення реєстру чинних, блокованих та скасованих сертифікатів ключів;

3) генерацію, створення резервних копій, використання особистих ключів засвідчувального центру;

4) зберігання особистих ключів і резервних копій особистих ключів засвідчувального центру.

26. Основними обов’язками адміністратора сертифікації є:

1) генерація пар ключів засвідчувального центру;

2) створення резервних копій особистих ключів засвідчувального центру;

3) зберігання особистих ключів і резервних копій особистих ключів засвідчувального центру;

4) забезпечення використання особистих ключів засвідчувального центру під час формування самопідписаних сертифікатів ключів засвідчувального центру;

5) забезпечення використання особистих ключів засвідчувального центру під час формування сертифікатів ключів кваліфікованих надавачів;

6) забезпечення використання особистих ключів засвідчувального центру під час надання інформації про статус сертифікатів ключів, сформованих засвідчувальним центром;

7) забезпечення використання особистих ключів засвідчувального центру під час зміни статусу сертифікатів ключів кваліфікованих надавачів;

8) знищення особистих ключів засвідчувального центру, строк чинності яких закінчився;

9) забезпечення внесення до реєстру чинних, блокованих та скасованих сертифікатів ключів інформації, передбаченої Законом;

10) забезпечення створення резервних копій реєстру чинних, блокованих та скасованих сертифікатів ключів;

11) участь у відновленні роботи інформаційно-телекомунікаційної системи засвідчувального центру після збоїв.

27. Системний адміністратор відповідає за належне функціонування інформаційно-телекомунікаційної системи засвідчувального центру.

28. Основними обов’язками системного адміністратора є:

1) установлення, налаштування, супроводження операційних систем, загальносистемного та спеціального програмного забезпечення на робочих місцях адміністраторів засвідчувального центру та на серверах засвідчувального центру;

2) забезпечення функціонування вебсайта засвідчувального центру;

3) забезпечення резервування реєстру засвідчувального центру;

4) забезпечення відновлення роботи інформаційно-телекомунікаційної системи засвідчувального центру після збоїв;

5) підключення робочих місць адміністраторів засвідчувального центру та серверів засвідчувального центру до інформаційної мережі Національного банку;

6) підключення вебсайта засвідчувального центру до інформаційної мережі Національного банку та до мережі Інтернет;

7) забезпечення технічного обслуговування технічного обладнання засвідчувального центру (крім засобів криптографічного захисту інформації);

8) налаштування ведення журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи засвідчувального центру.

29. Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру.

30. Основними обов’язками адміністратора безпеки є:

1) проектування, розроблення, експлуатація, обслуговування та модернізація комплексної системи захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру;

2) контроль процесу генерації пар ключів засвідчувального центру та процесу створення резервних копій особистих ключів засвідчувального центру;

3) контроль за зберіганням особистих ключів та резервних копій особистих ключів засвідчувального центру;

4) контроль за зберіганням особистих ключів адміністраторів;

5) участь у знищенні особистих ключів засвідчувального центру;

6) контроль за своєчасним знищенням адміністраторами їхніх особистих ключів;

7) участь у відновленні роботи інформаційно-телекомунікаційної системи засвідчувального центру після збоїв;

8) ведення журналів обліку, передбачених документацією на комплексну систему захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру;

9) перегляд та аналіз журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи засвідчувального центру;

10) щорічне проведення перевірок дотримання адміністраторами реєстрації, адміністраторами сертифікації, системними адміністраторами вимог документації щодо комплексної системи захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру.

31. Адміністратором безпеки може бути особа, яка має стаж роботи у сфері захисту інформації або кібербезпеки не менше трьох років та відповідає хоча б одній із умов:

1) має вищу освіту за спеціальністю у сферах захисту інформації або кібербезпеки;

2) має вищу освіту за спеціальністю у сфері інформаційних технологій та пройшла курси підвищення кваліфікації у сфері захисту інформації або кібербезпеки.

32. Забороняється суміщення обов’язків адміністратора безпеки з обов’язками адміністратора реєстрації, адміністратора сертифікації, системного

адміністратора.

IV. Внесення до Довірчого списку відомостей/змін про кваліфікованих надавачів, виключення відомостей про кваліфікованих надавачів із Довірчого списку

33. Заявник для внесення відомостей про нього до Довірчого списку подає до засвідчувального центру заяву про внесення до Довірчого списку та документи, визначені частиною другою статті 30 Закону.

34. Надавач електронних довірчих послуг до подання заяви про внесення до Довірчого списку зобов'язаний:

1) виконати вимоги Положення про кваліфікованих надавачів електронних довірчих послуг, унесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116;

2) розробити регламент роботи кваліфікованого надавача та погодити його із засвідчувальним центром;

3) укласти з Національним банком договір про надання засвідчувальним центром послуг у рамках Публічної пропозиції Національного банку України на укладення Єдиного договору банківського обслуговування та надання інших послуг Національним банком України, розміщеної на сторінці офіційного Інтернет-представництва Національного банку;

4) внести кошти на поточний рахунок зі спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або забезпечити страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам електронних довірчих послуг чи третім особам унаслідок неналежного виконання кваліфікованим надавачем своїх зобов'язань, у розмірі, визначеному частиною третьою статті 16 Закону.

35. Засвідчувальний центр за результатами розгляду заяви про внесення до Довірчого списку та документів, визначених частиною другою статті 30 Закону, зобов'язаний протягом 15 робочих днів із дня реєстрації заяви про внесення до Довірчого списку прийняти рішення про внесення до Довірчого списку відомостей про кваліфікованого надавача або про відмову у внесенні до Довірчого списку відомостей про кваліфікованого надавача.

Засвідчувальний центр надсилає заявнику повідомлення про прийняте рішення після прийняття відповідного рішення не пізніше трьох робочих днів із дати прийняття цього рішення.

36. Засвідчувальний центр приймає рішення про відмову у внесенні до Довірчого списку відомостей про кваліфікованого надавача у разі:

1) подання не в повному обсязі документів, передбачених частиною другою статті 30 Закону або подання неналежним чином засвідчених копій документів;

2) виявлення в заяві про внесення до Довірчого списку та документах, що додаються до неї, недостовірної інформації;

3) виявлення в заяві про внесення до Довірчого списку та документах, що додаються до неї, хоча б однієї з причин, зазначених у пункті 14 розділу I цього Регламенту;

4) виявлення порушень надавачем електронних довірчих послуг вимог, установлених Законом, цим Регламентом, нормативно-правовими актами Національного банку у сфері електронних довірчих послуг та інформаційної безпеки.

37. Заявник зобов’язаний не пізніше ніж через п’ять робочих днів після подання заяви про внесення до Довірчого списку та документів, визначених частиною другою статті 30 Закону, подати документи для формування сертифіката ключа кваліфікованого надавача (окремо для кожної кваліфікованої електронної довірчої послуги) відповідно до вимог положення сертифікаційних практик, визначених у розділі VI цього Регламенту.

38. Кваліфікований надавач у разі виникнення підстав, передбачених Законом для внесення змін відомостей про нього до Довірчого списку, зобов’язаний протягом п’яти робочих днів із дня настання таких підстав подати до засвідчувального центру:

1) заяву про внесення змін до Довірчого списку разом із документами, що підтверджують відповідні зміни;

2) документи для формування сертифікатів ключів кваліфікованого надавача (окремо для кожної кваліфікованої електронної довірчої послуги) відповідно до вимог положення сертифікаційних практик, визначених у розділі VI цього Регламенту, якщо зміни відомостей, що містяться в Довірчому списку про цього кваліфікованого надавача, пов’язані з формуванням нових сертифікатів ключів кваліфікованого надавача.

39. Засвідчувальний центр за результатами розгляду заяви про внесення змін до Довірчого списку зобов’язаний протягом двох робочих днів із дня реєстрації заяви про внесення змін до Довірчого списку прийняти рішення про внесення відповідних змін до Довірчого списку або про відмову у внесенні змін

до Довірчого списку.

Засвідчувальний центр надсилає заявнику повідомлення про прийняте рішення після прийняття відповідного рішення.

40. Засвідчувальний центр приймає рішення про відмову у внесенні змін до Довірчого списку в разі:

1) неподання документів, що є підставою для внесення відповідних змін до Довірчого списку, або подання неналежним чином засвідчених копій документів;

2) виявлення в заяві про внесення змін до Довірчого списку та документах, що додаються до неї, недостовірної інформації;

3) виявлення в заяві про внесення до Довірчого списку та документах, що додаються до неї, хоча б однієї з причин, зазначених у пункті 14 розділу I цього Регламенту;

4) виявлення порушень надавачем електронних довірчих послуг вимог, установлених Законом, цим Регламентом, нормативно-правовими актами Національного банку у сфері електронних довірчих послуг та інформаційної безпеки.

41. Засвідчувальний центр надсилає до центрального засвідчувального органу подання про внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача протягом строків, зазначених у частині восьмій статті 30 Закону.

Подання про внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача включає:

1) повідомлення про прийняте рішення щодо внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача;

2) відомості про кваліфікованого надавача та кваліфіковані електронні довірчі послуги, які ним надаватимуться;

3) кваліфіковані сертифікати ключів, сформовані засвідчувальним центром, які кваліфікований надавач використовуватиме для надання відповідних кваліфікованих електронних довірчих послуг (у разі внесення до Довірчого списку відомостей про кваліфікованого надавача, якому засвідчувальний центр для надання кваліфікованих електронних довірчих послуг сформував сертифікати ключів або якщо зміни відомостей, що містяться в Довірчому списку про цього кваліфікованого надавача, пов’язані з формуванням нових сертифікатів ключів кваліфікованого надавача).

42. Засвідчувальний центр надсилає до центрального засвідчувального органу подання про виключення кваліфікованого надавача з Довірчого списку у разі:

1) подання кваліфікованим надавачем заяви про виключення відомостей про нього з Довірчого списку;

2) отримання інформації про припинення діяльності кваліфікованого надавача;

3) отримання інформації про набрання законної сили рішенням суду про виключення кваліфікованого надавача з Довірчого списку, визнання кваліфікованого надавача банкрутом.

V. Політика сертифіката

43. Засвідчувальний центр для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки кваліфікованим надавачам відповідно до вимог Закону формує такі сертифікати ключів засвідчувального центру:

1) самопідписані сертифікати ключів засвідчувального центру, що використовуються для перевірки сертифікатів ключів кваліфікованих надавачів і СВС;

2) сертифікати ключів засвідчувального центру, що використовуються для надання інформації про статус сертифікатів ключів кваліфікованих надавачів за запитом на інтерактивну перевірку статусу сертифіката ключа.

44. Засвідчувальний центр формує сертифікати ключів кваліфікованим надавачам, що використовуються кваліфікованими надавачами для надання електронних довірчих послуг/кваліфікованих електронних довірчих послуг відповідно до вимог Закону з урахуванням вимог їхніх регламентів роботи.

Кваліфіковані надавачі для надання кожної електронної довірчої послуги використовують окремий сертифікат ключа, сформований засвідчувальним центром.

45. Засвідчувальний центр зобов’язаний розмістити на вебсайті засвідчувального центру:

1) сертифікати ключів засвідчувального центру відразу після їх формування;

2) сертифікати ключів кваліфікованих надавачів не пізніше ніж наступного

робочого дня після внесення до Довірчого списку відомостей про кваліфікованих надавачів;

3) повний та частковий СВС на інформаційному ресурсі Засвідчувального центру відразу після їх формування.

46. Доступ до сертифікатів ключів засвідчувального центру, сертифікатів ключів кваліфікованих надавачів, повного та часткового СВС забезпечується цілодобово.

47. Підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування сертифіката ключа, здійснюється засобами програмно-технічного комплексу засвідчувального центру шляхом перевірки удосконаленого електронного підпису на запиті на формування сертифіката ключа з використанням відкритого ключа заявника, що міститься в запиті на формування сертифіката ключа.

48. Засвідчувальний центр здійснює ідентифікацію, автентифікацію, верифікацію заявників під час розгляду документів для внесення відомостей/змін відомостей про заявника до Довірчого списку, формування, блокування, скасування та поновлення сертифіката ключа кваліфікованого надавача, під час розгляду документів щодо припинення надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем, під час розгляду документів про прийняття від кваліфікованих надавачів на зберігання документованої інформації в разі припинення їхньої діяльності відповідно до вимог Закону та законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму.

49. Засвідчувальний центр здійснює ідентифікацію заявника шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади.

50. Засвідчувальний центр здійснює ідентифікацію:

1) юридичної особи за її установчими документами та даними, одержаними з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань;

2) фізичної особи за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

51. Засвідчувальний центр здійснює перевірку обсягів повноважень:

1) уповноваженого представника юридичної особи за документом, який відповідно до вимог законодавства України підтверджує його повноваження або згідно з даними Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, що визначають повноваження представника;

2) уповноваженого представника колегіального органу юридичної особи за документом, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

52. Засвідчувальний центр здійснює:

1) автентифікацію уповноваженого представника заявника під час оброблення документів у формі електронних документів, передбачених цим Регламентом і Законом, шляхом перевірки та підтвердження кваліфікованого електронного підпису на відповідному документі;

2) верифікацію уповноваженого представника заявника під час оброблення документів у формі паперових документів, передбачених цим Регламентом і Законом, на підставі поданих заявником офіційних документів або засвідчених у встановленому порядку їх копій. Документи, які заявник подав для встановлення ідентифікаційних даних уповноваженого представника заявника, мають бути чинними (дійсними) на момент їх подання та включати всі необхідні ідентифікаційні дані.

53. Усі складові частини програмно-технічного комплексу засвідчувального центру перебувають у межах контрольованих зон об'єктів Національного банку, на яких вони розташовані.

Національний банк зобов'язаний забезпечити з дотриманням вимог Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України від 04 липня 2007 року № 243 (зі змінами), зареєстрованих у Міністерстві юстиції України 17 серпня 2007 року за № 955/14222, управління фізичним доступом до приміщень, в яких розташовані:

1) засоби кваліфікованого електронного підпису чи печатки, в яких зберігаються та використовуються особисті ключі засвідчувального центру;

2) засоби кваліфікованого електронного підпису чи печатки, в яких зберігаються резервні копії особистих ключів засвідчувального центру;

3) технічні засоби програмно-технічного комплексу засвідчувального центру.

54. Національний банк відшкодовує шкоду, заподіяну засвідчувальним центром кваліфікованим надавачам, у повному розмірі в установленому законом порядку.

Керівник засвідчувального центру, заступник керівника засвідчувального центру, адміністратор реєстрації, адміністратор сертифікації, системний адміністратор, адміністратор безпеки несуть відповідальність за неналежне виконання своїх обов'язків та розголошення інформації з обмеженим доступом згідно із законом.

Функціональні обов'язки керівника засвідчувального центру, заступника керівника засвідчувального центру, адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки визначаються цим Регламентом.

55. Засвідчувальний центр забезпечує ведення журналів аудиту подій, в яких реєструються події таких типів:

1) спроби створення, знищення, встановлення паролів, зміни прав доступу в інформаційно-телекомунікаційній системі засвідчувального центру;

2) заміни програмного забезпечення, технічних засобів інформаційно-телекомунікаційної системи засвідчувального центру;

3) технічне обслуговування інформаційно-телекомунікаційної системи засвідчувального центру;

4) генерація, використання, знищення особистих ключів засвідчувального центру;

5) формування, блокування, скасування та поновлення сертифікатів ключів, формування СВС;

6) спроби несанкціонованого доступу до інформаційно-телекомунікаційної системи засвідчувального центру;

7) надання доступу адміністраторам до інформаційно-телекомунікаційної системи засвідчувального центру;

8) збої в роботі інформаційно-телекомунікаційної системи засвідчувального центру.

56. Адміністратор безпеки засвідчувального центру зобов'язаний вести журнали обліку, передбачені документацією на комплексну систему захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру.

57. Записи в журналах аудиту подій та журналах обліку повинні містити дату та час події, а також ідентифікувати суб’єкта, що здійснив або ініціював подію.

58. Час, що використовується в журналах аудиту подій в електронній формі, повинен бути синхронізований із Всесвітнім координованим часом із точністю до секунди.

59. Засвідчувальний центр забезпечує захист журналів аудиту подій від неавторизованого перегляду, несанкціонованої модифікації та від знищення.

60. Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор мають право переглядати журнали аудиту подій, пов’язані з виконанням їх функціональних обов’язків.

Керівник засвідчувального центру, заступник керівника засвідчувального центру, адміністратор безпеки мають право переглядати всі журнали аудиту подій, які ведуться у засвідчувальному центрі, та всі журнали обліку, передбачені документацією на комплексну систему захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру.

61. Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор зобов’язані:

1) переглядати журнали аудиту подій не рідше одного разу на місяць;

2) повідомляти адміністратора безпеки про наявність несанкціонованої модифікації в інформаційно-телекомунікаційній системі засвідчувального центру, виявлену під час перегляду журналів аудиту подій.

62. Адміністратор безпеки зобов’язаний переглядати журнали аудиту подій не рідше одного разу на тиждень.

63. Засвідчувальний центр забезпечує зберігання протягом п’яти років:

1) журналів аудиту подій;

2) журналів обліку, передбачених документацією на комплексну систему захисту інформації інформаційно-телекомунікаційної системи засвідчувального центру.

64. Засвідчувальний центр забезпечує зберігання документованої інформації (документів, на підставі яких кваліфікованим надавачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані сертифікати ключів, усіх сформованих сертифікатів ключів, а також реєстрів сформованих сертифікатів ключів), списків відкликаних

сертифікатів протягом строку, встановленого Правилами застосування переліку документів, що утворюються в діяльності Національного банку України та банків України, затвердженими постановою Правління Національного банку України від 27 листопада 2018 року № 130 (зі змінами), до передавання на архівне зберігання.

65. Засвідчувальний центр обліковує та зберігає звіти про роботу кваліфікованих надавачів електронних довірчих послуг протягом п’яти років.

66. Національний банк зобов’язаний створити систему резервування та відновлення функціонування інформаційно-телекомунікаційної системи засвідчувального центру, яка має забезпечити резервування на основних майданчиках та у віддаленому резервному пункті такої інформації, із забезпеченням її захисту від несанкціонованого доступу:

1) інструкції щодо відновлення роботи інформаційно-телекомунікаційної системи засвідчувального центру;

2) програмне забезпечення інформаційно-телекомунікаційної системи засвідчувального центру;

3) резервні копії особистих ключів засвідчувального центру;

4) резервна копія реєстру засвідчувального центру;

5) усі сформовані засвідчувальним центром сертифікати ключів;

6) журнали аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи засвідчувального центру.

67. Інформація, зазначена в підпунктах 1–3 пункту 66 розділу V цього Регламенту, резервується в разі внесення змін до відповідних інструкцій/зміни програмного забезпечення/заміни чи генерування нових особистих ключів засвідчувального центру.

Періодичність резервування інформації, зазначеної в підпунктах 4–6 пункту 66 розділу V цього Регламенту, – не рідше ніж один раз на тиждень.

68. Засвідчувальний центр здійснює відновлення функціонування інформаційно-телекомунікаційної системи засвідчувального центру відповідно до плану забезпечення безперервної роботи, затвердженого керівником засвідчувального центру.

69. Адміністратор сертифікації за участю адміністратора безпеки здійснює генерацію пар ключів засвідчувального центру з такими параметрами:

1) для формування та перевірки сертифікатів ключів кваліфікованих надавачів і СВС зі ступенем розширення основного поля еліптичної кривої не менше 431 згідно з національним стандартом України ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”, затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002);

2) для надання та перевірки інформації про статус сертифікатів ключів кваліфікованих надавачів за запитом на інтерактивну перевірку статусу сертифіката ключа зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

3) для формування та перевірки сертифікатів ключів кваліфікованих надавачів і СВС із використанням еліптичної кривої NIST P-256 для алгоритму ECDSA згідно з національним стандартом України ДСТУ ETSI TS 119 312:2015 “Електронні підписи й інфраструктури (ESI). Криптографічні комплекти”, прийнятим наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 05 листопада 2015 року № 145 (зі змінами) (далі – ДСТУ ETSI TS 119 312:2015);

4) для надання та перевірки інформації про статус сертифікатів ключів кваліфікованих надавачів за запитом на інтерактивну перевірку статусу сертифіката ключа із використанням еліптичної кривої NIST P-256 для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;

5) для формування та перевірки сертифікатів ключів кваліфікованих надавачів і СВС з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI TS 119 312:2015;

6) для надання та перевірки інформації про статус сертифікатів ключів кваліфікованих надавачів за запитом на інтерактивну перевірку статусу сертифіката ключа з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI TS 119 312:2015.

Особисті ключі засвідчувального центру генеруються, зберігаються, використовуються виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

70. Адміністратор сертифікації створює резервні копії особистих ключів засвідчувального центру за участю адміністратора безпеки. Адміністратор безпеки реєструє факти створення резервних копій особистих ключів засвідчувального центру у відповідному журналі обліку.

Резервні копії особистих ключів засвідчувального центру зберігаються у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

71. Особистий ключ засвідчувального центру та всі його резервні копії після закінчення строку дії сертифіката ключа засвідчувального центру знищуються способом, що унеможливлює їх відновлення.

Адміністратор сертифікації здійснює знищення особистих ключів засвідчувального центру та їх резервних копій за участю адміністратора безпеки.

72. Засвідчувальний центр не надає засоби кваліфікованого електронного підпису чи печатки заявникам. Заявник самостійно генерує пари ключів.

73. Заявник після генерації пар ключів подає до засвідчувального центру запит на формування сертифіката ключа кваліфікованого надавача відповідно до вимог положення сертифікаційних практик, визначених у розділі VI цього Регламенту.

VI. Положення сертифікаційних практик

74. Засвідчувальний центр формує кваліфікованому надавачеві сертифікати ключів у разі прийняття засвідчувальним центром рішення щодо внесення до Довірчого списку:

1) відомостей про кваліфікованого надавача;

2) змін відомостей про кваліфікованого надавача.

75. Заявник для формування сертифіката ключа подає до засвідчувального центру згідно з вимогами пунктів 10, 12, 13 розділу I цього Регламенту:

1) заяву про отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

2) запит на формування сертифіката ключа.

76. Заявник зобов’язаний забезпечити відповідність запиту на формування сертифіката ключа Вимогам до запиту на формування сертифіката ключа кваліфікованого надавача, визначеним у додатку до цього Регламенту.

Заявник має право включити до запиту на формування сертифіката ключа додаткові ідентифікаційні дані кваліфікованого надавача та необов’язкові додаткові спеціальні атрибути, визначені в таких стандартах для сертифікатів ключів:

1) національний стандарт України ДСТУ ETSI EN 319 412-1:2016 (ETSI EN 319 412-1:2016, IDT) “Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних”, прийнятий наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 21 червня 2016 року № 183 (зі змінами);

2) національний стандарт України ДСТУ ETSI EN 319 412-3:2016 (ETSI EN 319 412-3:2016, IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профіль сертифіката юридичної особи”, прийнятий наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 27 грудня 2016 року № 451 (зі змінами);

3) національний стандарт України ДСТУ ETSI EN 319 412-5:2016 (ETSI EN 319 412-5:2016, IDT) “Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 5. Системи контролю якості”, прийнятий наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 23 вересня 2016 року № 279 (зі змінами).

77. Засвідчувальний центр за результатами розгляду поданих заявником документів для формування сертифіката ключа, зазначених у пункті 75 розділу VI цього Регламенту, приймає рішення про відмову у формуванні сертифіката ключа заявника, якщо:

1) подано не всі необхідні документи;

2) подано неналежним чином засвідчені копії документів;

3) установлено невідповідність даних, зазначених у поданих документах, фактичним;

4) виявлено невідповідність даних, зазначених у запиті на формування сертифіката ключа або в заяві про отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, з даними, унесеними до реєстру засвідчувального центру;

5) відкритий ключ, що міститься у запиті на формування сертифіката ключа, за відомостями з реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів не є унікальним;

6) перевірка належності заявнику особистого ключа, що відповідає

відкритому ключу, який міститься у запиті на формування сертифіката ключа, є негативною;

7) запит на формування сертифіката ключа не відповідає вимогам, наведеним у додатку до цього Регламенту.

Засвідчувальний центр у разі прийняття рішення про відмову у формуванні сертифіката ключа заявника надає заявнику вмотивовану відмову у формуванні сертифіката ключа в письмовому вигляді.

78. Засвідчувальний центр у разі відсутності зауважень до поданих заявником документів для формування сертифіката ключа, зазначених у пункті 75 розділу VI цього Регламенту, формує сертифікат ключа кваліфікованого надавача не пізніше ніж на наступний день після прийняття рішення про внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача.

Засвідчувальний центр встановлює у кваліфікованому сертифікаті відкритого ключа кваліфікованого надавача додаткові розширення, які містяться у запиті на формування сертифіката ключа, за умови, що додаткові розширення були визначені як некритичні, а об’єктні ідентифікатори таких розширень зареєстровані в установленому порядку.

79. Кваліфікований надавач після формування його сертифіката ключа зобов’язаний перевірити правильність відомостей, що містяться в сертифікаті ключа. Кваліфікований надавач у разі виявлення некоректних даних (помилки в реквізитах) зобов’язаний повідомити про це засвідчувальний центр. Засвідчувальний центр у такому разі скасовує сертифікат ключа кваліфікованого надавача та формує новий сертифікат ключа.

80. Засвідчувальний центр після формування сертифіката ключа кваліфікованого надавача та перевірки заявником правильності відомостей, що містяться в сертифікаті ключа Центру:

1) надсилає до центрального засвідчувального органу подання про внесення до Довірчого списку відомостей/змін відомостей про кваліфікованого надавача відповідно до вимог пункту 41 розділу IV цього Регламенту;

2) здійснює публікацію сертифіката ключа кваліфікованого надавача на вебсайті засвідчувального центру відповідно до вимог пункту 45 розділу V цього Регламенту.

81. Кваліфікований надавач:

1) зобов’язаний використовувати сертифікати ключів кваліфікованих надавачів, сформовані у засвідчувальному центрі, виключно за призначенням (сферою використання) – для надання електронних довірчих

послуг/кваліфікованих електронних довірчих послуг;

2) несе відповідальність за неправильне використання сертифікатів ключів кваліфікованого надавача, сформованих у засвідчувальному центрі, та особистих ключів кваліфікованого надавача згідно із Законом;

3) має право використовувати пару ключів тільки протягом строку дії відповідного сертифіката ключа кваліфікованого надавача та за умови, що сертифікат ключа чинний.

82. Засвідчувальний центр:

1) скасовує сертифікат ключа кваліфікованого надавача у випадках та в строки, передбачені частинами першою та третьою статті 25 Закону;

2) блокує сертифікат ключа кваліфікованого надавача у випадках та в строки, передбачені частинами шостою та сьомою статті 25 Закону;

3) поновлює сертифікат ключа кваліфікованого надавача у випадках та в строки, передбачені частиною десятою статті 25 Закону.

83. Заявник подає до засвідчувального центру заяву про скасування сертифіката ключа кваліфікованого надавача, заяву про блокування сертифіката ключа кваліфікованого надавача, заяву про поновлення сертифіката ключа кваліфікованого надавача згідно з вимогами пунктів 10, 12, 13 розділу I цього Регламенту.

84. Скасування, блокування, поновлення сертифіката ключа кваліфікованого надавача набирає чинності з моменту внесення відповідних змін до реєстру засвідчувального центру.

Відомості щодо скасування/блокування/поновлення сертифіката ключа кваліфікованого надавача вносяться до СВС із зазначенням дати та часу здійснення відповідної операції.

Засвідчувальний центр повідомляє кваліфікованого надавача про зміну статусу сертифіката ключа кваліфікованого надавача відразу після здійснення скасування/блокування/поновлення сертифіката ключа кваліфікованого надавача.

85. Засвідчувальний центр надає інформацію про статус сертифіката ключа кваліфікованого надавача (чинний/скасований/блокований) шляхом публікації СВС на вебсайті засвідчувального центру та за запитом на інтерактивну перевірку статусу сертифіката ключа.

86. Засвідчувальний центр публікує на вебсайті засвідчувального центру повний та частковий СВС.

Повний СВС публікується не рідше одного разу на тиждень, не пізніше закінчення строку дії попереднього СВС та містить інформацію про всі відкликані сертифікати ключів, сформовані засвідчувальним центром.

Частковий СВС публікується не рідше одного разу на дві години, не пізніше закінчення строку дії попереднього часткового СВС та містить інформацію про всі відкликані сертифікати ключів, статус яких був змінений в інтервалі часу між часом випуску останнього повного СВС та часом формування поточного часткового СВС.

У кожному СВС зазначається дата та час формування наступного СВС. Наступний СВС може бути опублікований до настання граничного терміну його дії для видання наступного СВС. Засвідчувальний центр підписує кожен СВС особистим ключем засвідчувального центру, що призначений для формування та перевірки сертифікатів ключів кваліфікованих надавачів і СВС.

87. Інформація про статус сертифіката ключа за запитом на інтерактивну перевірку статусу сертифіката ключа розповсюджується відповідно до вимог, установлених національним стандартом України ДСТУ ETSI EN 319 411-2:2016 (ETSI EN 319 411-2:2016, IDT) “Електронні підписи й інфраструктури (ESI). Вимоги політики та безпеки для провайдерів трастових послуг, які видають сертифікати. Частина 2. Вимоги до провайдерів трастових послуг, які видають кваліфіковані сертифікати ЄС”, прийнятим наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 21 червня 2016 року № 183 (зі змінами).

88. Строк дії сертифіката ключа засвідчувального центру не може перевищувати десяти років.

Строк дії сертифіката ключа кваліфікованого надавача, сформованого у засвідчувальному центрі, не може перевищувати п’яти років.

Директор
Департаменту безпеки Олександр СКОМАРОВСЬКИЙ

Додаток
до Регламенту роботи
Засвідчувального центру
Національного банку України
(пункт 76 розділу VI)

Вимоги до запиту на формування сертифіката ключа кваліфікованого надавача

1. Формат запиту на формування сертифіката ключа кваліфікованого надавача має відповідати специфікації синтаксису запиту на формування сертифіката, визначеній в RFC 2986 “PKCS #10: Certification Request Syntax Specification”.

2. Параметри відкритого ключа у запиті на формування сертифіката ключа кваліфікованого надавача мають відповідати таким вимогам:

1) ступінь розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

2) ступінь розширення основного поля еліптичної кривої не менше 256 для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;

3) довжина ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI TS 119 312:2015.

3. Запит на формування сертифіката ключа кваліфікованого надавача має містити обов’язкові реквізити, зазначені в таблицях 1, 2 цього додатка.

Продовження додатка

Таблиця 1

Обов’язкові реквізити, що належать до структури certificationRequestInfo
запиту на формування сертифіката ключа кваліфікованого надавача

№ з/п	Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту
1	2	3	4
1	CountryName	Назва країни	Країна, в якій зареєстрований заявник: id-at-countryName AttributeType: : = {id-at 6} X520countryName : : = PrintableString (SIZE (2)) код згідно з міжнародним стандартом ISO 3166 (для України – UA)
2	OrganizationName	Найменування організації	Повне (або офіційне скорочене) найменування заявника згідно з установчими документами або відомостями про державну реєстрацію: id-at-organizationName AttributeType: : = {id-at 10} X520organizationName : : = DirectoryString (SIZE (64))
3	SerialNumber[1]	Серійний номер	Унікальний реєстраційний номер заявника: id-at-serialNumber AttributeType: : = {id-at 5} serialNumber: : =PrintableString (SIZE (64)). Цей реквізит формується за правилом: UA-<код за ЄДРПОУ>-<1-4 цифри(за потреби)>

[1] Поле встановлюється, якщо відкритий ключ згенеровано за криптографічним алгоритмом згідно з ДСТУ 4145-2002.

Продовження додатка

Продовження таблиці 1

1	2	3	4
4	StateOrProvinceName[1]	Назва області	Область, у якій зареєстрований заявник: id-at-stateOrProvinceName AttributeType : : = {id-at 8} X520stateOrProvinceName : : = DirectoryString (SIZE (64))
5	LocalityName	Назва міста	Місто, в якому зареєстрований заявник: id-at-localityName AttributeType: : = {id-at 7} X520localityName : : = DirectoryString (SIZE (64))
6	CommonName	Загальне ім’я	Назва кваліфікованої послуги кваліфікованого надавача: id-at-commonName AttributeType: : = {id-at 3} X520commonName : : = DirectoryString (SIZE (64))
7	OrganizationIdentifier[2]	Ідентифікатор заявника	Унікальний ідентифікатор заявника: id-at-organizationIdentifier OBJECT IDENTIFIER ::= {id-at 97}. Правила заповнення цього реквізиту: NTRUA-“код за ЄДРПОУ” (відповідно до пункту 5.1.4 глави 5 ДСТУ ETSI EN 319 412-1:2016)

[1] Якщо місцем реєстрації заявника є місто Київ або місто Севастополь, реквізит stateOrProvinceName не заповнюється.

[2] Поле встановлюється, якщо відкритий ключ згенеровано за криптографічним алгоритмом згідно з ДСТУ ETSI TS 119 312:2015.

Продовження додатка

Продовження таблиці 1

1	2	3	4
8	SubjectPublicKeyInfo	Інформація про відкритий ключ заявника	Значення відкритого ключа, параметри криптографічних перетворень (для ДСТУ 4145-2002 та ECDSA) та ідентифікатор криптографічного алгоритму, що використовується для обчислення відкритого ключа
9			Ідентифікатор криптографічного алгоритму, що використовується для обчислення відкритого ключа згідно з ДСТУ 4145-2002, визначається відповідно до вимог, установлених технічними вимогами до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються Міністерством юстиції України та Державною службою спеціального зв’язку та захисту інформації України
10			Ідентифікатор криптографічного алгоритму, що використовується для обчислення відкритого ключа ECDSA згідно з ДСТУ ETSI TS 119 312:2015: id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9.62(10045) id-publicKeyType(2) 1}
11			Ідентифікатор криптографічного алгоритму, що використовується для обчислення відкритого ключа RSA: rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

Продовження додатка

Таблиця 2

Інші реквізити, що належать до складу запиту на формування сертифіката ключа кваліфікованого надавача

№ з/п	Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту
1	2	3	4
1	SignatureAlgorithm	Назва криптографічного алгоритму, що використовується для підписання запиту	1) значення реквізиту для алгоритмів кваліфікованого електронного підпису згідно з ДСТУ 4145-2002 визначається відповідно до вимог, установлених технічними вимогами до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються Міністерством юстиції України та Державною службою спеціального зв’язку та захисту інформації України; 2) значення реквізиту для алгоритму кваліфікованого електронного підпису ECDSA з алгоритмом гешування SHA256: ecdsa-with-SHA256 OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 2}; 3) значення реквізиту для алгоритму кваліфікованого електронного підпису ECDSA з алгоритмом гешування SHA512: ecdsa-with-SHA512 OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 4};

Продовження додатка

Продовження таблиці 2

1	2	3	4
			4) значення реквізиту для алгоритму кваліфікованого електронного підпису RSA з алгоритмом гешування SHA256: sha-256WithRSAEncryption OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}; 5) значення реквізиту для алгоритму кваліфікованого електронного підпису RSA з алгоритмом гешування SHA512: sha-512WithRSAEncryption OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
2	Signature	Удосконалений електронний підпис	Результат підписання структури certificationRequestInfo