Проект

Правління Національного банку України

П О С Т А Н О В А

_____ м. Київ №_____

Про затвердження вимог до кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру

Відповідно до статей 7, 15, 56 Закону України “Про Національний банк України”, статті 9 Закону України “Про електронні довірчі послуги”, Правління Національного банку України **постановляє**:

1. Затвердити Вимоги до кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, що додаються.

2. Кваліфікованим надавачам електронних довірчих послуг у банківській системі здійснити процедуру набуття статусу кваліфікованого надавача електронних довірчих послуг в засвідчувальному центрі не пізніше двох років з дня набрання чинності Закону України “Про електронні довірчі послуги”.

3. Департаменту безпеки (Олександр Скомаровський) після офіційного опублікування довести зміст цієї постанови до відома банків України для використання в роботі.

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

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

Голова Яків СМОЛІЙ

Інд. 56

Проект

ЗАТВЕРДЖЕНО
Постанова Правління
Національного банку України
___ _____ 2019 року № ___

Вимоги до кваліфікованих надавачів електронних
довірчих послуг, внесених до Довірчого списку
за поданням засвідчувального центру

1. Ці вимоги розроблені відповідно до статті 7 Закону України “Про Національний банк України”, статті 9 Закону України “Про електронні довірчі послуги”.

2. Ці вимоги визначають організаційні умови створення кваліфікованих надавачів електронних довірчих послуг у банківській системі України, кваліфікованих надавачів електронних довірчих послуг при здійсненні переказу коштів (учасників платіжних систем) (далі разом – надавачі), а також організаційні, технічні та технологічні вимоги, яких повинні дотримуватися надавачі та їх відокремлені пункти реєстрації у своїй діяльності.

3. Ці Вимоги базуються на нормах національних стандартів України

ДСТУ ETSI EN 319 401:2016 «Електронні підписи й інфраструктури (ESI). Загальні вимоги політики для провайдерів довірчих послуг», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183, (ETSI EN 319 401:2016, IDT) (далі – ДСТУ ETSI EN 319 401);

ДСТУ ETSI EN 319 411-1:2016 «Електронні підписи й інфраструктури (ESI). Вимоги політики та безпеки для провайдерів трастових послуг, які видають сертифікати. Частина 1. Загальні вимоги», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183, (ETSI EN 319 411-1:2016, IDT) (далі – ДСТУ ETSI EN 319 411-1);

ДСТУ ETSI EN 319 411-2:2016 «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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183, (ETSI EN 319 411-2:2016, IDT) (далі – ДСТУ ETSI EN 319 411-2);

ДСТУ ETSI EN 319 421:2016 «Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183, (ETSI EN 319 421:2016, IDT) (далі – ДСТУ ETSI EN 319 421);

У разі виникнення розбіжностей між нормами зазначених стандартів та нормами цих Вимог застосовуються норми цих Вимог.

4. У цих Вимогах терміни вживаються в такому значенні:

довірча послуга – електронна довірча послуга або кваліфікована електронна довірча послуга;

засіб електронного підпису чи печатки – засіб удосконаленого електронного підпису чи печатки або засіб кваліфікованого електронного підпису чи печатки;

інформаційно-телекомунікаційна система надавача – сукупність інформаційних і телекомунікаційних систем надавача та його відокремлених пунктів реєстрації, що об’єднує програмно-технічний комплекс, який використовується для надання довірчих послуг, фізичне середовище, інформацію, що обробляється в зазначених системах, а також працівників надавача;

клієнт – клієнт банку або користувач платіжної системи (фізична особа або представник юридичної особи), що звернувся до надавача для отримання довірчих послуг або отримує довірчі послуги;

особисті ключі надавача – особисті ключі, які надавач використовує для надання довірчих послуг.

Інші терміни цих Вимогах вживаються у значенні, наведеному в Законах України “Про електронні довірчі послуги”, “Про електронні документи та електронний документообіг”, “Про платіжні системи та переказ коштів в Україні”, “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення”.

5. Надавачами є суб’єкти банківської системи або учасники платіжних систем або окремі юридичні особи, створені суб’єктами банківської системи/учасниками платіжних систем виключно для надання довірчих послуг.

Функції надавача у суб’єкта банківської системи/учасника платіжних систем може виконувати окремий спеціально створений підрозділ, що призначений виключно для надання довірчих послуг, або функції надавача можуть виконувати працівники наявних підрозділів.

6. Відомості про надавачів та кваліфіковані електронні довірчі послуги, які ним надаватимуться, вносяться до Довірчого списку за поданням засвідчувального центру. Надавачі мають право надавати електронні довірчі

послуги та кваліфіковані електронні довірчі послуги. Кваліфіковані електронні довірчі послуги, що надаються надавачами, внесеними до Довірчого списку за поданням засвідчувального центру, визнаються всіма суб'єктами відносин у сфері електронних довірчих послуг відповідно до вимог законодавства.

7. Засвідчувальний центр приймає рішення про внесення до Довірчого списку та надає кваліфіковані електронні довірчі послуги надавачам відповідно до Регламенту роботи засвідчувального центру.

На підставі прийнятого засвідчувальним центром рішення про внесення до Довірчого списку надавач засвідчує чинність одного або декількох своїх відкритих ключів (окремо для кожної кваліфікованої електронної довірчої послуги) у засвідчувальному центрі відповідно до вимог Регламенту роботи засвідчувального центру.

8. Надавач до подання заяви про внесення до Довірчого списку:

1) розробляє та погоджує свій регламент роботи із засвідчувальним центром. Надавач має право подавати на погодження проект Регламенту роботи у формі паперового документа або електронного документа. Погоджений регламент роботи надавача затверджується керівником надавача;

2) укладає з Національним банком України договір про надання засвідчувальним центром послуг відповідно до вимог Публічної пропозиції Національного банку України на укладення Єдиного договору банківського обслуговування та надання інших послуг Національним банком України, затвердженої рішенням Правління Національного банку України 03.01.2017 № 2-рш (зі змінами);

3) резервує кошти для забезпечення відшкодування збитків, які можуть бути завдані клієнтам, користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання надавачем своїх зобов'язань відповідно до вимог статей 13, 16 Закону України "Про електронні довірчі послуги".

9. Надавач зобов'язаний підтримувати розмір зарезервованих коштів в актуальному стані відповідно до розміру мінімальної заробітної плати, встановленого Законом України "Про Державний бюджет України" на відповідний рік.

У разі зміни розміру мінімальної заробітної плати протягом року або відшкодування збитків, завданих клієнтам, користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання своїх зобов'язань, надавач протягом трьох місяців вживає вичерпних заходів для відновлення розміру зарезервованих коштів.

10. Права та обов'язки надавачів визначені статтею 13 Закону України "Про електронні довірчі послуги".

Крім того, надавач зобов'язаний визначити відповідальність його

відокремлених пунктів реєстрації та контролювати виконання відокремленими пунктами реєстрації встановлених законодавством вимог інформаційної безпеки та процедури реєстрації клієнтів. Надавач несе відповідальність за діяльність його відокремлених пунктів реєстрації.

11. Надавач надає послуги своїм клієнтам на основі договору, що може бути окремим договором або частиною договору про надання банківських послуг.

Договір про надання довірчих послуг може бути змінено виключно за взаємною згодою сторін.

Надавач має право надавати довірчі послуги своїм працівникам для виконання їх службових обов'язків без укладання договору, на основі розпорядчого акту та заяви про отримання довірчих послуг, з дотриманням вимог щодо їх ідентифікації.

12. Договір про надання довірчих послуг має містити:

перелік довірчих послуг;

права та обов'язки сторін;

умови використання клієнтами засобів електронного підпису чи печатки (у разі коли довірча послуга передбачає використання засобу електронного підпису чи печатки);

умови використання клієнтом особистих ключів (у разі коли довірча послуга передбачає використання особистих ключів);

умови публікації сертифікатів відкритих ключів клієнта (у разі коли довірча послуга передбачає формування сертифікатів відкритих ключів);

строк дії договору;

умови оплати;

порядок внесення змін до договору;

порядок розірвання договору.

13. Підставами для розірвання договору про надання довірчих послуг є:

згода сторін;

рішення суду про розірвання договору;

оголошення клієнта померлим, визнання клієнта безвісно відсутнім, недієздатним, обмеження цивільної дієздатності клієнта;

виключення надавача з Довірчого списку (у разі надання кваліфікованих електронних довірчих послуг);

припинення діяльності надавача.

14. Якщо договором про надання довірчих послуг передбачено формування сертифікатів відкритих ключів, розірвання такого договору є підставою для скасування надавачем всіх сертифікатів відкритих ключів, сформованих для клієнта відповідно до договору.

15. Надавач визначає такі ролі для надання довірчих послуг:

1) керівник надавача;

2) заступник(и) керівника надавача (за необхідності);

3) адміністратор реєстрації (за необхідності – якщо надавач надає довірчі послуг, що передбачають ідентифікацію та верифікацію клієнтів);

4) адміністратор сертифікації (за необхідності – якщо надавач надає довірчі послуг, що передбачають формування та видачу сертифікатів відкритих ключів);

5) системний адміністратор;

6) адміністратор безпеки.

16. Надавач призначає працівників, що виконують функції керівника надавача, заступника(ів) керівника надавача, адміністратора(ів) реєстрації, адміністратора(ів) сертифікації, системного(их) адміністратора(ів), адміністратора(ів) безпеки розпорядчим документом.

17. Керівником надавача є керівник юридичної особи. Заступником керівника надавача є заступник керівника юридичної особи або відповідальна особа за інформаційну безпеку банку (Chief information security officer, CISO) або керівник підрозділу, що призначений виключно для надання довірчих послуг.

Керівник та заступник(и) керівника здійснюють загальне керівництво діяльністю надавача і контроль за його діяльністю.

Керівник надавача:

дає доручення, обов’язкові для працівників надавача, що виконують функції адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки;

затверджує розпорядчі документи, інструкції, проектну й експлуатаційну документацію, інші документи, що визначають організаційні, технічні та технологічні умови діяльності надавача;

підписує документи, які надавач подає до засвідчувального центру.

Керівник надавача зобов’язаний забезпечити створення умов для безперервної особистої освіти та постійне підвищення кваліфікації працівників надавача у сферах захисту персональних даних, інформаційних технологій, захисту інформації або кібербезпеки.

Заступник керівника надавача виконує функції керівника надавача в разі його відсутності або за його дорученням.

18. Адміністратор реєстрації відповідає за ідентифікацію та верифікацію клієнтів, надання за потреби допомоги підписувачам під час генерації пар ключів та опрацювання відповідних документів і запитів.

До працівників відокремлених пунктів реєстрації, на яких покладено обов’язки з реєстрації клієнтів, повинні застосовуватись такі ж вимоги, як і до адміністраторів реєстрації.

19. Адміністратор сертифікації відповідає за:

формування сертифікатів відкритих ключів;

ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

генерацію, створення резервних копій, використання особистих ключів надавача;

зберігання особистих ключів і резервних копій особистих ключів надавача.

20. Системний адміністратор відповідає за належне функціонування програмно-технічного комплексу надавача.

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

Адміністратор безпеки відповідає за проведення перевірок дотримання адміністраторами реєстрації, адміністраторами сертифікації, системними адміністраторами положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою. Надавач встановлює періодичність (у днях, тижнях або місяцях) проведення таких внутрішніх перевірок, але не рідше ніж один раз на рік.

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

22. Працівники надавача повинні мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію.

Системним адміністратором, адміністратором сертифікації може бути особа, яка має вищу освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом у зазначених сферах не менше трьох років.

Адміністратором безпеки може бути особа, яка має вищу освіту за спеціальністю у сферах захисту інформації, кібербезпеки або у сфері інформаційних технологій та пройшла курси підвищення кваліфікації у сфері захисту інформації або кібербезпеки і має стаж роботи сферах захисту інформації або кібербезпеки не менше трьох років.

23. Надавач та його відокремлені пункти реєстрації повинні виконувати вимоги Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України, затвердженого постановою Правління Національного банку України № 265 від 17.06.2004 та зареєстрованого в Міністерстві юстиції України 09.07.2004 за № 857/9456 (зі змінами), Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених

постановою Правління Національного банку України № 243 від 04.07.2007 та зареєстрованих в Міністерстві юстиції України 17.08.2007 за № 955/14222 (зі змінами), Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України № 95 від 28.09.2018.

24. Надавач зобов'язаний забезпечити захист інформації, що обробляється в інформаційно-телекомунікаційній системі надавача, шляхом впровадження системи управління інформаційної безпеки або комплексної системи захисту інформації з підтвердженою відповідністю.

25. Надавач повинен забезпечити можливість ознайомлення клієнтів з інформацією про умови отримання довірчих послуг, зокрема шляхом розміщення відповідної інформації на веб-сайті надавача.

26. Надавач зобов'язаних розмістити на своєму веб-сайті таку інформацію:
відомості про надавача;
сертифікати відкритих ключів надавача;
перелік довірчих послуг, які надає надавач;
дані про засоби електронного підпису чи печатки, які надавач надає своїм клієнтам (у разі коли довірча послуга передбачає використання засобу електронного підпису чи печатки);
форми документів, на підставі яких надаються довірчі послуги;
реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;
відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;
інформація про порядок перевірки чинності сертифіката відкритого ключа;
перелік актів законодавства у сфері електронних довірчих послуг.
Інформація на веб-сайті надавача повинна бути доступною для осіб з обмеженими фізичними можливостями.

27. Надавач зобов'язаний здійснювати ідентифікацію та верифікацію клієнта відповідно до вимог Закону України "Про електронні довірчі послуги" та законодавства у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму.

28. Надавач запроваджує управління фізичним доступом до приміщень, в яких розташовані технічні засоби програмно-технічного комплексу, що використовується для надання довірчих послуг, з дотриманням вимог Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України № 243 від 04.07.2007 та зареєстрованих в Міністерстві юстиції України 17.08.2007 за № 955/14222 (зі змінами).
Засоби кваліфікованого електронного підпису чи печатки, в яких

зберігаються та використовуються особисті ключі надавача, повинні розташовуватися у приміщеннях, що відповідають вимогам Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України № 243 від 04.07.2007 та зареєстрованих в Міністерстві юстиції України 17.08.2007 за № 955/14222 (зі змінами).

Засоби кваліфікованого електронного підпису чи печатки/носії ключової інформації, в яких зберігаються резервні копії особистих ключів надавача, повинні зберігатися із забезпеченням їх захисту від несанкціонованого доступу.

29. Генерація, зберігання, використання особистих ключів надавача здійснюється виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

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

Після закінчення строку дії сертифіката відкритого ключа надавача особистий ключ надавача та всі його резервні копії знищуються способом, що унеможливлюють їх відновлення.

30. Надавач несе відповідальність у сфері електронних довірчих послуг відповідно до статті 36 Закону України “Про електронні довірчі послуги”.

Керівник, заступник керівника, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор несуть відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані клієнтів, згідно із законодавством України.

Надавач повинен встановити відповідальність за недотримання 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.

Права та обов’язки, відповідальність, а також необхідні професійні знання, досвід і кваліфікація керівника, заступника керівника, адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки визначаються у посадових інструкціях працівників надавача.

31. Надавач зобов’язаний забезпечити ведення журналів аудиту подій в інформаційно-телекомунікаційній системі надавача.

Надавач зобов’язаний забезпечити захист журналів аудиту подій від неавторизованого перегляду, від несанкціонованої модифікації, від знищення.

Надавач зобов’язаний визначити які саме журнали аудиту подій мають право переглядати керівник надавача, заступник(и) керівника надавача, адміністратор(и) реєстрації, адміністратор(и) сертифікації, системний(і) адміністратор(и), адміністратор(и) безпеки та частоту перегляду для кожного із журналів аудиту подій.

Під час перегляду журналів аудиту подій вивчаються зафіксовані події та перевіряється наявність несанкціонованої модифікації.

32. Надавач зобов’язаний забезпечити резервне копіювання журналів аудиту подій, сертифікатів відкритих ключів, списків відкликаних сертифікатів.

Резервні копії журналів аудиту подій, сертифікатів відкритих ключів, списків відкликаних сертифікатів повинні зберігатися в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

33. Надавач зобов’язаний забезпечити зберігання журналів аудиту подій протягом 5 років, після чого забезпечує їх передачу на архівне зберігання.

34. У журналах аудиту подій повинні реєструватися події таких типів:

спроби створення, знищення, встановлення паролів, зміни прав доступу в інформаційно-телекомунікаційній системі;

заміни програмного забезпечення, технічних засобів інформаційно-телекомунікаційної системи;

технічне обслуговування інформаційно-телекомунікаційної системи;

генерація, використання, знищення особистих ключів надавача;

формування, блокування, скасування та поновлення сертифікатів відкритих ключів, формування списків відкликаних сертифікатів відкритих ключів;

спроби несанкціонованого доступу до інформаційно-телекомунікаційної системи;

надання доступу персоналу до інформаційно-телекомунікаційної системи;

збої в роботі інформаційно-телекомунікаційної системи;

інші події, необхідні для збору доказів.

Усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час події, а також ідентифікувати суб’єкта, що здійснив або ініціював подію.

35. Час, що використовується в інформаційно-телекомунікаційній системі надавача, в тому числі у журналах аудиту подій в електронній формі, повинен бути синхронізований із Всесвітнім координованим часом з точністю до секунди.

36. Записи подій у журналах аудиту подій в паперовій формі повинні бути підписані адміністратором безпеки.

37. Надавач обліковує та зберігає протягом строків, визначених

законодавством у сфері архівної справи, договори про надання кваліфікованих електронних довірчих послуг, а також документи (засвідчені в установленому порядку копії документів), що використовуються під час ідентифікації та верифікації клієнта.

Знищення архівних документів має здійснюватися комісією, до складу якої входять керівник надавача/заступник керівника надавача, адміністратор сертифікації, адміністратор безпеки. Після завершення процедури знищення архівних документів складається відповідний акт, який затверджує керівник надавача/заступник керівника надавача.

38. Генерацію особистих та відкритих ключів надавача здійснює адміністратор сертифікації у присутності адміністратора безпеки.

Генерація особистих та відкритих ключів клієнта може здійснюватися на території надавача або на території клієнта.

39. Надавач зобов'язаний здійснювати свою діяльність відповідно до вимог законодавства у сфері електронних довірчих послуг та регламенту роботи надавача, який визначає організаційні, технічні та інші умови діяльності надавача. Регламент роботи надавача розробляється відповідно до цих Вимог та вимог законодавства України в сфері електронних довірчих послуг.

Надавач самостійно визначає обсяг положень регламенту роботи, що розміщуються на веб-сайті надавача для ознайомлення.

40. Регламент роботи надавача повинен містити:

1) загальні відомості про надавача (найменування надавача; код за Єдиним державним реєстром підприємств та організацій України; місцезнаходження, номери телефонів, електронна адреса веб-сайту, режим роботи надавача);

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

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

4) опис функцій адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки;

5) політику сертифіката;

6) положення сертифікаційних практик;

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

41. У політиці сертифіката визначається кожна кваліфікована електронна довірча послуга, що передбачає формування та обслуговування надавачем кваліфікованих сертифікатів відкритих ключів, окремо або у сукупності. У політиці сертифіката визначаються:

1) перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем;

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

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

4) механізм підтвердження володіння клієнтом особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа;

5) умови ідентифікації та верифікації клієнта (документи, які клієнт повинен надати для отримання довірчих послуг, вимоги щодо особистої присутності клієнта);

6) механізм автентифікації клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем;

7) механізм автентифікації клієнтів під час обробки заяв на блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа;

8) опис фізичного середовища (опис приміщень надавача, в яких розміщена інформаційно-телекомунікаційна система надавача, механізми контролю доступу до них);

9) процедурний контроль (система дисциплінарних стягнень за недотримання працівниками надавача своїх 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);

10) порядок ведення журналів аудиту подій;

11) порядок ведення архівів надавача (із зазначенням видів документів та даних, що підлягають архівуванню, строків зберігання архівів, механізму та

порядку зберігання і захисту архівів);

12) порядок та умови генерації, зберігання, використання пар ключів надавача;

13) порядок та умови резервного копіювання особистого ключа надавача, збереження, доступу та використання резервних копій.

14) порядок та умови генерації пар ключів клієнтів.

Механізм отримання клієнтом особистого ключа в результаті надання кваліфікованої електронної довірчої послуги надавачем.

Механізм надання клієнтом запиту на формування кваліфікованого сертифіката відкритого ключа надавачу для формування кваліфікованого сертифіката відкритого ключа;

42. У положенні сертифікаційних практик визначаються практичні та процедурні засади реалізації всіх політик сертифіката у сукупності. У положеннях сертифікаційних практик зазначаються:

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

2) порядок надання сформованого кваліфікованого сертифіката відкритого ключа клієнту;

3) порядок та умови публікації сформованого кваліфікованого сертифіката відкритого ключа клієнта на веб-сайті надавача;

4) умови використання кваліфікованого сертифіката відкритого ключа клієнта 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 клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем;

6) порядок та умови блокування, поновлення, скасування кваліфікованих сертифікатів відкритих ключів клієнтів:

перелік суб'єктів, уповноважених подавати запити на блокування, поновлення, скасування кваліфікованих сертифікатів відкритих ключів клієнтів;

процедура подання запитів на блокування, поновлення, скасування кваліфікованих сертифікатів відкритих ключів клієнтів;

час оброблення запитів на блокування, поновлення, скасування кваліфікованих сертифікатів відкритих ключів клієнтів;

7) порядок та умови надання інформації про статус кваліфікованих сертифікатів відкритих ключів, сформованих надавачем:

частота формування списку відкликаних сертифікатів та строки його дії;

можливість та умови надання інформації про статус кваліфікованого сертифіката відкритого ключа у режимі реального часу;

8) строки чинності кваліфікованих сертифікатів відкритих ключів, сформованих надавачем.

43. Надавач зобов’язаний щороку до 15 січня подавати до засвідчувального центру звіт про діяльність за попередній рік. Форма звіту встановлюється у регламенті роботи засвідчувального центру.

44. Надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг з дотриманням вимог статті 31 Закону України “Про електронні довірчі послуги”.

Директор
Департаменту безпеки Олександр СКОМАРОВСЬКИЙ