monobank | Universal Bank

ПОГОДЖЕНО

ЗАТВЕРДЖЕНО

ПОЛІТИКА СЕРТИФІКАТІВ ТА ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ «УНІВЕРСАЛ БАНК»

Дата	Версія	Опис змін
__ вересня 2024р	1.0	Перша редакція

Зміст

1. ВСТУП

1.1. Огляд

Ця Політика сертифікатів та Положення сертифікаційних практик визначає перелік усіх правил, які застосовує кваліфікований надавач електронних довірчих послуг monobank | Universal Bank АТ "УНІВЕРСАЛ БАНК" (далі – Надавач) у процесі реєстрації користувачів електронних довірчих послуг, зокрема підписантів та створювачів електронних печаток (далі – користувачів) формування та супровід кваліфікованих сертифікатів відкритих ключів (далі – кваліфіковані сертифікати) Надавача та користувачів, зокрема управління їх статусом (блокування, поновлення та скасування).

Політика сертифікатів та Положення сертифікаційних практик є більш розширеною редакцією розділів 6 та 7 Регламенту роботи Надавача, погодженого керівником Засвідчувального центру та затвердженого Головою Правління АТ «УНІВЕРСАЛ БАНК» з метою більш детального опису політики та процедур у відповідності до вимог державних стандартів України та RFC 3647.

Дотримання вимог, зазначених у цій Політиці сертифікатів та Положенні сертифікаційних практик, є обов'язковим для керівника Надавача та його працівників, що є структурним підрозділом АТ «УНІВЕРСАЛ БАНК». Посадові обов'язки працівників Надавача (далі – персонал) безпосередньо пов'язані з реєстрацією користувачів, формуванням та підтримкою їх кваліфікованих сертифікатів. Ці обов'язки також стосуються фізичних та юридичних осіб, які на підставі договорів, укладених з Надавачем, прямо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або супроводом їх кваліфікованих сертифікатів, зокрема, відокремленими пунктами реєстрації Надавача.

Визнання користувачами вимог, визначених цією Політикою сертифікатів та Положенням сертифікаційних практик, є обов'язковою умовою та підставою для укладення з ними договору про надання кваліфікованих електронних довірчих послуг.

Ця Політика сертифікатів відповідає вимогам, визначеним у:

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), IDT) «Електронні підписи та інфраструктури (ESI); Політика та вимоги безпеки для постачальників довірчих послуг, які видають сертифікати; Частина 1: Загальні вимоги», затвердженого наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185 (далі – ДСТУ ETSI EN 319 411-1:2022);

ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), IDT) «Електронні підписи та інфраструктури (ESI); Політика та вимоги безпеки для постачальників довірчих послуг, які видають сертифікати; Частина 2: Вимоги до постачальників довірчих послуг, які видають кваліфіковані сертифікати ЄС», затвердженого наказом державного підприємства «Український науково-дослідний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185 (далі – ДСТУ ETSI EN 319 411). -2:2022).

1.2. Найменування та ідентифікація документа

Див. пункт 5.3 ДСТУ ETSI EN 319 411-1:2022 та ДСТУ ETSI EN 319 411-2:2022.

Повна назва цього документа: Політика сертифікатів та Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ "УНІВЕРСАЛ БАНК".

Скорочена назва цього документа: QTSP-CP/CPS.

Версія: 1.0.

Ідентифікатор об’єкта (OID) цієї Політики сертифікатів та Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ "УНІВЕРСАЛ БАНК" .призначається відповідно до стандартів ITU X 660, ASN.1.

Ідентифікатор об’єкта (OID) цієї Політики сертифікатів та Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ "УНІВЕРСАЛ БАНК":

1.3.6.1.4.1.54069.2.2.1.1

Додаткову інформацію наведено в розділі 7 цієї Політики сертифікатів та Положення сертифікаційних практик.

1.3. Учасники PKI

Учасниками інфраструктури відкритих ключів з якими співпрацює Надавач є:

Надавач, який надає кваліфіковані електронні довірчі послуги у складі відокремлених підрозділів АТ “Універсал банк” та реєстраційні органи представлені окремими відокремленими пунктами Надавача, які є фізичними та юридичними особами, які на підставі договірних зобов’язань з Надавачем здійснюють процедури реєстрації користувачів.

Засвідчувальний центр. Засвідчувальний центр створено для внесення кваліфікованих надавачів електронних довірчих послуг (банків та інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг) до Довірчого списку відповідно до вимог Закону України “Про електронну ідентифікацію та електронні довірчі послуги”. Засвідчувальний центр надає кваліфікованим надавачам електронних довірчих послуг, внесеним до Довірчого списку за його поданням, кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки та подає їх до Довірчого списку.

Центральний засвідчувальний орган (далі – ЦЗО) веде національний Довірчий список.

Субєкти, Підписувачі, Клієнти (користувачі) Надавача у цьому документі Суб'єкт (суб’єкти - це те саме, що й Підписник (підписувачі).

Підписник фізична особа, якій видаються сертифікати.

Для цілей цього документа права та обов'язки Суб’єкта (суб’єктів) та Підписника (підписувачів) має виключно Клієнт.

Клієнти (Суб’єкти, Підписувачі) Надавача отримують від нього кваліфіковані електронні довірчі послуги на умовах Договору. Клієнтами можуть бути, як клієнти АТ "УНІВЕРСАЛ БАНК", співробітники АТ "УНІВЕРСАЛ БАНК" так і інші фізичні та юридичні особи, що звернулися до Надавача з метою отримання його послуг та уклали Договір про надання кваліфікованих електронних довірчих послуг.

Інші учасники, зокрема:

Органи оцінки відповідності[1], акредитовані на проведення сертифікації засобів кваліфікованого електронного підпису чи печатки, формують, підтримують в актуальному стані та публікують на своїх офіційних веб-сайтах переліки сертифікованих ними засобів кваліфікованого електронного підпису чи печатки.

Органи оцінки відповідності вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, які вони надають, з урахуванням:

[1] Перелік засобів кваліфікованого електронного підпису та печатки, відповідність вимогам яких підтверджена у рамках державної експертизи у сфері криптографічного та технічного захисту інформації, доступний на сайті Адміністрації Держспецзв’язку Перелік засобів криптографічного захисту інформації, які мають експертний висновок за результатами державної експертизи у галузі КЗІ (cip.gov.ua)

вимог законодавства щодо порядку надання і використання кваліфікованих електронних довірчих послуг, вимог законодавства у сфері захисту інформації;

вимог, встановлених Національним банком України у разі надання довірчих послуг у банківській системі України та на ринках небанківських фінансових послуг, а також при наданні платіжних послуг;

національних та міжнародних стандартів у сфері довірчих послуг.

Міністерство цифрової трансформації України - головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах електронної ідентифікації та електронних довірчих послуг.

Контролюючий орган, функції якого покладено на Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, здійснює заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг.

Розробники та постачальники засобів кваліфікованого електронного підпису чи печатки (розробники – здійснюють розробку та/або супровід апаратно-програмних пристроїв чи програмного забезпечення, що використовуються для надання кваліфікованих електронних довірчих послуг, створення електронного підпису чи печатки).

1.3.1. Надавач

Надавач є кваліфікованим надавачем електронних довірчих послуг, який надає кваліфіковані електронні довірчі послуги відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги», здійснює реєстрацію користувачів, формування та підтримку їх кваліфікованих сертифікатів, у тому числі управління їх статусом (блокування, поновлення та скасування).

Надавач здійснює реєстрацію користувачів самостійно та/або через віддалені пункти реєстрації Надавача.

1.3.1.1. Права Надавача

Надавач має право:

- надавати кваліфіковані електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг;
- отримувати документи та/або електронні дані, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті;
- отримувати в електронній формі, за допомогою мобільного застосунку monobank, заяви на отримання послуг від користувачів;
- отримувати за допомогою мобільного застосунку monobank електронні копії документів та фотозображення користувачів, які подали запит на отримання послуг;
- на основі отриманих від мобільного застосунку monobank інформації та завірених документів формувати кваліфіковані сертифікати користувачів.
- під час формування та видачі кваліфікованих сертифікатів перевіряти інформацію про осіб, яким видано такі сертифікати, з використанням інформаційних ресурсів ЄІС МВС (відомості, що містяться в ЄДР), а також інформацію з інших публічних електронних реєстрів згідно з Закону України «Про публічні електронні реєстри», отримані в процесі електронної взаємодії з використанням інтегрованої системи електронної ідентифікації (https://id.gov.ua/);
- отримувати консультації від центрального засвідчувального органу, контролюючого органу або засвідчувального центру з питань, пов'язаних з наданням електронних довірчих послуг;
- звертатися до органів з оцінки відповідності для отримання документів про відповідність;
- звертатися до Засвідчувального центру із заявами про формування кваліфікованих сертифікатів відкритих ключів, їх скасування, блокування або поновлення;

– самостійно обирати в рамках кожної послуги, які стандарти використовуватимуться для надання кваліфікованих електронних довірчих послуг, із переліку стандартів, визначеного Кабінетом Міністрів України.

1.3.1.2. Обов'язки Надавача

Надавач зобов'язаний забезпечити:

– надання користувачам всієї необхідної інформації щодо отримання та використання послуг;
– захист персональних даних користувачів відповідно до вимог Закону України «Про захист персональних даних»;
– функціонування програмно-технічного комплексу, що використовується для надання електронних довірчих послуг, та захисту інформації, що в них обробляється, відповідно до вимог законодавства у сфері електронних довірчих послуг;
– створення та функціонування веб-сайту Надавача;
– впровадження, супровід та оприлюднення на веб-сайті Надавача інформації з реєстру діючих, заблокованих та скасованих сертифікатів відкритих ключів;
– можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про стан кваліфікованих сертифікатів через мережі зв'язку загального користування;
– цілодобовий прийом та перевірку заяв користувачів в електронній формі на скасування їх кваліфікованих сертифікатів;
– прийом та перевірку заяв користувачів у паперовій формі на скасування, блокування та поновлення їх кваліфікованих сертифікатів протягом одного робочого дня з моменту надходження заяви та відповідно до режиму роботи Надавача;
– скасування, блокування та поновлення дії кваліфікованих сертифікатів відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги»;
– встановлення, під час формування кваліфікованого сертифіката, власності відкритого ключа та відповідного йому особистого ключа користувачеві;
– внесення даних користувача до відповідного кваліфікованого сертифіката;
– здійснення організаційно-технічних заходів щодо управління ризиками, пов'язаними з безпекою електронних довірчих послуг;
– інформування керівництва АТ «УНІВЕРСАЛ БАНК» та, у разі потреби, органу захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливає на надання електронних довірчих послуг або стосується персональних даних користувачів, без необґрунтованої затримки не пізніше ніж протягом 24 годин з моменту момент, коли їм стало відомо про таке порушення;
– інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливає на надання їм електронних довірчих послуг або стосується їх персональних даних, невідкладно, але не пізніше двох годин з моменту, коли стало відомо про таке порушення;
– постійне зберігання всіх сформованих кваліфікованих сертифікатів;
– постійне зберігання документів та електронних даних, отриманих у зв'язку з наданням електронних довірчих послуг;
– внесення коштів на поточний рахунок із спеціальним режимом використання в установі банку (рахунок у Національному банку України - для банків - кваліфікованих надавачів електронних довірчих послуг, кваліфікованого надавача електронних довірчих послуг, створеного Національним банком України) для відшкодування шкоди, яка може бути завдана користувачам або третім особам внаслідок неналежного виконання Надавачем своїх зобов'язань, або страхування відповідальності для забезпечення відшкодування такої шкоди в розмірі, визначеному Законом України "Про електронну ідентифікацію та електронні довірчі послуги";
– відновлення суми внеску на поточному рахунку зі спеціальним режимом використання на рахунку у Національному банку України - для банків - кваліфікованих надавачів електронних

довірчих послуг, кваліфікованого надавача електронних довірчих послуг, створеного Національним банком України або розміру страхової суми, визначеної Законом України " Про електронну ідентифікацію та електронні довірчі послуги» протягом трьох місяців у разі зміни розміру мінімальної заробітної плати або у разі відшкодування збитків, завданих користувачам або третім особам внаслідок неналежного виконання ними своїх обов'язків;

- використання під час надання кваліфікованих електронних довірчих послуг виключно кваліфікованих сертифікатів, сформованих Засвідчувальним центром;
- наймання працівників і, за необхідності, виконання робіт субпідрядними організаціями, які мають необхідні знання, досвід і кваліфікацію для надання електронних довірчих послуг, а також застосування адміністративних та управлінських процедур, які відповідають національним або міжнародним стандартам;
- чітке та вичерпне повідомлення будь-якої особи, яка звернулася за електронною довірчою послугою, про умови використання такої послуги, у тому числі про будь-які обмеження щодо її використання, до укладення договору про надання електронних довірчих послуг;
- інформування Засвідчувального центру та Контролюючого органу про намір припинити свою діяльність та про зміни у наданні кваліфікованих електронних довірчих послуг протягом 48 годин з моменту таких змін;
- передачу документованої інформації Засвідчувальному центру або іншому кваліфікованому надавачу електронних довірчих послуг у разі припинення діяльності з надання кваліфікованих електронних довірчих послуг;
- приєднання до програмного інтерфейсу ЦЗО з метою забезпечення взаємодії, дослідження поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень.

1.3.2. Органи реєстрації

Реєстраційні органи Надавача можуть бути представлені окремими відокремленими пунктами реєстрації Надавача, які є фізичними або юридичними особами, які на підставі договірних зобов'язань з Надавачем здійснюють процедури реєстрації користувачів.

До працівників відокремлених пунктів реєстрації Надавача, відповідальних за реєстрацію користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації, визначених п. 5.2.1.2 цієї Політики сертифікатів та Положень сертифікаційних практик.

Відповідно до цієї Політики сертифікатів та Положень сертифікаційних практик реєстрація користувачів може здійснюватися Надавачем віддалено, без їх особистої присутності в приміщенні Надавача або у відокремленому пункті реєстрації Надавача з використанням мобільного застосунку monobank.

1.3.3. Клієнти (користувачі) Надавача

Користувачами є Клієнти, а саме підписувачі та створювачі електронних печаток, що пройшли реєстрацію (самостійно або через відокремлені пункти реєстрації Надавача) та яким Надавачем здійснюється формування та підтримка їх кваліфікованих сертифікатів.

Відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги»:

- підписувач – фізична особа, яка створює електронний підпис;
- створювач електронної печатки – юридична особа або фізична особа – підприємець, яка створює електронну печатку.

1.3.3.1. Права користувачів

Користувачі мають право:

- отримання електронних довірчих послуг;
- вільного вибору кваліфікованого надавача електронних довірчих послуг;
- оскарження в судовому порядку дій чи бездіяльності Надавача та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг;
- відшкодування завданої їм шкоди та захист їхніх прав і законних інтересів;
- подавати заяву про скасування, блокування та поновлення їх кваліфікованого сертифіката.

1.3.3.2. Обов'язки користувачів

Користувачі зобов'язані:

- забезпечувати конфіденційність і неможливість доступу інших осіб до особистого ключа;
- негайно повідомляти Надавача про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату електронних довірчих послуг, якщо така оплата передбачена договором про надання кваліфікованих електронних довірчих послуг, укладеним з Надавачем;
- своєчасно надавати Надавачу інформацію про зміну ідентифікаційних даних, що містяться у кваліфікованому сертифікаті;
- не використовувати особистий ключ у разі його зламу, а також у разі скасування чи призупинення дії кваліфікованого сертифіката.

1.3.4. Довіряючі сторони

Довіряючі сторони – це фізичні та/або юридичні особи, а також їх інформаційно-комунікаційні системи, які використовують кваліфіковані сертифікати користувачів з метою їх автентифікації або з метою перевірки та підтвердження електронного підпису чи печатки.

1.3.5. Інші учасники

Іншими учасниками є фізичні та/або юридичні особи, які прямо чи опосередковано пов’язані з формуванням та/або підтримкою кваліфікованих сертифікатів Надавача та користувачів.

До інших учасників також відносяться Засвідчувальний центр, Контролюючий орган та Міністерство цифрової трансформації України.

Засвідчувальний центр:

- формує кваліфіковані сертифікати Надавача з використанням самопідписаного сертифіката електронної печатки Засвідчувального центру;
- погоджує Регламент роботи Надавача та зміни до нього
- погоджує порядок синхронізації часу з Всесвітнім координованим часом (UTC) Надавача;
- погоджує план припинення діяльності Надавача.

Адміністрація Державної служби спеціального зв’язку та захисту інформації України є Контролюючим органом, яка, зокрема:

- здійснює державний контроль за дотриманням вимог законодавства про електронні довірчі послуги;

- взаємодіє з Засвідчувальним центром та Центральним засвідчувальним органом з питань державного контролю за дотриманням вимог законодавства;
- взаємодіє з органами влади з питань захисту персональних даних шляхом негайного інформування про порушення вимог законодавства про захист персональних даних, виявлені під час перевірок Надавача;
- інформує громадськість у разі отримання від Надавача або за результатами його перевірки інформації про порушення конфіденційності та/або цілісності інформації, що впливає на надання електронних довірчих послуг або стосується персональних даних користувачів;
- видає приписи щодо усунення порушень вимог законодавства щодо електронних довірчих послуг;
- накладає адміністративні штрафи за порушення вимог законодавства щодо електронних довірчих послуг;
- аналізує документи за результатами проведення процедур оцінки відповідності Надавача у рамках заходів невиїзного державного нагляду (контролю).

Міністерство цифрової трансформації України, а саме Центральний засвідчувальний орган впроваджує, підтримує в актуальному стані та публікує на своєму офіційному веб-сайті Довірчий список, в якому міститься інформація про кваліфікованих надавачів електронних довірчих послуг разом з інформацією про кваліфіковані електронні довірчі послуги, які вони надають.

Розробники та постачальники засобів кваліфікованого електронного підпису чи печатки (розробники – здійснюють розробку та/або супровід апаратно-програмних пристроїв чи програмного забезпечення, що використовуються для надання кваліфікованих електронних довірчих послуг, створення електронного підпису чи печатки).

1.4. Використання сертифіката

Див. пункт 5.5 ДСТУ ETSI EN 319 411-1:2022 та ДСТУ ETSI EN 319 411-2:2022.

1.4.1. Належне використання сертифіката

1.4.1.1. Види кваліфікованих сертифікатів

Надавач формує кваліфіковані сертифікати наступних типів:

1) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем кваліфікованого електронного підпису фізичної особи та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірку та підтвердження кваліфікованого електронного підпису;

2) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем кваліфікованого електронного підпису фізичної особи, що представляє юридичну особу та підтверджує її ідентифікаційні дані під час автентифікації, дані юридичної особи та зв'язок між ними, а також створення, перевірку та підтвердження кваліфікованого електронного підпису;

3) кваліфікований сертифікат електронної печатки, який асоціюється з відкритим ключем кваліфікованої електронної печатки юридичної особи або фізичної особи – підприємця та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованої електронної печатки;

4) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем удосконаленого електронного підпису фізичної особи та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірку та підтвердження удосконаленого електронного підпису;

5) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем удосконаленого електронного підпису фізичної особи, що представляє юридичну особу та підтверджує її

ідентифікаційні дані під час автентифікації, дані юридичної особи та зв'язок між ними, а також створення, перевірку та підтвердження удосконаленого електронного підпису;

6) кваліфікований сертифікат електронної печатки, який асоціюється з відкритим ключем удосконаленої електронної печатки юридичної особи або фізичної особи – підприємця та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження удосконаленої електронної печатки;

7) кваліфікованого сертифіката шифрування, який асоціюється з відкритим ключем фізичної особи, відповідний якому особистий ключ знаходиться в засобі КЕП та використовується для спрямованого шифрування під час обміну інформацією;

8) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи, що представляє юридичну особу, відповідний якому особистий ключ знаходиться в засобі КЕП, та використовується для спрямованого шифрування під час обміну інформацією;

9) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем печатки юридичної особи або фізичної особи – підприємця, відповідний якому особистий ключ знаходиться в засобі КЕП та використовується для спрямованого шифрування під час обміну інформацією;

10) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи та використовується для спрямованого шифрування під час обміну інформацією;

11) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи, що представляє юридичну особу та використовується для спрямованого шифрування під час обміну інформацією;

12) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем печатки юридичної особи або фізичної особи – підприємця та використовується для спрямованого шифрування під час обміну інформацією;

Відповідно до цієї Політики сертифікатів та Положення сертифікаційних практик Надавач формує кваліфікований сертифікат користувача, що використовує мобільний застосунок monobank та пов'язує відкритий ключ кваліфікованого електронного підпису з фізичною особою та підтверджує її ідентифікаційні дані під час автентифікації в застосунку, а також створення, перевірки та підтвердження кваліфікованого електронного підпису.

1.4.1.2. Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати Надавача формуються Засвідчувальним центром та/або ЦЗО на строк дії не більше 5 років.

Кваліфіковані сертифікати користувачів формуються Надавачем зі строком дії 1 або 2 роки.

Кваліфіковані сертифікати повинні містити інформацію про початок і кінець строку їх дії.

1.4.2. Заборони щодо використання сертифіката

Кваліфікований сертифікат дозволяється використовувати лише відповідно до призначення відкритого ключа («keyUsage»), зазначеного в ньому.

1.4.3. Використання тестових сертифікатів

Формування тестових сертифікатів здійснюється Надавачем шляхом інтеграції з тестовим програмно-технічним комплексом, який функціонує на офіційному веб-сайті ЦЗО у складі інструменту моніторингу у сфері електронних довірчих послуг в Україні.

1.5. Керування Політикою сертифікатів та Положенням сертифікаційних практик

1.5.1. Відповідальність за Політику сертифікатів та Положення сертифікаційних практик

Ця Політика сертифікатів та Положення сертифікаційних практик підтримується Надавачем.

Надавач внесений до Довірчого списку за поданням Засвідчувального центру.

Головний офіс Надавача представлений функціональним підрозділом АТ «УНІВЕРСАЛ БАНК», який організовує надання кваліфікованих електронних довірчих послуг Надавача та відокремленими пунктами реєстрації Надавача та забезпечує виконання вимог законодавства України.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені АТ «УНІВЕРСАЛ БАНК».

Надавач: АКЦІОНЕРНЕ ТОВАРИСТВО «УНІВЕРСАЛ БАНК»,

Юридична адреса: 04082, Україна, м. Київ, вул. Автозаводська, 54/19.

Код ЄДРПОУ: 21133352

ІПН: 211333513023

Адреса електронної пошти головного офісу Надавача: ca@universalbank.com.ua

Ця Політика сертифікатів та Положення сертифікаційних практик структурована відповідно до RFC 3647 «Інфраструктура відкритих ключів Інтернету X.509 щодо Політики та практики сертифікації» та містить всю необхідну інформацію.

Ця Політика сертифікатів та Положення сертифікаційних практик, а також зміни до неї підписуються керівником Надавача, який несе відповідальність за дотримання визначених у ній правил, та затверджується Головою Правління АТ «УНІВЕРСАЛ БАНК».

1.5.2. Внесення змін до Політики сертифікатів та Положення сертифікаційних практик

Відповідно до п. 9.12 цієї Політики сертифікатів та Положення сертифікаційних практик.

1.6. Визначення та скорочення

1.6.1. Визначення термінів

У цій Політиці сертифікатів та Положення сертифікаційних практик терміни вживаються у значеннях, наведених у Цивільному кодексі України, Законі України «Про електронну ідентифікацію та електронні довірчі послуги», Положенні про кваліфікованих надавачів електронних довірчих послуг, унесених до Довірчого списку за поданням засвідчувального центру, затвердженому постановою Правління Національного банку України від 19.09.2019 № 116, зі змінами та доповненнями, Вимогах до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28.06.2024 № 764, інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Список скорочень

ООВ	Орган з оцінки відповідності
ЦЗО	Центральний засвідчувальний орган (Міністерство цифрової трансформації України)
CMP	Протокол керування сертифікатами
КЗІ	Криптографічний захист інформації
CRL	Список відкликаних сертифікатів
ІКС	Інформаційно-комунікаційна система
НКІ	Носії ключової інформації
ПТК	Програмно-технічний комплекс
OCSP	Онлайн-протокол статусу сертифіката
Контролюючий орган	Контролюючий орган (Адміністрація Держспецзв'язку України)
ДРАЦС	Державний реєстр актів цивільного стану громадян
ДРФОПП	Державний реєстр фізичних осіб - платників податків
TSP	Протокол позначки часу
ЄІС МВС	Єдина інформаційна система МВС України
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців

2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

Див. пункт 6.1 ДСТУ ETSI EN 319 411-1:2022 та ДСТУ ETSI EN 319 411-2:2022.

Надавач публікує умови договору надання електронних довірчих послуг та політику надання електронних довірчих послуг в електронному вигляді на своєму веб-сайті.

Про будь-які зміни в наданні кваліфікованих електронних довірчих послуг, які описані в Регламенті будуть попередньо узгоджені з Засвідчувальним центром, якщо цього вимагає чинне законодавство.

Чинні документи доступні на веб-сайті Надавача як і всі попередні версії документів.

Надавач повідомляє своїх Клієнтів про зміну Політики сертифікатів та Положення сертифікаційних практик шляхом публікації на веб-сайті.

2.1. Репозиторій

Надавач забезпечує:

- створення та функціонування веб-сайту Надавача;
- впровадження, супровід та оприлюднення на веб-сайті Надавача інформації з реєстру діючих, блокованих та скасованих сертифікатів відкритих ключів;
- можливість цілодобового доступу до реєстру діючих, блокованих та скасованих сертифікатів відкритих ключів та до інформації про стан сертифікатів відкритих ключів через мережі зв'язку загального користування.

Надавач також забезпечує інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на веб-сайті Надавача.

Надавач через веб-сайт (https://ca.monobank.ua/) надає безкоштовний доступ до:

- інформації про Надавача;
- даних про внесення відомостей про Надавача до Довірчого списку;
- цієї Політики сертифікатів та Положення сертифікаційних практик Надавача;
- Загальних умови надання кваліфікованих електронних довірчих послуг користувачам Надавача;
- кваліфікованих сертифікатів Надавача;
- переліку кваліфікованих електронних довірчих послуг, що надаються Надавачем;
- даних про засоби створення кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг Надавачем;
- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- інформації про відокремлені пункти реєстрації Надавача та виїзних адміністраторів реєстрації;
- реєстру діючих, блокованих та відкликаних сертифікатів відкритих ключів;
- відомостей про обмеження щодо використання користувачами кваліфікованих сертифікатів;
- даних про порядок перевірки чинності кваліфікованого сертифіката, у тому числі умови перевірки статусу сертифіката;
- переліку законодавчих актів у сфері електронних довірчих послуг.

Ця Політика сертифікатів та Положення сертифікаційних практик доступна 24 години на добу, 7 днів на тиждень у форматі тільки для читання на веб-сайті Надавача.

Надавач забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифікатів та Положення сертифікаційних практик Надавача, списків відкликаних сертифікатів, договорів, законодавчих актів та інших нормативних документів на веб-сайті Надавача.

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

Кваліфіковані сертифікати користувачів, які надали згоду на їх оприлюднення, оприлюднюються на веб-сайті Надавача (https://ca.monobank.ua/) одразу після формування таких сертифікатів.

Згода на публікацію кваліфікованого сертифіката надається користувачем при поданні заявки на формування кваліфікованого сертифіката.

2.2.2. Публікація сертифікатів Надавача

Кваліфіковані сертифікати Надавача публікуються на офіційному веб-сайті одразу після їх отримання від Засвідчувального центру та/або ЦЗО.

Кваліфіковані сертифікати серверів Надавача публікуються відразу після їх формування Надавачем.

Надавач забезпечує доступ до списків відкликаних сертифікатів, здійснює регулярне оновлення інформації та публікацію кваліфікованих сертифікатів Надавача на своєму офіційному веб-сайті: https://ca.monobank.ua/.

2.2.3. Доступ до сертифікатів користувачів

Кваліфіковані сертифікати користувачів після їх формування Надавачем публікуються та доступні користувачеві, для якого створено такі сертифікати, у разі його згоди на їх публікацію.

Надавач забезпечує цілодобовий доступ користувачів до їхніх власних кваліфікованих сертифікатів.

Доступ інших осіб до кваліфікованого сертифіката користувача надається за умови згоди власника сертифіката на його публікацію.

2.2.4. Строк дії сертифікатів

Дата та час початку та закінчення строку дії кваліфікованого сертифіката зазначається у такому кваліфікованому сертифікаті із точністю до однієї секунди.

Кваліфікований сертифікат вважається скасованим після настання дати та часу закінчення строку дії кваліфікованого сертифіката.

Блокований кваліфікований сертифікат автоматично скасовується Надавачем, якщо протягом 30 календарних днів користувач не поновить його чинність.

Строк дії кваліфікованих сертифікатів користувачів – не більше двох років.

Строк дії кваліфікованих сертифікатів Надавача становить не більше п'яти років.

2.3. Час і періодичність публікації

Кваліфіковані сертифікати серверів Надавача публікуються відразу після їх формування Надавачем.

Кваліфіковані сертифікати користувачів, які дали згоду на їх публікацію, оприлюднюються Надавачем одразу після формування таких сертифікатів.

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків, які відповідають таким вимогам:

- у кожному списку відкликаних сертифікатів зазначається граничний строк його дії до видання нового списку;
- новий список відкликаних сертифікатів може бути опубліковано до настання граничного строку його дії до видання наступного списку;
- на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис чи печатка Надавача.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Час зміни статусу кваліфікованих сертифікатів синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів користувачів.

Повний список відкликаних сертифікатів формується та публікується 1 (один) раз на тиждень та містить інформацію про всі відкликані кваліфіковані сертифікати, які були сформовані Надавачем.

Частковий список відкликаних сертифікатів формується та публікується кожні 2 (дві) години та містить інформацію про всі скасовані кваліфіковані сертифікати, статус яких був змінений в інтервалі між часом випуску останнього повного списку відкликаних сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

2.4. Контроль доступу до репозиторію

Репозиторій захищений від несанкціонованих змін. Надавач забезпечує цілодобову роботу власного веб-сайту.

Відповідальність за захист інформації на веб-сайті, в репозиторії та базі даних Надавача несуть відповідальні особи Надавача. Доступ до управління веб-сайтом, репозиторієм та базою даних Надавача надається адміністраторам Надавача. Захист інформації на веб-сайті, в репозиторії та базі даних Надавача здійснюється відповідно до внутрішніх документів з комплексної системи захисту інформації або системи управління інформаційної безпеки (далі – СУІБ).

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

Ідентифікація та автентифікація Клієнтів здійснюється Надавачем відповідно вимог Регламенту роботи кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ "УНІВЕРСАЛ БАНК", що публікується на веб-сайті Надавача у вільному доступі.

Для віддаленої ідентифікації за бажанням Клієнта Банку може бути використано ним (з використанням застосунку monobank) інформацію (далі – схема ідентифікації Bank ID) про нього, отриману Банком на умовах чинних (для Клієнта, а саме підписаних ним) договірних стосунків з Банком (згідно «Умов і правил обслуговування в АТ "УНІВЕРСАЛ БАНК" при наданні банківських послуг щодо продуктів monobank | Universal Bank» (для фізичних осіб) та/або «Моноправил для обслуговування бізнесу в АТ "УНІВЕРСАЛ БАНК"» (для юридичних осіб), що публікується на веб-сайті Банку у вільному доступі).

Порядок ідентифікації автентифікації Клієнтів детально описано в пункті 6.1.6.2. Регламенту роботи кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ "УНІВЕРСАЛ БАНК".

3.1. Позначення

Кваліфіковані сертифікати обов'язково містять інформацію, визначену частиною другою статті 23 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Кваліфіковані сертифікати можуть містити інформацію про обмеження щодо використання кваліфікованого електронного підпису чи печатки.

Кваліфіковані сертифікати можуть містити інші не обов'язкові додаткові спеціальні атрибути, зазначені в стандартах для кваліфікованих сертифікатів. Такі атрибути не повинні впливати на взаємодію та розпізнавання кваліфікованих електронних підписів або печаток.

Інформація, що міститься в кваліфікованих сертифікатах, відповідає позначенням (реквізитам, атрибутам), визначеним у стандартах профілів сертифікатів згідно з п. 7.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

Позначення, які використовуються в кваліфікованих сертифікатах користувачів, перераховані в таблиці 2.

Таблиця 2. Позначення, які використовуються в кваліфікованих сертифікатах користувачів

Найменування	Значення
Країна (C)	Назва країни згідно з ДСТУ ISO 3166-1:2009 «Коди назв країн світу» (ISO 3166-1:2006, IDT), затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 року № 471
Організація (O)	Найменування юридичної особи для кваліфікованого сертифіката юридичної особи або кваліфікованого сертифіката представника юридичної особи. Для кваліфікованих сертифікатів фізичних осіб, які не належать жодній юридичній особі, це поле недоступне
Організаційна одиниця (OU)	Назва підрозділу або відділу в організації. Для кваліфікованих сертифікатів фізичних осіб, які не належать жодній юридичній особі, це поле недоступне
Штат або провінція (S)	Назва провінції або центрального міста, де проживає або має штаб-квартиру користувач
Місцевість (L)	Назва населеного пункту нижчого рівня в провінції/місті, де безпосередньо проживає або знаходиться головний офіс користувача.
Загальна назва (CN)	ПІБ користувача, якому належить кваліфікований сертифікат
Адреса електронної пошти (E)	Адреса електронної пошти користувача, якому належить кваліфікований сертифікат
Назва (T)	Посада (для кваліфікованих довідок представників юридичних осіб у разі необхідності)
Унікальний ідентифікатор (UID)	Ідентифікатор користувача, якому належить кваліфікований сертифікат: для користувачів, які є фізичними особами, для UID використовується код платника податків або номер паспорта; для користувачів, які є приватними підприємцями, для UID використовується ДРФОПП; для користувачів, які є юридичними особами, для UID використовується код за ЄДРПОУ

3.1.1. Типи імен

Типи назв (реквізитів, атрибутів) кваліфікованого сертифіката, що відповідають інформації, що міститься в кваліфікованих сертифікатах, визначені стандартами профілів сертифікатів згідно з п. 7.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

3.1.2 Обов'язкові позначення

Кваліфікований сертифікат має всі необхідні позначення (реквізити, атрибути), визначені в стандартах профілів сертифікатів згідно з п. 7.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

3.1.3. Анонімність або використання псевдонімів

Анонімність не застосовуються.

Використання псевдонімів користувачів застосовується відповідно до законодавства України та Регламенту роботи Надавача.

3.1.4. Правила інтерпретації різних форм імені

Імена кодуються згідно з UTF-8. За необхідності застосовується транслітерація відповідно до Таблиці транслітерації українського алфавіту латиницею, затвердженої постановою Кабінету Міністрів України від 27.01.2010 № 55.

3.1.5. Унікальність імен

Надавач, перед формуванням сертифікату переконується, що сертифікати з однаковими даними, вказаними в полях «Common Name» і «SerialNumber», не видаються різним користувачам.

3.1.6. Визнання, автентифікація та роль торгових марок

Не застосовується.

3.2. Первинна перевірка та ідентифікація

3.2.1. Спосіб підтвердження володіння особистим ключем

Підтвердження права власності користувача на особистий ключ, якому відповідає відкритий ключ для формування кваліфікованого сертифіката, здійснюється одним із таких способів:

- візуальний та технічний контроль запису та передачі до Надавача запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після ідентифікації користувача, за умови його особистої присутності у приміщенні Надавача або його реєстраційних органів;
- технічний контроль запису та передачі до Надавача запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після ідентифікації заявника та отримання ідентифікаційних даних за допомогою ідентифікаційних механізмів, зазначених у підпунктах 3.2.2 пункту 3.2 цієї Політики сертифікатів та Положення сертифікаційних практик.

У всіх випадках за допомогою засобів створення кваліфікованого електронного підпису або печатки Надавача удосконалений електронний підпис, створений за допомогою особистого ключа користувача на запит на формування кваліфікованого сертифіката, перевіряється за допомогою відкритого ключа, що міститься в цьому запиті.

Підтвердження володіння користувачем особистим ключем здійснюється без розкриття особистого ключа.

3.2.2. Ідентифікація особи

Формування та видача кваліфікованого сертифіката без встановлення особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті, не допускається.

Ідентифікація особи, яка звернулася за послугою з формування кваліфікованого сертифіката, здійснюється одним із таких способів, визначених Регламентом роботи Надавача:

1. За особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством України порядку з Єдиного державного демографічного реєстру, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства України про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.
2. Віддалено (без особистої присутності особи), за допомогою додатку встановленого monobank, який оновлено та використовується його остання актуальна версія, відповідно до чинного законодавства України.

Клієнт, що є уповноваженим представником юридичної особи чи фізичної особи – підприємця, може ідентифікувати себе за допомогою мобільного застосунок monobank, якщо виконано наступні умови:

- юридичною чи фізичною особою – підприємцем відкрито рахунок в АТ «УНІВЕРСАЛ БАНК», уповноваженим представником юридичної особи чи фізичною особою – підприємцем;
- право отримання послуги представником юридичної особи чи фізичної особи – підприємця підтверджено уповноваженим представником цієї юридичної особи чи фізичної особи – підприємця.

Достовірність інформації про уповноваженого представника юридичної особи чи фізичної особи – підприємця встановлюється за інформацією з Єдиного державного реєстру підприємств та організацій України та документів, що підтверджують повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця та опрацьовуються (зберігаються) АТ «УНІВЕРСАЛ БАНК» з моменту відкриття рахунку.

3. З використанням інших способів ідентифікації, визначених законом, надійність яких є еквівалентною особистій присутності та підтверджена органом з оцінки відповідності.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи або фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) Надавач використовує інформацію про юридичну особу або фізичну особу - підприємця, що міститься в ЄДР або в комерційному, банківському чи судовому реєстрі, що ведеться країною резиденції іноземної юридичної особи, а також перевірити, чи є обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця достатньо для формування та видачі кваліфікованого сертифіката.

Перевірка цивільної правоздатності та дієздатності міжнародних організацій, відомості про які не внесені до ЄДР чи торговельного, банківського чи судового реєстру, що ведеться іноземною державою, за місцезнаходженням штаб-квартири міжнародної організації здійснюється з використанням інформації з міжнародного договору чи іншого офіційного документа, на підставі якого створена та/або діє міжнародна організація.

Надавач залишає за собою право підтримувати лише ті способи електронної ідентифікації та автентифікації, які має можливість забезпечити, із одночасним інформуванням користувачів про це на веб-сайті Надавача.

3.2.3. Неперевірена інформація про користувача

Використання неперевіреної інформації про користувача не допускається.

3.2.4. Підтвердження повноважень

Уповноважений представник юридичної особи або фізичної особи - підприємця підписує документи, необхідні для оформлення та видачі працівнику юридичної особи або фізичної особи – підприємця кваліфікованого сертифіката. Надавач під час формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи – підприємця здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи. Юридична особа або фізична особа – підприємець здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи – підприємця відповідно до вимог, встановлених підпунктом 3.2.2 цієї Політики сертифікатів та Положення сертифікаційних практик та перевіряє обсяг його повноважень згідно з документом, що визначає повноваження уповноваженого представника юридичної особи чи фізичної особи – підприємця, або з використанням відомостей, що містяться в ЄДР чи в комерційних, банківських чи судових реєстрах, які веде країна резидентства іноземної юридичної особи.

Уповноваженим представником юридичної особи є керівник юридичної особи, який зазначений в ЄДР, або працівник (керівник відокремленого підрозділу (філії) юридичної особи), який має повноваження на вчинення правочинів з третіми особами, зазначеними в ЄДР (наказ, довіреність тощо).

Перед формуванням кваліфікованого сертифіката представника юридичної особи та/або самозайнятої особи (адвоката, нотаріуса, приватного виконавця, арбітражного керуючого тощо) також перевіряються повноваження користувача шляхом перевірки документів, що посвідчують його повноваження або належність до юридичної особи, право на здійснення діяльності у визначеній сфері (довідка, наказ про призначення тощо) або шляхом перевірки інформації у відповідних державних інформаційних системах (реєстри, бази даних тощо).

3.3. Ідентифікація та автентифікація користувача для запитів на заміну сертифікатів

3.3.1. Ідентифікація та автентифікація користувача за заявкою на формування сертифіката за умови дійсності попереднього сертифіката

Не застосовується.

3.3.2. Ідентифікація та автентифікація користувача для отримання нового сертифіката в разі скасування сертифіката

У разі скасування кваліфікованого сертифіката користувача, для формування нового кваліфікованого сертифіката у Надавача, користувач повинен пройти ідентифікацію та автентифікацію відповідно до умов первинної ідентифікації та автентифікації користувача.

3.4. Ідентифікація та автентифікація користувача для запитів на блокування або скасування сертифіката

Користувач може подати заяву на блокування або скасування кваліфікованого сертифіката:

шляхом особистого звернення до Надавача або його відокремленого пункту реєстрації з заявою на блокування або скасування сертифіката в паперовому вигляді;

на скасування з використанням мобільного додатку monobank;

на блокування шляхом звернення до Надавача за допомогою засобів телефонного зв’язку за номерами телефонів, вказаних на веб-сайті Надавача.

4. ВИМОГИ ЩОДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

4.1. Запит на формування сертифіката

До переліку суб'єктів, уповноважених подавати запит на формування кваліфікованого сертифіката, входять користувачі, які пройшли процедури ідентифікації та автентифікації.

Запит на формування кваліфікованого сертифіката приймається до обробки після оформлення заявки на формування кваліфікованого сертифіката, ідентифікації та автентифікації особи користувача та підтвердження володіння користувачем особистим ключем, якому відповідає відкритий ключ для формування кваліфікованого сертифіката.

4.2. Обробка запиту на формування сертифіката

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмним забезпеченням Надавача за участю адміністратора сертифікації, працівника відокремленого пункту реєстрації Надавача, відповідального за реєстрацію користувача та який виконує функції адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх для обробки захищеними каналами зв'язку, що забезпечують конфіденційність та цілісність даних. Автоматична обробка запитів не виключає процесів ідентифікації особи користувача та підтвердження права власності користувача на особистий ключ, відповідно до якого надається відкритий ключ для формування кваліфікованого сертифіката.

Під час обробки запиту на формування кваліфікованого сертифіката засобами Надавача перевіряється унікальність відкритого ключа в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів та унікальність серійного номера кваліфікованого сертифіката користувача.

Термін обробки запиту на формування кваліфікованого сертифіката, поданого разом із заявою про реєстрацію, становить не більше однієї години.

4.3. Видача сертифіката

Надання сформованого кваліфікованого сертифіката користувачеві здійснюється одним із таких способів:

- шляхом надсилання файлу зі сформованим кваліфікованим сертифікатом на адресу електронної пошти, вказану користувачем у заявці на формування кваліфікованого сертифіката;
- шляхом запису файлу зі сформованим кваліфікованим сертифікатом на носій даних, наданий користувачем;
- шляхом оприлюднення сформованого кваліфікованого сертифіката на офіційному веб-сайті Надавача.

4.4. Прийняття сертифіката

Кваліфікований сертифікат користувача публікується на веб-сайті Надавача https://ca.monobank.ua/ відразу після його формування Надавачем за результатом обробки запиту на сертифікат.

Протягом 24 годин користувач повинен перевірити свої ідентифікаційні дані, внесені до кваліфікованого сертифіката Надавачем. Надавач, за необхідності, надає відповідні консультації щодо проведення такої перевірки. Користувач повинен використовувати особистий ключ для створення кваліфікованого електронного підпису лише після перевірки. Використання особистого ключа користувачем є фактом визнання ним кваліфікованого сертифіката, що відповідає його відкритому ключу.

Користувач може перевірити ідентифікаційні дані, внесені в кваліфікований сертифікат, ознайомившись із власним сертифікатом на веб-сайті Надавача, в додатку monobank (якщо він

використовувався для отримання послуги) або за допомогою спеціалізованого програмного забезпечення, доступного на веб-сайті Надавача: https://ca.monobank.ua/.

Якщо користувач протягом доби виявить невідповідність ідентифікаційних даних, введених Надавачем у кваліфікований сертифікат, користувач повинен звернутися до Надавача для скасування кваліфікованого сертифіката та формування нового сертифіката.

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката та виявлених Надавачем до моменту видачі користувачу сформованого кваліфікованого сертифіката, посадова особа Надавача проводить переформування кваліфікованого сертифіката з використанням попередньо сертифікованого відкритого ключа та з дотриманням вимог щодо запобігання перевищенню терміну дії особистого ключа та відповідного відкритого ключа більш ніж на два роки. Посадова особа, яка здійснила переформування кваліфікованого сертифіката, складає акт, у якому зазначаються дата і час скасування кваліфікованого сертифіката, ідентифікаційні дані користувача, що містяться в кваліфікованому сертифікаті, та невідповідні ідентифікаційні дані користувача, зазначені в заявці на формування кваліфікованого сертифіката. Акт підписується посадовою особою Надавача, яка здійснила переформування кваліфікованого сертифіката, та додається до документів (засвідчених у встановленому порядку копій документів), що використовувалися під час ідентифікації та реєстрації користувачів.

4.5. Використання пари ключів і сертифікатів

4.5.1. Використання Користувачем особистого ключа та сертифіката

При використанні особистого ключа користувач повинен дотримуватися таких правил:

- забезпечувати конфіденційність і неможливість доступу інших осіб до особистого ключа;
- негайно повідомляти Надавача про підозру або факт компрометації особистого ключа;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування чи блокування відповідного кваліфікованого сертифіката;
- особисто відповідає за захист пароля від особистого ключа.

Користувач повинен використовувати кваліфікований сертифікат, як установлено у призначенні ключа ("keyUsage") і згідно обмежень щодо його використання.

При використанні особистого ключа та кваліфікованого сертифіката користувач зобов'язаний дотримуватись вимог законодавства у сфері електронних довірчих послуг, а також положень:

- Регламенту роботи Надавача;
- цієї Політики сертифікатів та Положення сертифікаційних практик;
- Загальних умов надання кваліфікованих електронних довірчих послуг користувачам Надавача;
- Договору про надання кваліфікованих електронних довірчих послуг, укладеного з Надавачем.

4.5.2. Використання відкритого ключа та сертифіката довіреними сторонами

Кваліфіковані сертифікати користувача, сформовані Надавачем, можуть використовуватися будь-якими довіреними сторонами для забезпечення їх автентифікації, зокрема шляхом верифікації та підтвердження кваліфікованого електронного підпису чи печатки.

Перш ніж прийняти кваліфікований електронний підпис або печатку користувача, довірена сторона повинна перевірити таку інформацію:

- статус кваліфікованого сертифіката користувача, сферу використання кваліфікованого сертифіката користувача, обмеження щодо використання та інформацію про кваліфікований сертифікат користувача;
- відповідність особистого ключа відкритому ключу кваліфікованого електронного підпису чи печатки, який пов'язаний з кваліфікованим сертифікатом користувача.

Довіряюча сторона повинна виконати такі перевірки:

- перевірити статус кваліфікованого сертифіката користувача на момент накладення кваліфікованого електронного підпису чи печатки за допомогою OCSP-сервера Надавача (сервер перевірки статусу кваліфікованого сертифіката), сферу використання (поле KeyUsage у сертифікаті), обмеження щодо використання та інформацію про кваліфікований сертифікат для перевірки того, що кваліфікований сертифікат користувача наразі дійсний;
- перевірити статус кваліфікованого сертифіката Надавача при створенні кваліфікованого електронного підпису або печатки користувачем.

Кваліфікований електронний підпис або печатка вважаються дійсними, якщо результати перевірки у вищевказаних пунктах успішно завершені та одночасно дійсні.

Довіряюча сторона несе відповідальність за невиконання вищевказаної процедури перевірки або виконання перевірки, знаючи, що кваліфікований сертифікат недійсний на момент перевірки.

При використанні відкритого ключа та кваліфікованого сертифіката користувача довіряючі сторони повинні дотримуватись вимог законодавства у сфері електронних довірчих послуг, а також положень цієї Політики сертифікатів та Положення сертифікаційних практик.

4.6. Поновлення сертифіката

Користувач може протягом 30 календарних днів поновити чинність кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований Надавачем, якщо протягом 30 календарних днів користувач не поновить його чинність.

Надавач забезпечує:

- прийом та перевірку заяв користувачів на поновлення дії їх кваліфікованих сертифікатів, які були заблоковані Надавачем;
- прийом та перевірка заяв користувачів у паперовій формі на поновлення дії їх кваліфікованих сертифікатів, дію яких призупинено Надавачем, протягом одного робочого дня з моменту отримання заяви та відповідно до режиму роботи Надавача;
- поновлення дії кваліфікованих сертифікатів, які були заблоковані Надавачем відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Інформування користувачів про закінчення терміну дії кваліфікованого сертифіката здійснюється Надавачем за 7 днів до закінчення терміну дії кваліфікованого сертифіката, шляхом надсилання SMS/Push-повідомлень на номер телефону користувача, який вказаний в заявці на формування сертифіката.

4.7. Повторне формування сертифіката

Користувач може сформувати новий кваліфікований сертифікат після закінчення терміну дії та в разі нагальної потреби (компрометація особистого ключа або його пароля, втрата особистого ключа, зміни інформації, що міститься в кваліфікованому сертифікаті користувача) в такі способи:

- в мобільному застосунку monobank;
- за особистої присутності фізичної особи, фізичної особи - підприємця або уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманих у встановленому законодавством порядку з ЄДР, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДРПОУ, та про документи, що посвідчують особу, що підтверджують громадянство України чи спеціальний статус особи;

4.8. Модифікація сертифіката

Внесення змін до кваліфікованого сертифіката не допускається.

4.9. Скасування та блокування сертифіката

Надавач забезпечує:

- цілодобовий прийом та перевірку заяв користувачів в електронній формі про скасування їх кваліфікованих сертифікатів, сформованих Надавачем за допомогою застосунку monobank;
- прийом та перевірка заяв користувачів у паперовій формі про скасування та блокування їх кваліфікованих сертифікатів, сформованих Надавачем, протягом одного робочого дня з моменту надходження заяви та відповідно до режиму роботи Надавача;
- скасування та блокування кваліфікованих сертифікатів, сформованих Надавачем, відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Користувач має право призупинити дію кваліфікованого сертифіката за власним бажанням. Призупинення дії кваліфікованого сертифіката може бути здійснено Надавачем за заявою про зміну статусу кваліфікованого сертифіката в паперовому вигляді або після ідентифікації користувача за ключовою фразою, введеною в заяві на реєстрацію. Під призупиненням дії кваліфікованого сертифіката розуміється тимчасове припинення дії кваліфікованого сертифіката (блокування) на строк до 30 календарних днів.

Після призупинення дії кваліфікованого сертифіката користувач може поновити дію кваліфікованого сертифіката протягом 30 календарних днів. Заблокований кваліфікований сертифікат буде автоматично скасований Надавачем, якщо користувач не поновить його дію протягом зазначеного терміну.

Кваліфікований сертифікат стає недійсним з моменту зміни його статусу на «скасований».

Скасований кваліфікований сертифікат не можна поновити.

Кваліфікований сертифікат вважається призупиненим з моменту зміни його статусу на «заблокований».

Кваліфікований сертифікат, статус якого змінено на «заблокований», є недійсним і не використовується протягом періоду призупинення.

Кваліфіковані сертифікати користувачів, які дали згоду на їх публікацію, оприлюднюються одразу після формування таких сертифікатів.

Надавач формує CRL у вигляді повних та часткових списків, які відповідають таким вимогам:

- у кожному CRL зазначено термін його дії до видачі нового списку;
- новий CRL може бути опублікований до закінчення терміну його дії до публікації наступного списку;
- CRL повинен бути підписаний кваліфікованим електронним підписом або печаткою Надавача.

CRL публікується автоматично.

Час зміни статусу кваліфікованих сертифікатів синхронізується з Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Посилання на CRL присутнє в кваліфікованому сертифікаті користувачів.

Повний CRL формується та публікується 1 (один) раз на тиждень і містить інформацію про всі скасовані сертифікати, які були сформовані Надавачем.

Частковий CRL формується та оприлюднюється кожні 2 (дві) години та містить інформацію про всі кваліфіковані сертифікати, статус яких було змінено в проміжку часу між часом видачі останнього повного CRL та моментом формування поточного часткового CRL.

4.10. Послуга перевірки статусу сертифіката

Надавач забезпечує доступність інформації про статус сертифіката в режимі реального часу за допомогою CRL та OCSP-сервера.

4.11. Закінчення терміну дії сертифіката

Дата і час початку та закінчення терміну дії сертифіката користувача зазначаються в сертифікаті з точністю до однієї секунди.

Після закінчення терміну дії та часу дії сертифіката користувача, зазначених у ньому, такий сертифікат вважається скасованим.

4.12. Депонування та повернення ключів

Не застосовується.

5. КОНТРОЛЬ ОБ'ЄКТІВ, УПРАВЛІННЯ ТА ЕКСПЛУАТАЦІЯ

5.1. Контроль фізичної безпеки

5.1.1. Вимоги до приміщень Надавача

Приміщення Надавача розділене на функціональні зони відповідно до встановлених Надавачем рівнів безпеки приміщень.

Приміщення Надавача за рівнем безпеки поділяються на спеціальні та службові. Для кожного рівня безпеки приміщень визначається мінімально необхідний набір механізмів безпеки, зокрема: контроль доступу, виявлення вторгнень, пожежна сигналізація та пожежогасіння, альтернативні та резервні джерела живлення тощо.

Зазначені механізми безпеки приміщень можуть бути змінені на основі оцінених ризиків та обраних відповідних цим ризикам механізмів їх нейтралізації.

Компоненти, які мають вирішальне значення для безпечної роботи Надавача, повинні бути розташовані в захищеному та безпечному середовищі з фізичним захистом від вторгнення, контролем доступу через периметр безпеки та сигналізацією для виявлення вторгнення.

5.1.2. Фізичний доступ

Доступ до спеціальних та службових приміщень Надавача (зони безпеки) забезпечується із застосуванням організаційно-технічних заходів контролю (фізичний та логічний контроль).

Право доступу до спеціальних приміщень дата-центру мають особи внесені до Порядку доступу до приміщень дата-центру, а також керівник Надавача та персонал Надавача відповідно до своїх посадових обов'язків, які входять у відповідний перелік уповноважених працівників Надавача, які мають доступ до спеціальних приміщень Надавача.

Допущення сторонніх працівників до спеціальних приміщень здійснюється:

1) у штатних ситуаціях (планові перевірки, ремонтно-відновлювальні роботи тощо) - за рішенням Голови Правління АТ "УНІВЕРСАЛ БАНК" або особи, яка виконує його обов'язки, на підставі службової записки керівника Надавача та з подальшим включенням таких працівників до Заявки на доступ;

2) у надзвичайних ситуаціях (пожежа, повінь, стихійне лихо, аварії тощо) - без дозволу Голови Правління АТ "УНІВЕРСАЛ БАНК" або особи, яка виконує його обов'язки, з обов'язковою фіксацією причини для екстреного доступу до об'єкта.

При вході в дата-центр охоронець ідентифікує уповноважених працівників АТ "УНІВЕРСАЛ БАНК" за документами, що посвідчують особу (паспорт громадянина України, посвідчення водія).

Реєстрація доступу до спеціальної кімнати здійснюється в електронному або паперовому журналі доступу, який знаходиться в ЦОД.

Серверна шафа, в якій знаходиться обладнання Надавача, зачинена на ключ, зачинена з використанням кодового замку та/або опечатана відповідальними працівниками Надавача.

Територія дата-центру та серверна кімната, де розміщено обладнання Надавача, обладнані системою відеоспостереження, яка працює цілодобово, логи відеоспостереження зберігаються в дата-центрі.

Внесення/винесення обладнання зі спеціального приміщення здійснюється на підставі акту внесення/винесення обладнання, підписаного відповідальними працівниками якщо це передбачено договором.

ІКС Надавача складається з двох ідентичних незалежних майданчиків (основного та резервного), розташованих на відстані понад 100 км один від одного.

5.2. Процедурний контроль

5.2.1. Ролі персоналу Надавача

Персоналом Надавача є:

- керівник Надавача;
- заступник керівника Надавача;
- адміністратор реєстрації;
- адміністратор сертифікації;
- адміністратор безпеки;
- аудитор системи;
- системний адміністратор.

5.2.1.1. Керівник Надавача

Керівник Надавача в межах покладених на нього обов'язків відповідає за організацію та контроль процесів, спрямованих на забезпечення функціонування та розвитку Надавача та захист інформації в Надавача, а саме:

- здійснює загальне керівництво діяльністю Надавача і контроль за його діяльністю;
- дає доручення, обов'язкові для працівників Надавача, які виконують функції адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, аудитора системи, адміністратора безпеки;
- погоджує документи, що визначають організаційні, технічні та технологічні умови діяльності Надавача;
- затверджує інструкції, проектну й експлуатаційну документацію;
- підписує документи, які Надавач подає до засвідчувального центру;
- здійснює представництво та захист інтересів Надавача в сфері кваліфікованих електронних довірчих послуг.

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.

Керівником Надавача повинна бути встановлена чітка система контролю за дотриманням працівниками Надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних

довірчих послуг і вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо СУІБ.

5.2.1.2. Заступник керівника Надавача

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

5.2.1.3. Адміністратор реєстрації

Адміністратор реєстрації та працівник відокремленого пункту реєстрації, на якого покладено обов'язок з реєстрації Клієнтів, відповідає за:

- ідентифікацію, автентифікацію, верифікацію та реєстрацію Клієнтів;
- надання допомоги Клієнтам під час генерації пар ключів (у разі необхідності);
- опрацювання документів і запитів, наданих Клієнтами;
- перевірку законності звернень про блокування, поновлення та скасування сертифікатів ключів Клієнтів;
- перевірку документів, наданих Клієнтами заяв про формування, блокування, поновлення та скасування сертифікатів ключів;
- надання допомоги Клієнтам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;
- надання консультацій щодо умов та порядку надання кваліфікованих електронних довірчих послуг, які надає Надавач;
- встановлення належності відкритого ключа та відповідного йому особистого ключа Клієнту;
- ведення обліку Клієнтів.

До працівників відокремлених пунктів реєстрації Надавача, відповідальних за реєстрацію користувачів, ставляться такі ж вимоги, як і до адміністраторів реєстрації.

5.2.1.4. Адміністратор сертифікації

Адміністратор сертифікації відповідає за:

- формування кваліфікованих сертифікатів відкритих ключів;
- ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;
- генерацію, створення резервних копій та використання особистих ключів Надавача;
- збереження особистих ключів Надавача та їх резервних копій.

Основними обов'язками адміністратора сертифікації є:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача (зазначену у цьому абзаці генерацію здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки);
- зберігання особистих ключів Надавача та їх резервних копій;
- забезпечення використання особистих ключів Надавача під час формування та обслуговування сертифікатів ключів Надавача та Клієнтів;
- участь у знищенні особистих ключів Надавача та їх резервних копій (зазначене у цьому абзаці знищення здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки);
- забезпечення ведення, архівування та відновлення баз даних сертифікатів ключів Клієнтів;
- забезпечення публікації сертифікатів ключів Клієнтів та CRL на веб-сайті Надавача;
- створення резервних копій сертифікатів ключів Клієнтів;

– зберігання сертифікатів ключів Клієнтів, їх резервних копій, СВС та інших резервних копій, які передбачені вимогами законодавства України в сфері електронних довірчих послуг.

5.2.1.5. Адміністратор безпеки

Адміністратор безпеки відповідає за:

– належне функціонування СУІБ;
– проведення перевірок дотримання адміністраторами реєстрації, адміністраторами сертифікації, аудиторами системи, системними адміністраторами, працівниками ВПР, на яких покладено обов'язки реєстрації Клієнтів, вимог документації щодо СУІБ. Періодичність проведення таких перевірок – не рідше ніж один раз на рік.

Основними обов'язками адміністратора безпеки є:

– здійснення контролю за генерацією пар ключів Надавача та створенні резервних копій особистих ключів Надавача (зазначену у цьому абзаці генерацію здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки);
– контроль за формуванням, обслуговуванням і створенням резервних копій сертифікатів ключів Надавача, Клієнтів та СВС;
– контроль за зберіганням особистих ключів Надавача та їх резервних копій, особистих ключів адміністраторів;
– здійснення контролю за знищенням особистих ключів Надавача та їх резервних копій (зазначене у цьому абзаці знищення здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки), контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
– організація розмежування доступу до ресурсів ІКС Надавача;
– контроль за функціонуванням СУІБ;
– забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування СУІБ після збоїв, відмов, аварій ІКС Надавача;
– забезпечення режиму доступу до приміщень Надавача, в яких розміщена ІКС Надавача;
– ведення журналів обліку адміністратора безпеки, визначених документацією СУІБ;
– проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо СУІБ;
– контроль за дотриманням працівниками Надавача положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо СУІБ;
– контроль за веденням реєстру Надавача;
– контроль за веденням архіву Надавача.

Забороняється суміщення обов'язків адміністратора безпеки з обов'язками адміністратора реєстрації, адміністратора сертифікації, аудитора системи, системного адміністратора та працівників ВПР, на яких покладені обов'язки з реєстрації Клієнтів.

Адміністратором безпеки може бути особа, яка має стаж роботи у сфері захисту інформації або кібербезпеки не менше 3 (трьох) років та відповідає хоча б одній з умов:

– має вищу освіту за спеціальністю у сферах захисту інформації або кібербезпеки;
– має вищу освіту за спеціальністю у сфері інформаційних технологій та пройшла курси підвищення кваліфікації у сфері захисту інформації або кібербезпеки.

5.2.1.6. Аудитор системи

Аудитор системи відповідає за виявлення недоліків у функціонуванні СУІБ та своєчасне інформування про це Керівника Надавача, заступника Керівника Надавача та адміністратора безпеки.

Аудитор системи здійснює перегляд архівів та журналів аудиту подій ІКС Надавача.

Основними обов'язками Аудитора системи є:

– перегляд та у разі виявлення недоліків функціонування СУІБ проведення перевірок цілісності архівів, а також журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;

- забезпечення спостереження за функціонуванням СУІБ (реєстрація подій в ІКС Надавача, моніторинг подій тощо);
- участь у розслідуванні інцидентів з безпеки в ІКС Надавача.

5.2.1.7. Системний адміністратор

Системний адміністратор відповідає за належне функціонування засобів та обладнання ІКС Надавача.

Основними обов'язками системного адміністратора є:

- організація експлуатації та технічного обслуговування ІКС Надавача і адміністрування її технічних засобів;
- забезпечення функціонування веб-сайту Надавача;
- участь у впровадженні та забезпеченні функціонування СУІБ в ІКС Надавача;
- забезпечення ведення журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;
- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального ПЗ ІКС Надавача;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІКС Надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІКС Надавача, у зв'язку зі збоями.

5.2.2. Забезпечення персоналу

Чисельність персоналу Надавача є достатня для виконання завдань щодо формування та супроводу сертифікатів Надавача та користувачів Надавача.

Працівники Надавача відповідають кваліфікаційним вимогам, встановленим для відповідних посад, та мають офіційне працевлаштування. Перед призначенням на посаду у працівника перевіряються необхідні документи щодо освіти, кваліфікації, стажу роботи тощо.

Перелік посад, які є обов'язковими в Надавача, а також їх функції та завдання визначені п. 5.2.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

Обов'язковою є наявність не менше двох посад адміністратора безпеки у Надавача.

Вимоги до кваліфікації та досвіду роботи персоналу Надавача визначені п. 5.3.1 цієї Політики сертифікатів та Положення сертифікаційних практик..

5.2.3. Ролі довіреного персоналу, що вимагають розподілу обов'язків

Працівникам Надавача забороняється суміщення посадових обов'язків адміністратора безпеки з посадами адміністратора реєстрації, адміністратора сертифікації, системного адміністратора та аудитора системи.

Кожен працівник перед призначенням на посаду, пов'язану з наданням кваліфікованих електронних довірчих послуг Надавача та отриманням атрибутів доступу до ІКС Надавача, проходить перевірку своєї особи, ідентичності та кваліфікації відповідно з вимогами до займаної посади та пов'язаних з нею функціональних обов'язків.

5.3. Контроль персоналу

5.3.1. Вимоги до кваліфікації, досвіду та допуску персоналу

Персонал Надавача має необхідні знання, досвід та кваліфікацію для надання кваліфікованих електронних довірчих послуг.

Адміністратором сертифікації, адміністратором безпеки, аудитором системи, системним адміністратором може бути особа, яка має вищу освіту за спеціальністю інформаційні технології, захист інформації або кібербезпека, а також стаж роботи за фахом у цих сферах не менше трьох років.

5.3.2. Вимоги та процедури навчання персоналу

Керівник Надавача зобов'язаний забезпечити створення умов для безперервної особистісної освіти та постійного підвищення кваліфікації персоналу Надавача у сферах інформаційних технологій, захисту інформації чи кібербезпеки. безпека та захист персональних даних.

Співробітники Надавача регулярно беруть участь у семінарах, конференціях та нарадах з питань надання кваліфікованих електронних довірчих послуг, інформаційних технологій, захисту інформації, кібербезпеки та захисту персональних даних. Проходження навчання повинно бути підтверджено дипломом, сертифікатом тощо.

5.3.3. Санкції за несанкціоновані дії персоналу

Керівником Надавача встановлено чітку систему дисциплінарних стягнень за невиконання персоналом Надавача посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо комплексних систем захисту інформації або систем управління інформаційною безпекою.

Невиконання персоналом Надавача посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо системи управління інформаційною безпекою в організації, враховуючи режим роботи Надавача, передбачає дисциплінарну, адміністративну та кримінальну відповідальність, згідно:

- колективного договору між АТ «УНІВЕРСАЛ БАНК» та працівниками;
- договору на здійснення представництва Надавача (для відокремлених пунктів реєстрації Надавача);
- Кодексу України про адміністративні правопорушення;
- Кримінального кодексу України.

5.3.4. Контроль відокремлених пунктів реєстрації

До працівників відокремлених пунктів реєстрації Надавача, які відповідають за реєстрацію користувачів, ставляться такі ж вимоги, як і до адміністраторів реєстрації.

До працівників відокремлених пунктів реєстрації Надавача належать працівники юридичних осіб та фізичних осіб – підприємців, які на підставі договору з АТ «УНІВЕРСАЛ БАНК» здійснюють реєстрацію користувачів.

На працівників відокремлених пунктів реєстрації Надавача покладаються такі функціональні обов'язки:

- адміністратор реєстрації відокремленого пункту реєстрації Надавача;
- відповідальний за захист інформації у відокремленому пункті реєстрації Надавача;
- адміністратор виїзної реєстрації.

Адміністратор реєстрації відокремленого пункту реєстрації відповідає за виконання функцій і обов'язків адміністратора реєстрації, як це визначено цією Політикою сертифікатів та Положення сертифікаційних практик.

Відповідальні за захист інформації призначаються з числа адміністраторів реєстрації відокремленого пункту реєстрації Надавача.

За належну роботу комплексу засобів захисту відокремленого пункту реєстрації Надавача в межах своїх посадових обов'язків відповідає відповідальний за захист інформації у відокремленому пункті реєстрації Надавача.

Основними посадовими обов'язками відповідального за захист інформації у відокремленому пункті реєстрації Надавача є:

- організація експлуатації та обслуговування апаратно-програмного забезпечення відокремленого пункту реєстрації Надавача;
- участь у впровадженні та забезпеченні функціонування системи управління інформаційною безпекою відокремленого пункту реєстрації Надавача;
- контроль за роботою програмного комплексу відокремленого пункту реєстрації Надавача;
- контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації Надавача;
- участь у створенні та введенні в експлуатацію системи управління інформаційною безпекою відокремленого пункту реєстрації Надавача.

Допускається виконання системним адміністратором та адміністратором безпеки функцій особи, відповідальної за захист інформації у відокремленому пункті реєстрації Надавача, у частині, що не суперечить їхнім аналогічним функціям щодо до інших складових ІКС Надавача.

Адміністратор реєстрації на місці несе відповідальність за перевірку документів, наданих користувачами, їх заявок на формування, блокування, поновлення та скасування кваліфікованих сертифікатів і не бере участі у формуванні кваліфікованих сертифікатів користувачів.

Основними обов'язками адміністратора виїзної реєстрації є:

- ідентифікація та автентифікація користувачів;
- перевірка заявок на формування, блокування, поновлення та скасування кваліфікованих сертифікатів;
- встановлення права власності на відкритий ключ і відповідний особистий ключ для користувача.
- Додатковими обов'язками адміністратора виїзної реєстрації є:
- надання допомоги під час генерації пари ключів користувача;
- надання консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг;
- передача заявок на формування, блокування, поновлення, скасування кваліфікованих сертифікатів та запитів на формування кваліфікованих сертифікатів користувача віддаленому адміністратору реєстрації.

5.3.5. Документація яка надається персоналу

Організаційно-правовий статус керівника та персоналу Надавача, їх завдання і функції, права та обов'язки, відповідальність, а також професійні знання, досвід і кваліфікація визначаються посадовими інструкціями.

Посадові інструкції містять вимоги інформаційної безпеки та способи її забезпечення.

Керівник та працівники Надавача ознайомлені з положеннями своїх посадових інструкцій та діють відповідно до своїх посадових завдань і функцій.

Персонал Надавача повинен бути проінформований про зміни в організації процесів Надавача, що стосуються їх посадових обов'язків.

5.4. Ведення журналу аудиту подій

5.4.1. Види записаних подій

Процедури управління доказами та записами повинні передбачати ведення журналів аудиту подій таких типів:

- журнали аудиту;
- системні журнали;
- журнали роботи та доступу;
- журнали додатків;
- інші.

5.4.2. Частота обробки журналу аудиту подій

Журнали аудиту подій резервуються та переглядаються адміністратором безпеки та аудитором системи принаймні раз на тиждень, щоб впевнитись у відсутності несанкціонованих змін та перегляду і розслідування подій.

5.4.3. Строки зберігання журналу аудиту подій

Надавач зберігає журнали аудиту подій за місцем їх створення протягом 1 року, після чого вони передаються на архівне зберігання.

5.4.4 Захист журналу аудиту подій

Усі записи в журналах аудиту подій в електронному або паперовому вигляді повинні містити дату та час події, а також ідентифікувати суб'єкта, який її ініціював або брав у ній участь.

Час, записаний у журналі аудиту подій, синхронізовано з Всесвітнім координованим часом (UTC) з точністю до секунди.

Журнали аудиту подій захищені від несанкціонованого перегляду, модифікації та знищення.

Записи про події в паперових журналах аудиту подій повинні бути перевірені та завірені підписом адміністратором безпеки та/або аудитором системи.

5.4.5. Процедури резервного копіювання журналу аудиту подій

Резервне копіювання журналу аудиту подій здійснюється Надавачем відповідно до внутрішньої документації із захисту ІКС Надавача та документації СУІБ Надавача.

5.4.6. Синхронізація часу

- Синхронізацію часу у технічних засобах ІКС Надавача забезпечує комплекс засобів синхронізації часу за протоколом NTP з з точністю до однієї секунди.

Джерела синхронізації часу – сервери ЗЦ, ЦЗО та джерела, синхронізовані з державним еталоном одиниць часу і частоти.

5.5. Архів документів

5.5.1. Види документів і відомостей, що підлягають архівному зберіганню.

Архівне зберігання інформації здійснюється відповідно до внутрішніх організаційно-розпорядчих документів Надавача.

Обов'язковому архівуванню підлягають:

- кваліфіковані сертифікати Надавача та користувачів;
- CRL;
- журнали аудиту подій;
- документована інформація - документи (заявки на формування, блокування, поновлення, скасування сертифікатів користувачів), на підставі яких користувачам надавалися електронні довірчі послуги.

5.5.2. Терміни зберігання архіву

Документи в паперовій та електронній формах повинні зберігатися в порядку, встановленому законодавством у сфері архівної справи та законодавством в сфері електронних довірчих послуг.

Знищення архівних документів здійснюється комісією, до складу якої входять керівник Надавача, адміністратор безпеки та аудитор системи (у разі необхідності – адміністратор сертифікації). Після завершення процедури знищення архівних документів складається відповідний акт, який затверджується керівником Надавача.

Сертифікати Надавача, сертифікати серверів Надавача, сертифікати адміністраторів, сертифікати користувачів, а також CRL зберігаються постійно.

5.5.3. Захист архіву

Надавач забезпечує охорону архіву відповідно до внутрішніх організаційно-розпорядчих документів та законодавства в галузі архівної справи.

Для зберігання носіїв інформації з резервними та архівними копіями виділяється окреме сховище (сейф або безпечний відсік) з двома примірниками ключів та пристроями для опечатування. Один примірник ключа від сховища знаходиться в адміністратора безпеки, другий в опечатаному вигляді зберігається в сховищі (сейфі) керівника Надавач.

Приміщення архіву обладнується технічними засобами, що виключають можливість проникнення сторонніх осіб та неконтрольованого доступу до інформації, що архівується.

Надавач може накладати електронні позначки часу на записи, пов'язані з його діяльністю

5.5.4. Процедури резервного копіювання архіву

Надавач забезпечує резервне копіювання архіву відповідно до вимог СУІБ Надавача.

Інструменти серверів Надавача забезпечують автоматичне резервне копіювання даних. Автоматичне створення резервної копії необхідно виконувати не рідше одного разу на добу під час найменшого навантаження на центральний сервер Надавача.

Крім того, можна створити резервну копію сертифікатів на оптичних носіях або інших знімних носіях у ручному режимі. Після створення нової резервної копії попередня стає архівованою.

Відновлення сертифікатів з резервної копії здійснюється за допомогою центрального сервера Надавача шляхом зчитування сертифікатів з останньої (поточної) резервної копії та запису їх у базу даних сервера Надавача.

Знімні носії зберігаються в конвертах або пакетах, які опечатуються адміністратором безпеки. При цьому на упаковці вказується реєстраційний номер примірника. Факти створення та використання примірників фіксуються в окремому журналі.

Резервні копії баз даних та журнали аудиту подій зберігаються в приміщенні Надавача протягом 10 років. Контроль за автоматичним резервним копіюванням і ручним резервним копіюванням покладається на системного адміністратора. Адміністратор безпеки та адміністратор аудиту періодично контролюють процес створення та зберігання резервних копій.

5.5.5. Вимоги до електронної позначки часу

Вимоги до електронної позначки часу визначено законодавством України в сфері електронних довірчих послуг та Регламентом роботи Надавача.

5.5.6. Система збору архівів (внутрішня або зовнішня)

Системи архівного збору розміщені в службових та спеціальних приміщеннях Надавача.

Вимоги до службових та спеціальних приміщень описані в п. 5.1.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

5.5.7. Порядок отримання та перевірки архівної інформації

Доступ до архівних даних суворо обмежений. Лише уповноважені працівники Надавача мають доступ до цієї системи відповідно до своїх повноважень. Надавач оприлюднює інформацію з архіву тільки за рішенням суду.

5.6. Заміна ключа Надавача

Заміна пари ключів Надавача або серверів Надавача може бути:

- планова заміна пари ключів Надавача або серверів Надавача;
- позапланова заміна пари ключів Надавача або серверів Надавача.

Планова заміна пари ключів Надавача здійснюється не пізніше ніж за два роки до закінчення терміну дії кваліфікованого сертифіката Надавача для забезпечення безперебійної роботи Надавача та кваліфікованих сертифікатів користувачів Надавача.

Позапланова заміна пари ключів здійснюється у випадках компрометації або підозри на компрометацію особистих ключів Надавача, сертифікатів серверів Надавача (OCSP, TSP) або у разі збою криптомодуля (HSM) із особистим ключем.

Після заміни особистих ключів Надавач створює кваліфіковані сертифікати користувача з використанням нової пари ключів Надавача.

Доступ до чинного кваліфікованого сертифіката Надавача надається на офіційному веб-сайті Засвідчувального центру та ЦЗО.

5.7. Компрометація і аварійне відновлення

5.7.1. Процедури обробки інцидентів і компрометації

Надавач має План забезпечення безперервної діяльності Надавача, що включає в себе план реагування на інциденти та план аварійного відновлення.

Порядок дій та реагування персоналу Надавача на інциденти визначається Планом забезпечення безперервної діяльності Надавача та документацією системи управління інформаційною безпекою.

Процедури управління інцидентами повинні включати:

- здійснення заходів, визначених Порядком координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ та організацій незалежно від форм власності з питань запобігання, виявлення та ліквідації наслідків несанкціонованих дій. щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 № 94, зареєстрованого в Міністерстві юстиції України від 07.07.2008 за N 603/15294;
- інформування контролюючого органу та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли їм стало відомо про таке порушення, у порядку, встановленому Кабінетом Міністрів України;
- інформування користувачів електронних довірчих послуг про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли їм стало відомо про таке порушення, у порядку, встановленому Кабінетом Міністрів України.

5.7.2. Процедури відновлення, якщо обчислювальні ресурси, програмне забезпечення та/або дані пошкоджено

Визначається Планом забезпечення безперервної діяльності Надавача та документацією системи управління інформаційною безпекою Надавача.

5.7.3. Процедури відновлення після компрометації ключа

У разі виникнення підозри щодо компрометації особистого ключа Надавача або його серверів, робота криптомодулів (HSM) з цими особистими ключами призупиняється, служба захисту інформації Надавача починає службове розслідування.

У разі підтвердження факту компрометації особистого ключа Надавача або його серверів, керівник Надавача, адміністратор безпеки та аудитор системи зобов'язані вжити наступних заходів:

- зупинити роботу криптомодулів з скомпрометованими особистими ключами Надавача або його серверів;
- повідомити Засвідчувальний центр, ЦЗО про компрометацію особистого ключа Надавача або його серверів;
- скасувати кваліфікований сертифікат Надавача або його серверів, що відповідає скомпрометованому особистому ключу;
- ініціювати знищення скомпрометованого особистого ключа Надавача або його серверів у криптомодулі;
- згенерувати новий особистий ключ Надавача або його серверів та ініціювати формування відповідного йому кваліфікованого сертифіката Надавача або його серверів;
- активувати новий особистий ключ Надавача або його серверів.

Детальний порядок відновлення після компрометації особистого ключа Надавача або його серверів визначається документацією системи управління інформаційною безпекою Надавача.

5.7.4. Можливості безперервності бізнесу після аварії

Надавач має два аналогічних географічно рознесених майданчика, які працюють паралельно один одному. Все обладнання та канали зв'язку мають повне резервування.

У разі непередбаченої аварії або катастрофи, збою одного з майданчиків, Надавач продовжує свою роботу на іншому майданчику. Резервні копії особистих ключів, даних та інформації, які є критично важливими для відновлення роботи Надавача, завжди перебувають в актуальному стані та надійно захищені.

5.8. Припинення діяльності Надавача

5.8.1. Підстави припинення діяльності Надавача

Надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг у разі:

1) прийняття Засвідчувальним центром або ЦЗО рішення про скасування статусу кваліфікованого надавача електронних довірчих послуг;

2) рішення Надавача про припинення надання кваліфікованих електронних довірчих послуг, зазначених у Довірчому списку;

3) припинення діяльності Надавача (припинення юридичної особи), за винятком випадків правонаступництва, визначених у п. 5.8.4 цієї Політики сертифікатів та Положення сертифікаційних практик;

4) набрання законної сили рішенням суду про скасування статусу кваліфікованого надавача, визнання Надавача банкрутом.

Про рішення щодо припинення надання кваліфікованих довірчих послуг Надавач зобов'язаний повідомити користувачів, Засвідчувальний центр, ЦЗО та Контролюючий орган не пізніше п'яти робочих днів з дати прийняття такого рішення.

ЦЗО та/або Засвідчувальний центр зобов'язаний оприлюднити інформацію про рішення про припинення діяльності АТ «Універсал банк» з надання кваліфікованих електронних довірчих послуг, у тому числі у зв'язку з скасуванням статусу кваліфікованого надавача електронних довірчих послуг, не пізніше наступного робочого дня після прийняття такого рішення:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;
- направлення Надавачу повідомлення про таке рішення із зазначенням підстави його прийняття.

У повідомленні ЦЗО та/або Засвідчувального центра про припинення надання кваліфікованих довірчих послуг Надавачем має бути зазначена дата публікації.

Надавач припиняє діяльність з надання кваліфікованих довірчих послуг через три місяці з дати оприлюднення ЦЗО та/або Засвідчувальним центром на своєму офіційному веб-сайті повідомлення про припинення надання Надавачем кваліфікованих електронних довірчих послуг.

З дня оприлюднення ЦЗО та/або Засвідчувальним центром на своєму офіційному веб-сайті інформації про припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавач зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

Надавач, припиняючи діяльність з надання кваліфікованих електронних довірчих послуг, передає обслуговування користувачів, з якими укладено договори про надання кваліфіковані електронні довірчі послуги, іншому надавачу кваліфікованих електронних довірчих послуг.

У разі відмови користувача від продовження отримання послуг за договором про надання кваліфіковані електронні довірчі послуги, укладеним з Надавачем у іншого надавача кваліфікованих електронних довірчих послуг до закінчення строку дії відповідного договору Надавач зобов'язаний повернути такому користувачеві кошти за послуги, які не можуть бути надані в майбутньому, якщо вони були раніше оплачені користувачем.

Якщо користувач погодився продовжити отримання послуг за договором про надання кваліфікованих електронних довірчих послуг, укладеним з Надавачем у іншого надавача електронних довірчих послуг до закінчення строку дії відповідного договору, Надавач зобов'язаний оплачувати подальше надання кваліфікованих електронних довірчих послуг такому користувачеві за тарифами, встановленими відповідним надавачем.

Центральний засвідчувальний орган з дати, визначеної як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем, вносить відповідні зміни до Довірчого списку.

У разі припинення надання кваліфікованих електронних довірчих послуг Надавач зобов'язаний передати іншому надавачу або Засвідчувальному центу документовану інформацію (документи, на підставі яких користувачам надано кваліфіковані електронні довірчі послуги та сформовано кваліфіковані сертифікати (усі блоковані, поновлені, скасовані та сформовані кваліфіковані сертифікати, а також CRL).

Передача документованої інформації має бути здійснена Надавачем не пізніше дати, визначеної ним як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або дати набрання законної сили відповідним рішенням суду.

Засвідчувальний центр скасовує виданий ним кваліфікований сертифікат Надавачу у день, визначений Надавачем, як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або в день набрання чинності відповідного рішення суду.

5.8.2. Повідомлення про припинення діяльності Надавача

Про прийняте рішення про припинення надання кваліфікованих електронних довірчих послуг Надавач зобов'язаний повідомити користувачів, ЦЗО та/або Засвідчувальний центр та КО не пізніше п'яти робочих днів з дня прийняття такого рішення.

ЦЗО та/або Засвідчувальний центр зобов'язаний оприлюднити інформацію про рішення Надавача щодо припинення діяльності Надавача з надання кваліфікованих електронних довірчих послуг, у тому числі у зв'язку з позбавленням статусу кваліфікованого надавача електронних довірчих послуг, не пізніше наступного робочого дня після прийняття такого рішення шляхом:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;
- направлення до Надавача повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО та/або Засвідчувальний центр зобов'язаний оприлюднити на своєму офіційному веб-сайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем не пізніше наступного робочого дня з дня отримання повідомлення про виникнення підстав передбачених підпунктами 2 - 4 пункту 5.8.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

Повідомлення ЦЗО та/або Засвідчувального центра про припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем повинно містити дату публікації.

5.8.3. Дата припинення діяльності Надавача

Надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дати оприлюднення на своєму офіційному веб-сайті ЦЗО та/або Засвідчувальним центром повідомлення про припинення надання кваліфікованих електронних довірчих послуг Надавачем.

З дати публікації на офіційному веб-сайті ЦЗО та/або Засвідчувальним центром повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем та до дати припинення діяльності з надання кваліфікованих електронних довірчих послуг, Надавач зобов'язаний надавати кваліфіковані електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

ЦЗО вносить відповідні зміни до Довірчого списку в день, визначений як дата припинення діяльності Надавача.

5.8.4. Правонаступництво

З метою забезпечення безперервного надання кваліфікованих електронних довірчих послуг своїм користувачам ЦЗО може прийняти рішення про внесення змін до Довірчого списку щодо заміни кваліфікованого надавача електронних довірчих послуг шляхом заміни інформації про Надавача на інформацію про іншого кваліфікованого надавача електронних довірчих послуг, якщо перехід відповідних прав та обов'язків здійснюється за взаємною згодою таких надавачів, договором або на інших підставах правонаступництва, визначених законодавством.

У разі відмови користувача від продовження обслуговування за договором про надання кваліфікованих електронних довірчих послуг, укладеним з Надавачем , який припиняє діяльність з надання кваліфікованих електронних довірчих послуг, іншому кваліфікованому надавачу електронних довірчих послуг до закінчення терміну дії відповідного договору, Надавач зобов'язується повернути такому користувачеві кошти за послуги, які не можуть бути надані в майбутньому, якщо вони були раніше оплачені користувачем.

У разі згоди користувача на продовження обслуговування за договором про надання кваліфікованих електронних довірчих послуг, укладеним з Надавачем, який припиняє діяльність з надання кваліфікованих електронних довірчих послуг, з іншим кваліфікованим надавачем електронних довірчих послуг до закінчення строку дії відповідного договору Надавач зобов'язується оплатити подальше надання такому користувачеві кваліфіковані електронні довірчі послуги за тарифами, встановленими відповідним кваліфікованим надавачем електронних довірчих послуг.

5.8.5. Передача документованої інформації

Надавач, у разі припинення діяльності з надання кваліфікованих електронних довірчих послуг, зобов'язаний передати всю документовану інформацію користувачів до іншого кваліфікованого надавача електронних довірчих послуг, який виявив намір продовжувати обслуговувати користувачів до закінчення строку дії відповідних договорів про надання кваліфікованих електронних довірчих послуг, або до Засвідчувального центру, на підставі яких користувачам надано кваліфіковані електронні довірчі послуги та сформовано, блоковано, поновлено, скасовано кваліфіковані сертифікати, усі сформовані кваліфіковані сертифікати, а також реєстри сформованих кваліфікованих сертифікатів.

5.8.6. План припинення діяльності

У Надавача є затверджений План припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем (далі – План припинення).

План припинення визначає умови, яких повинен дотримуватися Надавач з метою запобігання негативних наслідків у разі припинення ним діяльності з надання кваліфікованих електронних довірчих послуг, а також для забезпечення стабільності та довговічності кваліфікованих електронних довірчих послуг.

Надавач затверджує План припинення та, за необхідності, вносить до нього зміни з метою оновлення інформації, що міститься в ньому.

План припинення та зміни до нього затверджуються в установленому законодавством порядку.

План припинення визначає:

- порядок повідомлення користувачів, ЦЗО, Засвідчувального центру, персоналу Надавача, відокремлених пунктів реєстрації Надавача, пов'язаних осіб та контрагентів про припинення діяльності з надання кваліфікованих електронних довірчих послуг;
- домовленості та договори з третіми особами щодо продовження виконання зобов'язань у разі припинення діяльності Надавача з надання кваліфікованих електронних довірчих послуг (передачі послуг користувача іншому кваліфікованому надавачу електронних довірчих послуг).

План припинення є конфіденційним і перевіряється ООВ.

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

6.1. Генерація та встановлення пари ключів

6.1.1. Генерація пари ключів

6.1.1.1. Генерація пари ключів Надавача

Генерація особистого ключа Надавача здійснюється в криптографічному модулі (далі – криптомодуль), що має чинний позитивний експертний висновок у сфері криптографічного захисту інформації, виданий Адміністрацією Державної служби спеціального зв'язку та захисту інформації України та відповідає вимогам визначеним в ДСТУ EN 419 211-{2,3,4,5,6}:2016, який розташований у спеціальному приміщенні адміністратором сертифікації під наглядом адміністратора безпеки.

Перед процесом генерації адміністратор сертифікації проходить автентифікацію в криптомодулі. Дані автентифікації в криптомодулі створюються згідно з експлуатаційною документацією на криптомодуль перед початком процесу генерації. Як дані автентифікації можуть використовуватися паролі доступу до криптомодуля або інші засоби чи механізми, зазначені в експлуатаційній документації.

У процесі генерації особистий ключ Надавача зберігається в постійному накопичувачі криптомодуля. Запит на формування кваліфікованого сертифіката Надавача, що містить відкритий ключ, записується на постійний диск сервера Надавача або на знімний диск адміністратора сертифікації.

Факти генерації особистого ключа Надавача фіксуються в журналі криптомодуля та журналі ключових даних. За фактом генерації особистого ключа Надавача складається акт.

Генерація особистих ключів серверів Надавача (OCSP, TSP) здійснюється в криптомодулі адміністратором сертифікації під наглядом адміністратора безпеки.

У процесі генерації особисті ключі серверів Надавача (OCSP, TSP) зберігаються в криптомодулі. Запити на формування сертифікатів серверів Надавача (OCSP, TSP), що містять відкриті ключі, записуються на постійний диск центрального сервера або на знімний диск адміністратора сертифікації.

Факти генерації особистих ключів серверів Надавача (OCSP, TSP) фіксуються в журналі криптомодуля та журналі ключових даних. За фактом генерації особистих ключів серверів Надавача (OCSP, TSP) складається акт.

6.1.1.2. Генерація пари ключів користувача

Під час надання кваліфікованої електронної довірчої послуги зі створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток Надавач забезпечує:

- створення умов для генерації пари ключів користувача;

- допомогу під час генерації пари ключів користувача у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення зі значенням параметрів особистого ключа та їх копіювання;
- захист від доступу сторонніх осіб до параметрів особистого ключа користувача при використанні кваліфікованого електронного підпису чи печатки.

Особистий ключ у парі ключів користувача може бути згенерований:

- на робочому місці користувача;
- на АРМ генерації ключів в офісах Надавача та його відокремлених пунктах реєстрації;
- за допомогою мобільного застосунку monobank з використанням криптографічних бібліотек, що мають чинний позитивний експертний висновок у сфері криптографічного захисту інформації, виданий Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

У разі, якщо пара ключів була згенерована користувачем поза межами приміщення Надавача та/або за відсутності відповідного персоналу, ідентифікація такого користувача, перевірка достатності його цивільної дієздатності та дієздатності, генерація та видача йому кваліфікованого сертифіката здійснюється Надавачем після перевірки факту володіння користувачем особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката.

Для генерації особистих ключів використовуються засоби створення кваліфікованого та/або удосконаленого електронного підпису чи печатки і належать користувачам, або надаються Надавачем.

Сформований особистий ключ користувача захищений за допомогою атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані власника особистого ключа).

Для надання кваліфікованих електронних довірчих послуг Надавач використовує кваліфіковані засоби створення електронного підпису чи печатки, які мають позитивний експертний висновок за результатами їх державної експертизи в галузі КЗІ.

Забезпечення користувачів засобами створення кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів та їх технічна підтримка та обслуговування здійснюється Надавачем на договірних засадах.

Надання Надавачем засобів кваліфікованого або удосконаленого електронного підпису чи печатки у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватися шляхом передачі цих засобів на носіях інформації безпосередньо користувачу або шляхом надання доступу через веб-сайт Надавача.

6.1.3. Відкритий ключ користувача

Відкритий ключ надається для формування кваліфікованого сертифіката в складі запиту на формування кваліфікованого сертифіката, який є файлом у форматі PKCS#10, що містить відкритий ключ користувача та додаткову інформацію для формування кваліфікованого сертифіката.

Запит у форматі PKCS#10 формується під час генерації особистого та відкритого ключів засобами кваліфікованого електронного підпису чи печатки. Формування запиту передбачає створення удосконаленого та/або кваліфікованого електронного підпису за допомогою особистого ключа з однієї пари з відкритим ключем.

6.1.4. Доставка сертифікатів Надавача довіряючим сторонам

Кваліфіковані сертифікати Надавача, Засвідчувального центру та/або ЦЗО публікуються на веб-сайті Надавача.

Контейнер ланцюжків сертифікатів, доступний для завантаження довіряючими сторонами, розміщений на веб-сайті Надавача.

Доступ до чинних кваліфікованих сертифікатів Надавача надається на офіційному веб-сайті Засвідчувального центру та/або ЦЗО.

6.1.5. Розміри ключів Надавача

Надавачем забезпечується генерація особистих ключів та відповідних їм відкритих ключів з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 431 біт, що відповідає ДСТУ 4145-2002;

- алгоритм електронного підпису ECDSA з довжиною ключа 521 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT).

6.1.6. Параметри ключів та контроль якості

Під час генерації пари ключів використовується апаратний генератор випадкових чисел (ГВЧ), який включає статистичну перевірку виходу генератора. Статистична перевірка випадкових бітових послідовностей з апаратної ГВЧ здійснюється згідно з Методикою генерації ключових даних, яка погоджена з Державною службою спеціального зв'язку та захисту інформації України. Ключі генеруються та зберігаються в апаратному криптомодулі.

6.1.7. Основні цілі використання

Особисті ключі Надавача використовуються для таких цілей:

- накладення підпису на сертифікати користувачів;
- накладення підпису на сертифікат OCSP серверу;
- накладення підпису на CRL.

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

6.2.1. Стандарти та засоби керування криптографічним модулем

Для зберігання особистих ключів серверів Надавача використовуються криптомодулі, виконані у вигляді окремих апаратних пристроїв. Криптомодулі повинні мати сертифікат про оцінку відповідності або чинний позитивний експертний висновок за результатами державної експертизи в галузі КЗІ.

6.2.2. Доступ до особистого ключа Надавача

Доступ до особистих ключів Надавача мають лише відповідальні особи Надавача в межах своїх службових обов'язків:

- адміністратор безпеки;
- адміністратор сертифікації.

Атрибути доступу (логін та пароль) до особистих ключів Надавача зберігаються у конверті, опечатаному особистою печаткою відповідальної особи, який зберігається у сховищі (сейфі), розташованому у спеціальному та/або службовому приміщенні Надавача, ключі та доступ до якого мають виключно відповідальні особи, вказані вище.

Управління особистими ключами Надавача здійснюється відповідальними особами після їх автентифікації на центральному сервері Надавача за їхніми персональними атрибутами доступу.

6.2.3. Зберігання особистого ключа користувача

Не застосовується.

6.2.4. Резервне копіювання особистого ключа

Резервне копіювання особистих ключів Надавача та його серверів здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

Під час резервного копіювання особистих ключів Надавача створюється щонайменше дві резервні копії особистого ключа з криптомодуля. Кожна резервна копія особистого ключа Надавача записується (за потреби з розподілом таємниці) на зовнішній засіб кваліфікованого електронного підпису чи печатки, який є програмно-апаратним або апаратним пристроєм у захищеній формі, що забезпечує їх цілісність і конфіденційність.

Під час резервного копіювання особистих ключів серверів Надавача (OCSP, TSP) створюється щонайменше дві резервні копії кожного особистого ключа. Кожна резервна копія особистого ключа записується (за потреби з розподілом таємниці) на НКІ. У випадку, якщо особисті ключі серверів не зберігаються в криптомодулях, їх резервні копії створюються шляхом копіювання з основних НКІ на резервні.

Факти резервного копіювання особистих ключів Надавача та серверів Надавача (OCSP, TSP) фіксуються в журналі криптомодуля та/або журналі ключових даних.

6.2.5. Архівація особистого ключа

Не застосовується.

6.2.6. Відновлення особистого ключа

Відновлення особистих ключів Надавача і серверів (TSP, OCSP) здійснюється з резервних копій.

Факти відновлення особистих ключів Надавача та серверів (TSP, OCSP) з резервних копій фіксуються в журналі криптомодуля та журналі ключових даних. За фактом відновлення особистих ключів складаються відповідні акти.

6.2.7. Зберігання особистого ключа в криптографічному модулі

Особисті ключі Надавача та серверів (TSP, OCSP) зберігаються та захищені від несанкціонованого доступу в мережевих криптомодулях, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

6.2.8. Активація особистих ключів

Особисті ключі та ключі серверів (TSP, OCSP) Надавача зберігаються в HSM та не можуть бути використані без даних активації. Надавач зберігає дані активації безпечним способом і доступ до них можуть отримати лише уповноважені працівники Надавача.

6.2.9. Деактивація особистих ключів

Не застосовується.

6.2.10. Знищення особистих ключів

Після закінчення терміну дії кваліфікованого сертифіката Надавача та серверів Надавача (OCSP, TSP) відповідний особистий ключ та всі його резервні копії знищуються.

Знищення особистих ключів Надавача та серверів Надавача (OCSP, TSP) здійснюється згідно з експлуатаційною документацією на відповідні засоби створення кваліфікованого електронного підпису чи печатки, НКІ або мережеві криптомодулі, в яких вони зберігалися та використовувалися. Процедури знищення особистого ключа повинні гарантувати, що ключі не можна буде відновити після знищення.

Факти знищення особистих ключів Надавача та серверів Надавача (OCSP, TSP), а також їх резервних копій фіксуються в журналі криптомодуля та журналі ключових даних. За фактом знищення особистих ключів складаються акти.

6.2.11. Можливості мережевого криптомодуля

Мережевий криптомодуль підтримує процедури, які охоплюють безпечне функціонування ІКС Надавача (генерація, резервне копіювання, зберігання, знищення).

Усі мережеві криптомодулі, що містять копії особистого ключа Надавача та його серверів (OCSP, TSP), фізично захищені від несанкціонованого доступу.

Усі операції підписання з використанням особистого ключа Надавача виконуються в криптомодулі Надавача.

6.3. Інші аспекти керування парами ключів

6.3.1. Архівація відкритих ключів

Відкриті ключі, на основі яких були сформовані кваліфіковані сертифікати, постійно зберігаються в базі даних Надавача.

6.3.2. Термін дії сертифіката та умови використання пари ключів

Строки дії особистих ключів Надавача відповідають термінам дії кваліфікованих сертифікатів відповідних відкритих ключів і становлять:

- для особистих ключів Надавача та його серверів (OCSP, TSP) - не більше 5 років;
- для особистих ключів адміністраторів і користувачів Надавача - не більше 2 років.

6.4. Дані активації

6.4.1. Створення та встановлення даних активації

Не застосовується.

6.4.2. Захист даних активації

Особисті ключі, що зберігаються в НКІ, повинні бути захищені паролями, що складаються щонайменше з 8 символів, які містять великі та малі латинські літери, цифри та символи.

6.4.3. Інші аспекти даних активації

Відсутні.

6.5. Контроль комп'ютерної безпеки

6.5.1. Спеціальні технічні вимоги до комп’ютерної безпеки

Надавач забезпечує захист інформаційних ресурсів від зовнішніх загроз, атак і несанкціонованого витоку інформації шляхом створення та підтримки захищених інформаційних технологій, в рамках яких доступ до інформації різних категорій організовано таким чином, щоб лише авторизованим користувачам або процесам надається можливість працювати з конкретною інформацією, доступ до якої обмежений і гарантується цілісність, коли вона обробляється в електронному вигляді, у вигляді друкованого документа або набору даних, що містяться на знімному носії.

Надавач забезпечує:

- конфіденційність та цілісність інформації, яка зберігається та обробляється в складових компонентах ІКС Надавача, а також передається між ними;
- конфіденційність особистих ключів, які використовуються Надавачем;
- конфіденційність технологічної інформації, що забезпечує функціонування Надавача;
- доступ до інформації та ресурсів ІКС Надавача користувачам відповідно до правил, встановлених політикою безпеки Надавача;
- спостереження за діями користувачів шляхом впровадження механізмів і процедур контролю, реєстрації та аудиту зареєстрованих подій.

6.5.2. Комп'ютерна безпека

Надавач проходить випробування в частині функціонування ІКС Надавача, перевірений визнаними органами з оцінки відповідності та належним чином контролюється відповідно до [EN 319 401] та вимог чинного законодавства.

Після проходження оцінки відповідності органом з оцінки відповідності Надавач отримує сертифікат відповідності Надавача вимогам до надавачів електронних довірчих послуг. У разі проведення перевірок контролюючими органами Надавач отримує відповідний акт перевірки, складений комісією з відповідними висновками за результатами перевірки.

6.6. Елементи безпеки життєвого циклу

6.6.1. Контроль розробки системи

При розробці та впровадженні ІКС, Надавачу слід враховувати існуючі тенденції розвитку захищених інформаційних технологій, відомі розробки відповідних засобів захисту інформації та вимоги нормативно-правової бази з технічного захисту інформації.

З метою захисту інформації на всіх етапах життєвого циклу ІКС, Надавач має передбачати застосування таких заходів та засобів захисту інформації:

- організаційно-правові заходи, що здійснюються поза межами ІКС Надавача;
- інженерно-технічні заходи, що реалізуються поза межами ІКС Надавача;
- апаратно-технічне та програмне забезпечення захисту від несанкціонованого доступу до інформації, яка обробляється та зберігається в ІКС Надавача.

Розробка програмного забезпечення захисту інформації та оновлення його компонентів здійснюється безпосередньо від розробника. Завантаження з офіційних сайтів розробників дозволено.

Надавач отримує апаратні засоби комплексу засобів захисту безпосередньо від розробника, або в організацій, які мають відповідні ліцензії на впровадження комплексу засобів захисту комплексу технічних рішень.

6.6.2. Інструменти управління безпекою

Контроль за дотриманням вимог безпеки в ІКС Надавача здійснює служба захисту інформації Надавача, на яку покладено забезпечення захисту інформації.

Супровід роботи та обслуговування ІКС Надавача здійснюється адміністраторами відповідно до їх посадових обов'язків. Моніторинг інформації про стан роботи ІКС Надавача, такої як інформація про використання апаратних ресурсів, збої, відмови та проблеми в роботі програмного забезпечення та сервісів, здійснюється в автоматичному режимі. Адміністратори Надавача отримують повідомлення від системи моніторингу у разі виникнення/усунення аварійної ситуації.

6.6.3. Контроль безпеки протягом життєвого циклу

Надавач гарантує, що обладнання та робочі місця адміністраторів Надавача своєчасно модернізуються та мають останні оновлення безпеки.

6.7. Контроль безпеки мережі

Надавач виконує всі технічні дії для забезпечення захисту в ІКС Надавача відповідно до внутрішньої документації із захисту інформації, включаючи використання заходів безпеки для запобігання несанкціонованим та зловмисним діям у мережі, захист від мережевих атак, контроль підключень, перевірка та відстеження стану всіх мережевих підключень, сканування та аудит подій мережевого екрану, і всієї ІКС Надавача.

Міжмережевий екран призначений для захисту від мережевих атак зловмисників і обмеження доступу до ресурсів Надавача.

Програмний комплекс антивірусного захисту інформації, має чинний позитивний експертний висновок у сфері технічного захисту інформації, виданий Адміністрацією Державної служби спеціального зв'язку та захисту інформації України, та забезпечує захист ІКС Надавача від вірусів, шкідливих і небажаних програм.

6.8. Кваліфікована електронна позначка часу

6.8.1. Створення кваліфікованої електронної позначки часу

Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованої електронної позначки часу відповідає пункту 88 Вимог до надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання, затверджених постановою Кабінету Міністрів України від 28.06.2024 № 764.

Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає вчинення дій, передбачених частиною першою статті 26 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», з дотриманням вимог стандарту ETSI EN 319 421.

Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованої електронної позначки часу включає:

- створення кваліфікованої електронної позначки часу;
- передача кваліфікованої електронної позначки часу користувачу електронної довірчої послуги.

Кваліфікована електронна позначка часу передбачає презумпцію точності дати та часу, які вона вказує, а також цілісності електронних даних, з якими ця дата та час пов'язані.

Кваліфікована електронна позначка часу має відповідати таким вимогам:

- пов'язувати дату та час з електронними даними таким чином, щоб виключити можливість зміни електронних даних, які неможливо виявити;
- базуватися на точному джерелі часу, синхронізованому з всесвітнім координованим часом (UTC) з точністю до секунди;
- до кваліфікованої електронної позначки часу додається кваліфікований електронний підпис або створена для нього кваліфікована електронна печатка Надавача або може бути використаний інший спосіб, еквівалентний додаванню кваліфікованого електронного підпису чи кваліфікованої електронної печатки до кваліфікованої електронної позначки часу, за умови, що він забезпечує еквівалентний рівень безпеки кваліфікованій електронній позначці часу та відповідає вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Створення кваліфікованої електронної позначки часу здійснюється Надавачем за запитом користувача.

Під час створення кваліфікованої електронної позначки часу користувач і Надавач за допомогою захищеного носія особистого ключа виконують такі дії:

1) користувач обчислює геш-значення електронних даних, на яких має бути створена кваліфікована електронна позначка часу;

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

- обчислене геш-значення;
- ідентифікатор об'єкта (OID) політики створення позначки часу (необов'язково);
- ідентифікатор використовуваного алгоритму гешування;
- унікальний ідентифікатор запиту (опціонально);
- додаткові розширення;

3) користувач подає сформований запит до Надавача;

4) Надавач перевіряє правильність формату запиту та опрацьовує його, формує кваліфіковану електронну позначку часу та відповідь, що містить кваліфіковану електронну позначку часу, або відповідь з інформацією про відмову у створенні кваліфікованої електронної позначки часу;

5) Надавач надсилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, яка містить такі дані:

- ідентифікатор об'єкта (OID) політики створення кваліфікованої електронної позначки часу, яка була використана;
- геш-значення електронних даних, для яких створено кваліфіковану електронну позначку часу;
- порядковий номер кваліфікованої електронної позначки часу;
- час створення кваліфікованої електронної позначки часу;
- додаткову інформацію про кваліфіковану електронну позначку часу;
- кваліфікований електронний підпис або печатка Надавача, накладена на кваліфіковану електронну позначку часу;

6) після отримання відповіді від Надавача користувач здійснює такі дії:

- перевіряє результат обробки запиту;
- перевіряє відповідність назви або назви суб'єкта, який наклав кваліфікований електронний підпис чи печатку на кваліфіковану електронну позначку часу, найменуванню Надавача;
- перевіряє відповідність призначення сертифіката Надавача (для створення позначки часу);
- перевіряє дійсність сертифіката Надавача;
- перевіряє кваліфікований електронний підпис або печатку, накладену на кваліфіковану електронну позначку часу;

- перевіряє відповідність між електронними даними та даними, для яких створено кваліфіковану електронну позначку часу (шляхом порівняння обчисленого геш-значення електронних даних із геш-значенням, зафіксованим у кваліфікованій електронній позначці часу);
- додає кваліфіковану електронну позначку часу до електронних даних.

6.8.2. Перевірка кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу повинна забезпечувати:

- зв'язок дати та часу з електронними даними таким чином, що повністю виключає можливість непомітної зміни електронних даних;
- точність часу в програмно-технічному комплексі Надавача, який синхронізується з всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Перевірку кваліфікованої електронної позначки часу може здійснити будь-яка особа з метою отримання інформації про дійсність кваліфікованої електронної позначки часу.

Під час перевірки та підтвердження кваліфікованої електронної позначки часу особа, яка проводить перевірку, виконує такі дії:

- отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, що дає можливість однозначно встановити Надавача;
- перевіряє кваліфікований електронний підпис або печатку, накладену на кваліфіковану електронну позначку часу, з використанням чинного (на момент створення кваліфікованої електронної позначки часу) сертифіката Надавача;
- перевіряє відповідність між кваліфікованою електронною позначкою часу та електронними даними, до яких вона додається (шляхом порівняння обчисленого геш-значення електронних даних і геш-значення, записаного в кваліфікованій електронній позначці часу).

6.8.3. Недійсність кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу вважається недійсною, якщо:

- недотримані вимоги щодо точності часу в програмно-технічному комплексі Надавача
- використовується скасований або заблокований сертифікат Надавача під час створення кваліфікованої електронної позначки часу.

Правильність реалізації криптографічних алгоритмів створення кваліфікованої електронної позначки часу та точність часу в пристроях створення кваліфікованого електронного підпису чи печатки (QSCD) забезпечується протоколом фіксації часу.

6.8.4. Отримання кваліфікованої електронної позначки часу Надавачем

Надавач отримує кваліфіковану електронну довірчу послугу зі створення, перевірки та підтвердження кваліфікованої електронної позначки часу від Засвідчувального центра та/або ЦЗО.

Механізм синхронізації часу із всесвітнім координованим часом (UTC) у програмно-технічному комплексі Надавача та склад технічного обладнання, що використовується в процесі синхронізації часу (його загальний опис), встановлюються порядком Синхронізації часу з Всесвітнім координованим часом (UTC).

Порядок синхронізації часу з Всесвітнім координованим часом (UTC) розроблено Надавачем та погоджено з Засвідчувальним центром.

7. ПРОФІЛІ СЕРТИФІКАТУ, CRL ТА OCSP

7.1. Профіль сертифіката

Надавач формує кваліфіковані сертифікати наступних типів:

1) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем кваліфікованого електронного підпису фізичної особи та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірку та підтвердження кваліфікованого електронного підпису;
2) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем кваліфікованого електронного підпису фізичної особи, що представляє юридичну особу та підтверджує її ідентифікаційні дані під час автентифікації, дані юридичної особи та зв'язок між ними, а також створення, перевірку та підтвердження кваліфікованого електронного підпису;
3) кваліфікований сертифікат електронної печатки, який асоціюється з відкритим ключем кваліфікованої електронної печатки юридичної особи або фізичної особи – підприємця та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованої електронної печатки;
4) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем удосконаленого електронного підпису фізичної особи та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірку та підтвердження удосконаленого електронного підпису. Використовується в рамках послуги удосконаленого електронного підпису Надавача ;
5) кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем удосконаленого електронного підпису фізичної особи, що представляє юридичну особу та підтверджує її ідентифікаційні дані під час автентифікації, дані юридичної особи та зв'язок між ними, а також створення, перевірку та підтвердження удосконаленого електронного підпису;
6) кваліфікований сертифікат електронної печатки, який асоціюється з відкритим ключем удосконаленої електронної печатки юридичної особи або фізичної особи – підприємця та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження удосконаленої електронної печатки;
7) кваліфікованого сертифіката шифрування, який асоціюється з відкритим ключем фізичної особи, відповідний якому особистий ключ знаходиться в засобі КЕП та використовується для спрямованого шифрування під час обміну інформацією;
8) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи, що представляє юридичну особу, відповідний якому особистий ключ знаходиться в засобі КЕП, та використовується для спрямованого шифрування під час обміну інформацією;
9) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем печатки юридичної особи або фізичної особи – підприємця, відповідний якому особистий ключ знаходиться в засобі КЕП та використовується для спрямованого шифрування під час обміну інформацією;
10) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи та використовується для спрямованого шифрування під час обміну інформацією;
11) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи, що представляє юридичну особу та використовується для спрямованого шифрування під час обміну інформацією;
12) кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем печатки юридичної особи або фізичної особи – підприємця та використовується для спрямованого шифрування під час обміну інформацією;

N з/п	Ідентифікатор	Політика	Особа	Використання		
				Кваліфікований підпис	Удосконалений підпис	Шифрування
1	кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем кваліфікованого електронного підпису фізичної особи та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірку та підтвердження кваліфікованого електронного підпису;					
	0.4.0.194112.1.2	QCP-n-qscd	Фіз. особа	так	ні	ні
2	кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем кваліфікованого електронного підпису фізичної особи, що представляє юридичну особу та підтверджує її ідентифікаційні дані під час автентифікації, дані юридичної особи та зв'язок між ними, а також створення, перевірку та підтвердження кваліфікованого електронного підпису;					
	0.4.0.194112.1.2	QCP-n-qscd	Фіз. особа, що представляє юр. особу	так	ні	ні
3	кваліфікований сертифікат електронної печатки, який асоціюється з відкритим ключем кваліфікованої електронної печатки юридичної особи або фізичної особи – підприємця та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованої електронної печатки;					
	0.4.0.194112.1.3	QCP-l-qscd	Юр. особа	так	ні	ні
4	кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем удосконаленого електронного підпису фізичної особи та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірку та підтвердження удосконаленого електронного підпису. Використовується в рамках послуги удосконаленого електронного підпису "«Універсальний банк. Підпис» та послуги "монобанк";					
	0.4.0.194112.1.0	QCP-n-	Фіз. особа	ні	так	ні
5	кваліфікований сертифікат електронного підпису, який асоціюється з відкритим ключем удосконаленого електронного підпису фізичної особи, що представляє юридичну особу та підтверджує її ідентифікаційні дані під час автентифікації, дані юридичної особи та зв'язок між ними, а також створення, перевірку та підтвердження удосконаленого електронного підпису;					
	0.4.0.194112.1.0	QCP-n	Фіз. особа, що представляє юр. особу	ні	так	ні
6	кваліфікований сертифікат електронної печатки, який асоціюється з відкритим ключем удосконаленої електронної печатки юридичної особи або фізичної особи – підприємця та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження удосконаленої електронної печатки;					
	0.4.0.194112.1.1	QCP-l	Юр. особа	ні	так	ні
7	кваліфікованого сертифіката шифрування, який асоціюється з відкритим ключем фізичної особи, відповідний якому особистий ключ знаходиться в засобі КЕП та використовується для спрямованого шифрування під час обміну інформацією;					
	0.4.0.194112.1.2	QCP-n-qscd	Фіз. особа	ні	ні	так
8	кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи, що представляє юридичну особу, відповідний якому особистий ключ знаходиться в засобі КЕП, та використовується для спрямованого шифрування під час обміну інформацією;					
	0.4.0.194112.1.2	QCP-n-qscd	Фіз. особа, що представляє юр. особу	ні	ні	так
9	кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем печатки юридичної особи або фізичної особи – підприємця, відповідний якому особистий ключ знаходиться в засобі КЕП та використовується для спрямованого шифрування під час обміну інформацією;					

N з/п	Ідентифікатор	Політика	Особа	Використання		
				Кваліфікований підпис	Удосконалений підпис	Шифрування
	0.4.0.194112.1.3	QCP-l-qscd	Юр. особа	ні	ні	так
10	кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи та використовується для спрямованого шифрування під час обміну інформацією;					
	0.4.0.194112.1.0	QCP-n-	Фіз. особа	ні	ні	так
11	кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем фізичної особи, що представляє юридичну особу та використовується для спрямованого шифрування під час обміну інформацією;					
	0.4.0.194112.1.0	QCP-n	Фіз. особа, що представляє юр. особу	ні	ні	так
12	кваліфікований сертифікат шифрування, який асоціюється з відкритим ключем печатки юридичної особи або фізичної особи – підприємця та використовується для спрямованого шифрування під час обміну інформацією;					
	0.4.0.194112.1.1	QCP-l	Юр. особа	ні	ні	так

Кваліфіковані сертифікати, сформовані Надавачем, відповідають вимогам наступних стандартів:

- ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) «Інформаційні технології – Взаємозв'язок відкритих систем — Частина 8: Довідник: Структури сертифікатів відкритих ключів та атрибутів», затверджений наказом державного підприємства «Український науково-навчальний центр з проблем стандартизації, сертифікації та якості» від 16.12.2021 № 512.
- ДСТУ ETSI EN 319 412-1:2021 (ETSI EN 319 412-1 V1.4.4 (2021-05), IDT) «Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 1: Огляд і загальні структури даних», затв. наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16.12.2021 № 512.
- ДСТУ ETSI EN 319 412-2:2021 (ETSI EN 319 412-2 V2.2.1 (2020-07), IDT) «Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 2: Профіль сертифікатів для сертифікатів, виданих фізичним особам », затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16.12.2021 № 512.
- ДСТУ ETSI EN 319 412-3:2021 (ETSI EN 319 412-3 V1.2.1 (2020-07), IDT) «Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 3: Профіль сертифікатів для сертифікатів, виданих юридичним особам », затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16.12.2021 № 512.
- ДСТУ ETSI EN 319 412-5:2019 (ETSI EN 319 412-5 V2.2.1 (2017-11), IDT) «Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 5: QCStements», затверджений наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 27.12.2019 № 515.
- ДСТУ ETSI TS 119 312:2021 (ETSI TS 119 312 V1.4.1 (2021-08), IDT) «Електронні підписи та інфраструктури (ESI); Криптографічні комплекси», затверджений наказом ДП «Український науково-навчальний центр». з проблем стандартизації, сертифікації та якості» від 28.12.2021 № 550.

Поля та формат інформації, що міститься в кваліфікованому сертифікаті:

Найменування	**Значення**
Версія	Версія 3 (версія 3) стандарт X.509

Найменування	Значення
Серійний номер	Номер сертифіката Значення цього поля унікальне
Алгоритм підпису	Криптографічний алгоритм. Визначає алгоритм, який використовується для підписання кваліфікованого сертифіката
Видавець	Назва Надавача, який формує кваліфікований сертифікат
Діє з	Термін дії кваліфікованих сертифікатів (відповідно до стандарту RFC 5280)
Діє до	Термін дії кваліфікованих сертифікатів (відповідно до стандарту RFC 5280)
Суб'єкт	Інформація про одержувача сертифіката (відповідає RFC 5280) Докладніше див. у розділі 3.1.1
Відкритий ключ	Відкритий ключ, що відповідає особистому ключу кваліфікованого сертифіката (відповідає стандарту RFC 5280)
Підпис	Кваліфікований електронний підпис Надавача, що надає послугу створення, перевірки та підтвердження кваліфікованого електронного підпису або печатки. Згенеровано та закодовано відповідно до RFC 5280 . стандарт

Надавач може включати розширення використання ключа (Key Usage extensions) в сертифікати користувача, які визначають сферу використання сертифікатів:

- EmailProtection - захист електронної пошти;
- IpSecEndSystem - захист протоколу IPSEC;
- IpSecTunnel – захист тунельного режиму протоколу IPSEC;
- IpSecUser - захист IP-протоколу в користувальницькій програмі - зв'язування значення дайджесту з часом, наданим раніше та прийнятим надійним джерелом часу;
- ServerAuth - автентифікація TLS веб-сервера;
- ClientAuth - автентифікація TLS веб-клієнта;
- Інші.

Надавач може включати розширення сертифіката (certificate extensions) в сертифікати користувача, які визначають сферу використання сертифікатів:

- limitCurrency - обмеження валют, для яких може бути використаний сертифікат;
- limitAmount - обмеження сум операцій, для яких може бути використаний сертифікат;
- інші.

7.2. Профіль CRL

Поширення інформації про статус кваліфікованих сертифікатів користувача здійснюється шляхом створення можливості перевірки статусу кваліфікованого сертифіката користувача в режимі реального

часу через мережі електронного зв'язку загального користування за протоколом OCSP та шляхом публікації CRL.

Посилання на CRL вносяться у всі кваліфіковані сертифікати користувачів.

CRL, сформовані Надавачем, відповідають вимогам RFC 5280 «Сертифікат інфраструктури відкритих ключів Інтернету X.509 і профіль відкликаних сертифікатів (CRL)».

Формат інформації в CRL, опублікованому Надавачем, відповідає стандарту ITU-T X.509 та регламенту RFC 5280. CRL мають принаймні такі поля:

Найменування	Значення
Версія	Версія CRL (версія 2).
Видавець	Назва постачальника, який видає CRL.
Дата набрання чинності	Поточна дата випуску (оновленої) CRL.
Наступне оновлення	Дата наступного (майбутнього) оновлення CRL
Відкликані сертифікати	Це поле містить інформацію про відкликані кваліфіковані сертифікати, зокрема: - серійний номер відкликаного кваліфікованого сертифіката; - дата та час скасування кваліфікованого сертифіката; - запис про скасування (розширену інформацію скасованого кваліфікованого сертифіката)
Алгоритм підпису	Алгоритм, який використовується для підписання CRL
Алгоритм гешування	Алгоритм гешування
Підпис	Значення електронного підпису Надавача
Розширення CRL	Інша розширена інформація (необов'язкове поле)

7.3. Профіль OCSP

Посилання на сервіс перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу вносяться у всі кваліфіковані сертифікати користувачів.

Процедура інтерактивного визначення статусу сертифіката та форматів даних відповідає вимогам наступних стандартів:

- ISO/IEC 8825-1:2002 «Інформаційна технологія - Правила кодування ASN.1 - Частина 1: Специфікація основних правил кодування (BER), правил канонічного кодування (CER) і правил відмінного кодування (DER).
- RFC 2560 "Інфраструктура відкритих ключів Інтернету X.509 Онлайновий протокол статусу сертифіката - OCSP".

8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

8.1. Аудит відповідності та інші оцінки

Для доведення відповідності вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, які вони надають, Надавач проходить процедуру оцінки відповідності у сфері електронних довірчих послуг з залученням іноземного органу з оцінки відповідності, акредитованого відповідно іноземним органом з акредитації, що є підписантом багатосторонньої угоди про визнання Міжнародного форуму з акредитації та/або Європейської кооперації з акредитації (EA MLA).

Надавач використовує кваліфіковані засоби кваліфікованого електронного підпису та печатки, які мають чинний експертний висновок, зареєстрований Адміністрацією Державної служби спеціального зв'язку за результатами Державної експертизи у сфері криптографічного захисту інформації.

В подальшому Надавач має намір використовувати кваліфіковані засоби електронного підпису, що мають сертифікат відповідності вимогам національних стандартів в сфері довірчих послуг.

Регламент роботи Надавача погоджено Засвідчувальним центром.

Результати оцінки відповідності Надавача у сферах електронної ідентифікації та електронних довірчих послуг будуть аналізуватися Засвідчувальним центром та контролюючим органом, функції якого здійснює Адміністрація Державної служби спеціального зв'язку та захисту інформації України. У разі негативних результатів оцінки відповідності та/або наданих органом з оцінки відповідності рекомендацій, Засвідчувальний центр та/або контролюючий орган може своїм рішенням призначити додаткову оцінку відповідності після усунення всіх недоліків, зазначених в аудиторському звіті.

Контролюючий орган уповноважений здійснювати такі заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг:

- перевірка Надавача за його заявою;
- перевірка Надавача у разі виявлення та підтвердження наявності недостовірних відомостей у поданих ними документах;
- перевірка Надавача після отримання інформації чи повідомлення про порушення вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг від засвідчувального центру, ЦЗО, суду, користувачів електронних довірчих послуг або третіх осіб;
- перевірка Надавача за обґрунтованим рішенням контролюючого органу.

8.2. Частота або обставини оцінки відповідності

Надавач проводить оцінку відповідності електронних довірчих послуг кожні два роки. Оцінка відповідності засобів кваліфікованого електронного підпису та печатки здійснюється відповідно до термінів дії сертифікатів відповідності.

8.3. Особа/кваліфікація оцінювача

Надавач проводить внутрішні аудити за допомогою співробітників і підрядника, який виконує роль незалежного аудитора.

8.3.1. Вимоги до кваліфікації контролюючого органу (КО)

Функції КО виконує Державна служба спеціального зв'язку та захисту інформації України.

Виїзний плановий або позаплановий захід державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг (далі - перевірка) здійснюється посадовими особами КО відповідно до їх функціональних обов'язків за місцезнаходженням надавача.

Перевірка здійснюється відповідно до рішення КО.

Рішення щодо проведення перевірки повинно містити:

1) найменування КО;
2) найменування Надавача,
3) місцезнаходження Надавача;
4) підставу для проведення перевірки;
5) предмет перевірки;
6) дати початку та закінчення перевірки;
7) посадовий та персональний склад комісії з перевірки.

8.3.2. Вимоги до кваліфікації органу з оцінки відповідності (ООВ)

ООВ - це підприємство, установа, організація чи її структурний підрозділ, що провадить діяльність з оцінки відповідності у сфері електронних довірчих послуг та акредитований національним органом з акредитації або іноземним органом з акредитації, який є підписантом багатосторонньої угоди про визнання Міжнародного форуму з акредитації та/або Європейської кооперації з акредитації (EA MLA).

ООВ повинен мати відповідну компетенцію для здійснення оцінки відповідності щодо підтвердження відповідності вимогам до надавачів та послуг, що ними надаються.

ООВ повинен дотримуватися положень, визначених у стандарті ДСТУ ETSI EN 319 403-1:2021 (ETSI EN 319 403-1 V2.3.1 (2020-06), IDT) «Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг», затвердженому наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16 грудня 2021 р. № 512.

8.4. Відносини оцінювача з суб’єктом оцінки

Зовнішній аудит виконується Органом оцінки відповідності в сфері довірчих послуг, який:

- є незалежним від власників, управління та операцій Надавача;
- є незалежним від Надавача, а саме ні він сам, ні його чи її найближчі родичі не мають жодних трудових чи ділових відносин з Надавачем.
- винагорода не залежить від результатів діяльності, проведеної під час аудиту.

Проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг здійснюється в порядку, затвердженому Кабінетом Міністрів України.

8.4.1. Відносини посадових осіб контролюючого органу (КО) з об'єктом оцінки

Відповідно до частини шостої статті 4 Закону України “Про основні засади державного нагляду (контролю) у сфері господарської діяльності” посадовій особі органу державного нагляду (контролю) забороняється здійснювати державний нагляд (контроль) щодо суб'єктів господарювання, з якими (або із службовими особами яких) посадова особа перебуває в родинних стосунках, або в разі виникнення у неї конфлікту інтересів згідно із законодавством у сфері запобігання і протидії корупції.

Члени комісії з перевірки зобов'язані:

- об'єктивно та неупереджено проводити перевірку;
- дотримуватися вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг, захисту інформації та захисту персональних даних;
- сумлінно, вчасно та якісно виконувати свої службові обов'язки та доручення голови комісії з перевірки;

- дотримуватися ділової етики у взаємовідносинах з керівником та працівниками Надавача;
- ознайомлювати керівника Надавача чи уповноваженого ним представника з результатами перевірки;
- надавати Надавачу консультаційну допомогу з питань проведення перевірки;
- не розголошувати інформацію з обмеженим доступом, яка стала їм відома у зв'язку з виконанням службових обов'язків.

8.4.2. Відносини експертів (аудиторів), що проводять оцінку відповідності, з об'єктом оцінки

Експерти (аудитори), що проводять оцінку відповідності, повинні бути незалежними та не мати спільних ділових інтересів та жодного ділового зв'язку з Надавачем.

8.5. Теми, охоплені оцінюванням

Орган оцінки відповідності проводить зовнішній аудит для оцінки відповідності цьому документу, вимогам законодавства, вимогам Національного банку України, вимогам національних та європейських стандартів у сфері електронних довірчих послуг.

8.5.1. Питання, що підлягають перевірці під час державного контролю

Предметом перевірки, що проводиться КО є стан дотримання вимог законодавства у сфері електронних довірчих послуг, у тому числі цієї Політики сертифікатів та Положення сертифікаційних практик за такими питаннями:

- загальні вимоги;
- забезпечення безпеки інформаційних ресурсів;
- кадрові ресурси;
- експлуатація засобів кваліфікованого електронного підпису чи печатки;
- вимоги до надання електронних довірчих послуг;
- політика сертифікатів;
- положення сертифікаційних практик;
- надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток;
- забезпечення безпеки фізичного доступу до приміщень.

8.5.2. Питання, що підлягають перевірці під час оцінки відповідності

Предметом оцінки відповідності, що проводиться ООВ, є стан дотримання вимог стандартів ДСТУ ETSI EN 319 403:2016 “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності провайдерів довірчих послуг. Вимоги до органів з оцінювання відповідності, що оцінюють провайдерів довірчих послуг” (ETSI EN 319 403:2015, IDT.

8.6. Дії, що вживаються внаслідок виявлення порушень

Надавач вживає заходів щодо усунення проблем, виявлених незалежним аудитом, у письмовій формі, повідомляючи про заходи, вжиті для їх запобігання під час наступної перевірки органом оцінки відповідності.

Результати оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг аналізуються Контролюючим органом. У разі негативних результатів оцінки відповідності та/або наданих органом з оцінки відповідності рекомендацій Контролюючий орган може своїм рішенням

призначити додаткову оцінку відповідності після усунення всіх недоліків, зазначених в аудиторському звіті.

Контролюючий орган має повноваження приймати рішення щодо проведення перевірки дотримання законодавства в сфері довірчих послуг Надавача. За результатами перевірки Контролюючий орган приймає рішення щодо відповідності чи невідповідності діяльності Надавача.

В разі складання Контролюючим органом за результатами перевірки Припису про усунення порушень Надавач зобов'язується вжити заходів щодо усунення недоліків та порушень, зазначених у приписі про усунення порушень, протягом визначеного у приписі строку.

8.6.1. Дії, що вживаються внаслідок порушення, виявленого за результатами державного контролю

Посадові особи КО під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг мають право, зокрема:

- у разі виявлення порушення вимог законодавства видавати обов'язкові для виконання приписи про усунення порушень і визначати строк усунення виявлених порушень;

- накладати на винних осіб адміністративні стягнення за порушення вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги" та нормативно-правових актів, прийнятих на виконання цього Закону;

- звертатися до суду щодо застосування заходів реагування.

За результатами проведення перевірок КО вживає таких заходів реагування:

1) вимагає усунення порушень вимог законодавства у сфері електронних довірчих послуг у встановлений приписом строк;

2) приймає рішення про блокування кваліфікованого сертифіката Надавача, якщо під час перевірки виникла підозра компрометації особистого ключа;

3) приймає рішення про скасування кваліфікованого сертифіката надавача, якщо під час перевірки виявлено факт компрометації особистого ключа.

Рішення про блокування або скасування кваліфікованого сертифіката Надавача, КО надсилає в день його прийняття до Засвідчувального центру;

4) надсилає до Засвідчувального центру подання про скасування статусу Надавача або послуги, яку надає Надавач, у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг Надавачем без чинних документів, визначених законодавством, що підтверджують відповідність комплексної системи захисту інформації ІКС Надавача та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг;
- непроходження додаткової державної експертизи комплексної системи захисту інформації або процедури оцінки відповідності ІКС Надавача у разі модернізації апаратного, апаратно-програмного пристрою чи програмного забезпечення, що входять до складу програмно-технічного комплексу, яка не передбачена проектною чи експлуатаційною документацією до комплексної системи захисту інформації та/або системи управління інформаційною безпекою ІКС Надавача;
- надання кваліфікованих електронних довірчих послуг за відсутності у Надавача поточного рахунку із спеціальним режимом використання у банку (рахунок у Національному банку України - для банків - кваліфікованих надавачів електронних довірчих послуг, кваліфікованого надавача електронних довірчих послуг, створеного Національним банком України) з необхідним обсягом коштів або чинного договору страхування цивільно-правової відповідальності з необхідним розміром страхової суми, що встановлені Законом України "Про

електронну ідентифікацію та електронні довірчі послуги", для забезпечення відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг або третім особам внаслідок неналежного виконання Надавачем своїх зобов'язань;

- порушення вимог до умов експлуатації комплексної системи захисту інформації або СУІБ ІКС Надавача;
- надання кваліфікованих електронних довірчих послуг Надавачем без чинних документів, визначених законодавством, що підтверджують його право власності та/або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються для надання кваліфікованих електронних довірчих послуг;
- встановлення факту надання недостовірних відомостей, наведених у документах, поданих Надавачем для внесення відомостей про нього до Довірчого списку;
- неусунення виявлених під час перевірки порушень у встановлений приписом строк;
- блокування або скасування кваліфікованого сертифіката Надавача.

8.6.2. Дії, що вживаються внаслідок порушення, виявленого за результатами оцінки відповідності

У разі прийняття рішення про невідповідність об’єкта оцінки відповідності вимогам у сфері електронних довірчих послуг ООВ видає замовнику процедури оцінки відповідності аудиторський звіт з висновками про невідповідність з переліком порушень.

КО надсилає до Засвідчувального центру подання про скасування статусу Надавача або послуги, яку надає Надавач, у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг Надавачем без чинних документів, визначених законодавством, що підтверджують відповідність комплексної системи захисту інформації та/або системи управління інформаційною безпекою ІКС Надавача та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг;
- непроходження додаткової державної експертизи комплексної системи захисту інформації або процедури оцінки відповідності ІКС Надавача у разі модернізації апаратного, апаратно-програмного пристрою чи програмного забезпечення, що входять до складу програмно-технічного комплексу, яка не передбачена проектною чи експлуатаційною документацією до комплексної системи захисту інформації та/або системи управління інформаційною безпекою ІКС Надавача.

8.7. Повідомлення результатів

8.7.1. Оформлення результатів державного контролю

Результати проведення перевірки Надавача оформлюються комісією з перевірки шляхом складення акту перевірки, форма якого затверджується КО.

Акт перевірки має містити такі відомості:

- найменування КО;
- персональний та посадовий склад комісії з перевірки;
- прізвище та ініціали керівника Надавача;
- реквізити посвідчення на проведення перевірки;
- дати початку і закінчення перевірки;
- адреса приміщень Надавача, в яких проводилася перевірка;
- результати попередньої перевірки;
- інформація про результати останньої оцінки відповідності у сфері електронних довірчих послуг, що передує перевірці;

- назва та короткий зміст документів, наданих під час перевірки;
- якісні та кількісні показники, встановлені під час перевірки, що характеризують діяльність Надавача, пов'язану з наданням електронних довірчих послуг;
- виявлені під час перевірки порушення і недоліки (за наявності) та пояснення Надавача про причини невиконання встановлених законодавством вимог (за наявності);
- висновки за результатами перевірки;
- факти протидії проведенню перевірки (за наявності);
- рекомендації щодо усунення виявлених порушень (у разі наявності);
- дата складення акту перевірки;
- підписи голови та членів комісії з перевірки;
- підпис керівника Надавача чи уповноваженого ним представника, що підтверджує факт ознайомлення з актом перевірки.

Акт перевірки складається у двох примірниках та підписується не пізніше останнього дня її проведення головою та всіма членами комісії з перевірки і керівником Надавача чи уповноваженим ним представником.

Член комісії з перевірки, який не погоджується з висновками комісії з перевірки, зазначеними в акті перевірки, зобов'язаний підписати його та письмово викласти свою окрему думку, що додається до акту перевірки. При цьому перед підписом акту перевірки зазначається "З окремою думкою, що додається".

Якщо керівник Надавача чи уповноважений ним представник має зауваження щодо фактів та висновків, викладених в акті перевірки, перед підписом зазначається "Із зауваженнями, що додаються".

Зауваження до акту перевірки оформлюються окремим документом та підписуються керівником Надавача чи уповноваженим ним представником.

Зауваження до акту перевірки та окрема думка члена комісії з перевірки є невід'ємними частинами акту перевірки.

Якщо керівник Надавача чи уповноважений ним представник відмовився від ознайомлення з актом перевірки або від його підписання після ознайомлення з ним, голова комісії з перевірки перед місцем для підпису керівника Надавача чи уповноваженого ним представника робить відповідне зазначення, яке засвідчується підписами голови та одного з членів комісії з перевірки.

8.7.2. Припис про усунення порушень, виявлених під час державного контролю

Посадові особи КО під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг мають право у разі виявлення порушення вимог законодавства у сфері електронних довірчих послуг видавати обов'язкові для виконання приписи про усунення порушень і визначати строк усунення виявлених порушень.

Припис про усунення порушень складається комісією з перевірки у двох примірниках протягом п'яти робочих днів після завершення перевірки. Один примірник припису не пізніше п'яти робочих днів з дня складення акту перевірки надається надавачу, а другий примірник з підписом керівника Надавача чи уповноваженого ним представника щодо погоджених строків усунення порушень вимог законодавства у сфері електронних довірчих послуг залишається у КО.

Форма припису про усунення порушень затверджується КО.

Припис про усунення порушень підписується головою та членами комісії з перевірки, які їх проводили.

У разі якщо керівник Надавача чи уповноважений ним представник відмовився від отримання припису про усунення порушень, такий припис надсилається рекомендованим листом, а на копії припису, що залишається у КО, проставляються відповідний вихідний номер і дата надсилання.

Керівник Надавача повинен вжити заходів до усунення недоліків та порушень, зазначених у приписі про усунення порушень, протягом визначеного у приписі строку.

Надавач зобов'язаний у визначений у приписі про усунення порушень строк письмово подати до КО інформацію про усунення порушень разом з підтвердними документами.

8.7.3. Оформлення результатів оцінки відповідності

Документ про відповідність повинен містити такі відомості:

- найменування ООВ;
- інформацію про акредитацію ООВ (дата та номер атестата про акредитацію);
- прізвище, ім'я, по батькові (у разі наявності) осіб, що проводили процедуру оцінки відповідності;
- період проведення процедури оцінки відповідності;
- реквізити Надавача (найменування, ідентифікаційні дані та контактна інформація);
- сфера оцінки відповідності;
- перелік кваліфікованих електронних довірчих послуг, які має намір надавати Надавач;
- найменування ІКС;
- найменування засобів кваліфікованого електронного підпису, які використовуються під час надання кваліфікованих електронних довірчих послуг;
- перелік вимог у сфері електронних довірчих послуг, національних стандартів та/або технічних специфікацій, щодо відповідності яким проводилася процедура оцінка відповідності;
- висновок щодо відповідності вимогам у сфері електронних довірчих послуг;
- строк дії документа про відповідність.

Про результати проведення процедури планової та повторної (позапланової) оцінки відповідності у сфері електронних довірчих послуг Надавач повинен повідомити КО шляхом надання копій документів про відповідність (за наявності) та аудиторських звітів не пізніше трьох робочих днів з дня їх отримання.

ООВ надає публічний доступ до актуальної інформації про результати оцінки відповідності у сфері електронних довірчих послуг.

8.8. Самоаудити

Протягом періоду формування сертифікатів, Надавач контролює дотримання цієї Політики сертифікатів та Положення сертифікаційних практик, суворо контролюючи якість своїх послуг, час від часу виконуючи самоперевірки, виданих сертифікатів.

Надавач проводить регулярні внутрішні аудити, щоб оцінювати дотримання вимог законодавства, внутрішньої політики та вимог цієї Політики сертифікатів та Положення сертифікаційних практик щонайменше раз на рік.

9. ІНШІ ДІЛОВІ ТА ЮРИДИЧНІ ПИТАННЯ

9.1. Оплата довірчих послуг

9.1.1. Плата за формування сертифіката

Розмір та порядок оплати за надання електронних довірчих послуг може встановлюватись згідно з правилами Надавача та Договору про надання кваліфікованих електронних довірчих послуг. Інформація про вартість послуг міститься в тарифних планах надання кваліфікованих електронних довірчих послуг Надавача, опублікованих на веб-сайті Надавача https://ca.monobank.ua/.

У разі надання кваліфікованих електронних довірчих послуг через відокремлені пункти реєстрації Надавача може стягуватися додаткова плата за надання кваліфікованих електронних довірчих послуг.

Поновлення заблокованих кваліфікованих сертифікатів здійснюється безкоштовно.

9.1.2. Плата за доступ до сертифіката

Плата за доступ до кваліфікованого сертифіката не стягується.

9.1.3. Плата за блокування/скасування або доступ до інформації про статус сертифіката

Плата за блокування/скасування кваліфікованого сертифіката або доступ до інформації про статус кваліфікованого сертифіката не стягується.

9.1.4. Плата за інші послуги

Надавач може надавати користувачам додаткові послуги. Перелік таких послуг та розмір оплати за них розміщується на веб-сайті https://ca.monobank.ua/.

9.1.5. Політика відшкодування

Надавач не відшкодовує оплачені рахунки, за якими були надані послуги.

9.2. Фінансова відповідальність

Надавач несе фінансову відповідальність згідно з вимогами частини п'ятої статті 16 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» щодо надання кваліфікованих електронних довірчих послуг шляхом внесення коштів на поточний рахунок із особливим режимом використання в банку (рахунок у Національному банку України - для банків - кваліфікованих надавачів електронних довірчих послуг, кваліфікованого надавача електронних довірчих послуг, створеного Національним банком України) або страхування цивільної відповідальності для забезпечення відшкодування шкоди, яка може бути заподіяна користувачам таких послуг або третім особам.

9.3. Конфіденційність ділової інформації

9.3.1. Обсяг конфіденційної інформації

У процесі надання послуг Надавач обробляє конфіденційну інформацію, яка не оприлюднюється для загального ознайомлення. Захист конфіденційної інформації здійснюється відповідно до чинного законодавства.

9.3.2. Неконфіденційна інформація

Інформація та документація, яка є доступною для загального ознайомлення, оприлюднюється на веб-сайті Надавача та не відноситься до конфіденційної інформації.

9.3.3. Відповідальність за захист конфіденційної інформації

Надавач здійснює захист, зберігає конфіденційну інформацію та несе відповідальність згідно з вимогами чинного законодавства.

9.4. Конфіденційність персональних даних

Обробка персональних даних Клієнтів Надавача здійснюється згідно Політики захисту персональних даних Надавача яка публікується у відкритому доступі на веб-сайті Надавача.

Політика захисту персональних даних Надавача розроблена відповідно до вимог Закону України «Про захист персональних даних», з урахуванням положень Регламенту Європейського Союзу (ЄС) 2016/679 (GDPR) та рекомендацій стандарту ДСТУ ISO/IEC 27701:2022 Методи забезпечення безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 щодо управління конфіденційною інформацією. Вимоги та настанови (ISO/IEC 27701:2019, IDT).

9.4.1. Поняття захисту персональних даних

Надавач у процесі надання кваліфікованих електронних довірчих послуг здійснює:

- захист персональних даних користувачів відповідно до вимог Закону України «Про захист персональних даних»;
- інформування керівництва АТ «УНІВЕРСАЛ БАНК» та, у разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливає на надання кваліфікованих електронних довірчих послуг або стосується персональних даних користувачів, не пізніше ніж протягом 24 годин з моменту, коли йому стало відомо про таке порушення;
- інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливає на надання їм кваліфікованих електронних довірчих послуг або стосується їх персональних даних, невідкладно, але не пізніше двох годин з моменту, коли йому стало відомо про таке порушення.

9.4.2. Визначення персональних даних

Термін «персональні дані» розуміється у значенні, наведеному у статті 2 Закону України «Про захист персональних даних».

9.4.3. Конфіденційність персональних даних

Персональні дані можуть відноситися до відкритої інформації у випадках, визначених чинним законодавством.

9.4.4. Відповідальність за захист персональних даних

Надавач гарантує дотримання вимог законодавства про захист персональних даних та несе відповідальність згідно з вимогами чинного законодавства.

Керівник Надавача забезпечує створення умов для безперервної особистісної освіти та постійного підвищення кваліфікації персоналу Надавача у сферах інформаційних технологій, захисту інформації та персональних даних.

9.4.5. Інформація та згода на використання персональних даних

Відповідно до Закону України «Про захист персональних даних», користувач, підписуючи заяву про приєднання до Публічного договору про надання кваліфікованих електронних довірчих послуг, надає Надавачу згоду на обробку його своїх персональних даних в рамках надання кваліфікованих електронних довірчих послуг.

9.4.6. Розкриття персональних даних

Надавач надає доступ до персональних даних користувачів лише у випадках, передбачених Законом України «Про захист персональних даних».

Керівник Надавача та персонал Надавача дотримуються вимог законодавства України у сфері захисту персональних даних та укладають договір про конфіденційність та нерозголошення інформації.

9.5. Права інтелектуальної власності

Відносини в сфері прав інтелектуальної власності Надавача регулюються відповідно до вимог чинного законодавства України.

9.6. Зобов’язання та гарантії

9.6.1. Зобов’язання та гарантії Надавача

Надавач надає кваліфіковані електронні довірчі послуги відповідно до вимог законодавства у сфері електронних довірчих послуг, цієї Політики сертифікатів та Положення сертифікаційних практик та інших процедур Надавача.

9.6.2. Зобов'язання та гарантії відокремлених пунктів реєстрації

На підставі договору, укладеного з АТ "УНІВЕРСАЛ БАНК", реєстрація користувачів здійснюється окремими реєстраційними пунктами Надавача, які виконують свої функції відповідно до цієї Політики сертифікатів та Положення сертифікаційних практик.

До працівників відокремлених пунктів реєстрації Надавача, які відповідають за реєстрацію користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації Надавача.

9.6.3. Обов'язки та гарантії користувачів

Надавач надає можливість користувачам підписувати та перевіряти підписані файли за допомогою віджетів для підписання та перевірки підписів, а також за допомогою спеціалізованого програмного забезпечення, розташованого на веб-сайті https://ca.monobank.ua/

Користувачі зобов'язані:

- забезпечувати конфіденційність і неможливість доступу інших осіб до особистого ключа;
- негайно повідомити Надавача про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату електронних довірчих послуг, якщо така оплата передбачена договором між Надавачем та користувачем;
- своєчасно надавати Надавачу інформацію про зміну ідентифікаційних даних, що містяться у кваліфікованому сертифікаті;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування чи блокування кваліфікованого сертифіката.

Користувач гарантує, що:

- для підпису використовує особистий ключ, який відповідає відкритому ключу в кваліфікованому сертифікаті;
- на момент підписання кваліфікований сертифікат є дійсним (не перебуває у статусі блокованого чи скасованого);

- особистий ключ і пароль до нього не скомпрометовані та не використовуються іншими особами;
- вся інформація, зазначена в кваліфікованому сертифікаті, є вірною;
- кваліфікований сертифікат використовується за призначенням, відповідно до положень цієї Політики сертифікатів та Положення сертифікаційних практик;
- до договору про надання кваліфікованих електронних довірчих послуг можуть бути включені додаткові умови. Зміст договору про надання кваліфікованих електронних довірчих послуг оприлюднено на сайті Надавача.

9.6.4. Зобов'язання та гарантії довіряючих сторін

Довіряюча сторона перед використанням кваліфікованого сертифіката повинна перевірити дійсність кваліфікованого сертифіката, виданого Надавачем, використовуючи послуги перевірки та підтвердження електронного підпису або печатки.

9.6.5. Зобов'язання та гарантії інших учасників

Перед прийняттям рішення про внесення Надавача до Довірчого списку та надання йому кваліфікованого статусу, Засвідчувальний центр переконався, що Надавач має:

- сертифікат відповідності комплексної системи захисту інформації вимогам нормативних документів у сфері захисту інформації або документи про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг;
- документи, що підтверджують право власності та право користування нежитловими приміщеннями Надавача, які використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання кваліфікованих електронних довірчих послуг;
- відповідний персонал Надавача;
- документи, що підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи (до окремих працівників) за фахом персоналу Надавача;
- документи, що підтверджують право власності або право користування засобами створення кваліфікованого електронного підпису чи печатки, які використовуються Надавачем для надання кваліфікованих електронних довірчих послуг;
- документи, що підтверджують внесення коштів на поточний рахунок Надавача зі спеціальним режимом використання в банку (рахунок у Національному банку України - для банків - кваліфікованих надавачів електронних довірчих послуг, кваліфікованого надавача електронних довірчих послуг, створеного Національним банком України) для відшкодування збитків, які можуть бути завдані користувачам внаслідок неналежного виконання Надавача своїх зобов'язань;
- цю Політику сертифікатів та Положення сертифікаційних практик;
- відомості про відокремлені пункти реєстрації та їх працівників, обов’язки яких будуть безпосередньо пов’язані з наданням кваліфікованих електронних довірчих послуг.

9.7. Відмова від гарантій

Надавач не надає жодних гарантій щодо послуг, що надаються ним, за винятком тих, які чітко визначені в п. 9.6.1 цієї Політики сертифікатів та Положення сертифікаційних практик.

9.8. Обмеження відповідальності

У разі, якщо Надавач заздалегідь належним чином інформує користувачів про обмеження щодо використання кваліфікованих електронних довірчих послуг, які він надає, за умови, що такі обмеження зрозумілі користувачам, він не несе відповідальності за шкоду, заподіяну внаслідок використання кваліфікованих електронних довірчих послуг з порушенням зазначених обмежень.

9.9. Відшкодування

Відшкодування збитків, які можуть бути завдані користувачам кваліфікованих електронних довірчих послуг або третім особам внаслідок неналежного виконання Надавачем своїх зобов'язань, здійснюється відповідно до вимог чинного законодавства України.

9.10. Термін дії та припинення

Ця Політика сертифікатів та Положення сертифікаційних практик діє з моменту її публікації та до закінчення терміну дії останнього сертифіката, виданого відповідно до цієї Політики сертифікатів та Положення сертифікаційних практик, або до припинення діяльності Надавача.

9.11. Індивідуальні повідомлення та спілкування з учасниками інфраструктури відкритих ключів

Надавач спілкується з учасниками інфраструктури відкритих ключів (PKI) шляхом:

- розміщення повідомлень та оголошень на веб-сайті Надавача;
- інформування Засвідчувального центру та/або Центрального засвідчувального органу, Контролюючого органу та Уповноваженого Верховної Ради України з питань прав людини, шляхом надсилання повідомлень у паперовій та електронній формах;
- відправки листів на електронну адресу користувача;
- здійснення телефонних дзвінків на номер телефону користувача;
- надсилання Push-повідомлень користувачам.

9.12. Зміни

Зміни до цієї Політики сертифікатів та Положення сертифікаційних практик вносяться Надавачем у разі:

- зміни вимог, процесів і процедур, описаних у цій Політиці сертифікатів та Положення сертифікаційних практик;
- зміни в законодавстві;
- зміни вимог до кваліфікованих надавачів електронних довірчих послуг щодо надання послуг.

Нові редакції цієї Політики сертифікатів та Положення сертифікаційних практик, після внесення до неї змін, оприлюднюються на веб-сайті Надавача.

Будь-які поправки, не зазначені в історії цієї Політики сертифікатів та Положення сертифікаційних практик, є граматичними та орфографічними змінами, які не впливають на суть або процеси та процедури, описані в цій Політиці сертифікатів та Положення сертифікаційних практик.

9.13. Процедури вирішення спорів

У разі виникнення суперечок або розбіжностей Надавач вирішує їх шляхом переговорів та консультацій з учасниками PKI.

У разі недосягнення згоди учасниками PKI, спори (розбіжності) вирішуються в судовому порядку відповідно до чинного законодавства України.

9.14. Регулююче право

На відносини, які регулюються цією Політикою сертифікатів та Положенням сертифікаційних практик, поширюється чинне законодавство України.

9.15. Відповідність чинному законодавству

Під час надання кваліфікованих електронних довірчих послуг Надавач повинен дотримуватись вимог нормативних актів:

- Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (Назва Закону в редакції Закону № 2801-IX від 01.12.2022);
- Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»;
- Положення про кваліфікованих надавачів електронних довірчих послуг, унесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19.09.2019 № 116, зі змінами та доповненнями;
- Вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28.06.2024 № 764;
- Переліку документів та електронних даних, отриманих у зв'язку з наданням електронних довірчих послуг, що підлягають постійному зберіганню, затвердженого постановою Кабінету Міністрів України від 23.07.2024 № 842;
- Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 23.07.2024 № 842;
- Таблиці транслітерації українського алфавіту латиницею, затвердженої постанови Кабінету Міністрів України від 27.01.2010 № 55, зі змінами та доповненнями;
- Положення про синхронізацію часу у програмно-технічних комплексах кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 24.12.2019 № 153;
- Положення про здійснення банками фінансового моніторингу, затвердженого постановою Правління Національного банку України від 19.05.2020 № 65, зі змінами та доповненнями;
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28.09.2017 № 95;
- Положення про організацію внутрішнього аудиту в банках України, затвердженого Постановою Правління Національного банку України від 10.05.2016 № 311, зі змінами та доповненнями (далі - Положення НБУ № 311);
- інших актів законодавства України у сфері електронних довірчих послуг.