ПОГОДЖЕНО
Заступник Голови Державної служби спеціального зв'язку та захисту інформації України

Олександр ПОТІЙ

«12» 01 2022 р.

ЗАТВЕРДЖУЮ
Директор ТОВ «АРТ-МАСТЕР»

Вікторія КОВАЛЬСЬКА

«19» 01 2022 р.

РЕГЛАМЕНТ РОБОТИ

Кваліфікованого Надавача електронних довірчих послуг «MASTERKEY»
ТОВ «АРТ-МАСТЕР»

Київ-2022

ЗМІСТ

1. ПОЗНАЧКИ ТА СКОРОЧЕННЯ

ВПР	-	відокремлений (віддалений) пункт реєстрації;
ВЗІ	-	відповідальний за захист інформації
ЕДП	-	електронна довірча послуга;
ЄДР	-	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань;
ЄДДР	-	Єдиний державний демографічний реєстр;
ЄДРПОУ	-	Єдиний державний реєстр підприємств та організацій України;
ІТС	-	інформаційно-телекомунікаційна система;
КЕП	-	кваліфікований електронний підпис чи електронні печатка;
КЗІ	-	криптографічній захист інформації;
КСЗІ	-	комплексна система захисту інформації;
НД ТЗІ	-	нормативний документ з технічного захисту інформації;
НКІ	-	носій ключової інформації - засіб кваліфікованого електронного підпису чи печатки, у вигляді апаратно-програмного або апаратного пристрою, який реалізує функцію захищеного зберігання особистого ключа кваліфікованого електронного підпису чи печатки;
ПІБ	-	прізвище ім’я по батькові;
ПЗ	-	програмне забезпечення;
ПТК	-	програмно-технічний комплекс;
РРО	-	реєстратор розрахункових операцій;
РС	-	робоча станція;
РНОКПП	-	реєстраційний номер облікової картки платника податків;
СВС	-	список відкликаних сертифікатів;
СЗІ	-	служба захисту інформації;
СКБД	-	система керування базами даних;
СПЗ	-	спеціалізоване програмне забезпечення;
ОС	-	операційна система;
УЕП	-	удосконалений електронний підпис чи електронна печатка;
УНЗР	-	унікальний номер запису в ЄДДР;
ФОП	-	фізична особа - підприємець
ЦЗО	-	Центральний засвідчувальний орган;
ЦОД	-	центр обробки даних;
СМР	-	сервер обробки запитів;
HTTP	-	Hyper Text Transfer Protocol (протокол прикладного рівня, що використовується для передавання гіпертексту);
LDAP	-	Lightweight Directory Access Protocol (полегшений протокол доступу до директорій/протоколів);
NTP	-	Network Time Protocol (мережевий протокол синхронізації внутрішнього годинника комп'ютера);
OCSP	-	Online Certificate Status Protocol (протокол визначення статусу сертифіката ключа);
OLS	-	Online Service;
PKCS	-	Public Key Cryptography Standards (стандарти криптографії з відкритими ключами);

TSP - Time Stamp Protocol (протокол фіксування часу);
URL - Unique Resource Locator (унікальна адреса інформаційного ресурсу в телекомунікаційній мережі);
UTC - Coordinated Universal Time (всесвітній координований час).

2. СФЕРА ЗАСТОСУВАННЯ

Регламент роботи Кваліфікованого Надавача електронних довірчих послуг «MASTERKEY» ТОВ «АРТ-МАСТЕР» (далі – Регламент) розроблено відповідно до чинного законодавства України у сфері електронних довірчих послуг.

Регламент визначає організаційні, методологічні, технологічні та технічні умови, встановлює порядок і процедури, обов'язкові до виконання посадовими особами Кваліфікованого Надавача електронних довірчих послуг «MASTERKEY» ТОВ «АРТ-МАСТЕР» (далі - Надавач) при наданні ними електронних довірчих послуг (далі – ЕДП).

Вимоги Регламенту є обов'язковими для:

- Надавача та його працівників;
- юридичних та фізичних осіб, підприємств та ФОП, установ та організацій незалежно від їх організаційно-правової форми та форми власності, які на підставі відповідних договорів, утворюють ВПР, а також їх працівники, які беруть безпосередню участь у наданні ЕДП від імені Надавача (далі – Уповноважені особи Надавача);
- юридичних та фізичних осіб – представників органів державної влади, органів місцевого самоврядування, підприємств та ФОП, установ та організацій незалежно від їх організаційно-правової форми та форми власності, що задіяні у впровадженні та забезпеченні функціонування систем електронного документообігу та користуються ЕДП Надавача, з моменту їх звернення до Надавача за отриманням установленим порядком ЕДП, до завершення терміну дії підписаного між ними відповідного договору (далі – Клієнти), Клієнтом може бути Клієнт або Створювач електронної печатки;
- юридичних та фізичних осіб – представників органів державної влади, органів місцевого самоврядування, підприємств та ФОП, установ та організацій незалежно від їх організаційно-правової форми та форми власності, які звернулися до Надавача за отриманням ЕДП (далі – Заявники);
- юридичних та фізичних осіб – представників органів державної влади, органів місцевого самоврядування, підприємств та ФОП, установ та організацій незалежно від їх організаційно-правової форми та форми власності, які використовують або мають намір використовувати інформаційно-телекомунікаційну систему Надавача (далі – Користувачі).

Визнання вимог цього Регламенту Заявниками, Клієнтами та Користувачами ЕДП є обов'язковою умовою та підставою для укладання Надавачем договорів про надання електронних довірчих послуг.

Положення цього Регламенту поширюються в електронній формі шляхом розміщення на офіційному електронному інформаційному ресурсі Надавача https://ca.masterkey.ua/. Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі Надавача.

Суб'єктами правових відносин у сфері ЕДП, що обумовлюються цим регламентом є Центральний засвідчувальний орган (далі – ЦЗО), Надавач, Заявники, Клієнті, та Користувачі.

Цей Регламент набуває чинності з дня розміщення на офіційному веб-сайті Надавача та діє до його скасування.

Регламент роботи Кваліфікованого Надавача електронних довірчих послуг «MASTERKEY» ТОВ «АРТ-МАСТЕР», затверджений 26 вересня 2019 року, зі змінами від 28 серпня 2020 року № 1 та від 14 вересня 2020 року № 2, скасовується із набуттям чинності цим Регламентом.

3. НОРМАТИВНІ ПОСИЛАННЯ

Цей Регламент розроблено на виконання та із дотриманням вимог таких нормативно-правових актів:

- Закон України від 22.05.2003 № 851-IV «Про електронні документи та електронний документообіг»;
- Закон України від 05.10.2017 № 2155-VIII «Про електронні довірчі послуги»;
- Постанова Кабінету Міністрів України від 19.09.2018 № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»:
- Постанова Кабінету Міністрів України від 10.10.2018 № 821 "Про затвердження Порядку зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг";
- Постанова Кабінету Міністрів України від 07.11.2018 № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»;
- Постанова Кабінету Міністрів України від 03.03.2020 № 193 "Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів";
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14.05.2020 № 269 «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих Надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації», зареєстровано в Міністерстві юстиції України 16.07.2020 за № 668/34951;
- Спільний наказ Міністерства цифрової трансформації України та Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 30.09.2020 № 140/614 «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг», зареєстровано в Міністерстві юстиції України 22.10.2020 р. за № 1039/35322;
- Наказ Міністерства цифрової трансформації України від 03.03.2021 № 28 «Про затвердження Порядку подання до центрального засвідчувального органу інформації про діяльність Надавачів електронних довірчих послуг та засвідчувального центру», зареєстровано в Міністерстві юстиції України 23.03.2021 за № 364/35986;
- Регламент роботи центрального засвідчувального органу, затверджений наказом Міністерства цифрової трансформації України від 27.08.2021 № 115, зареєстровано в Міністерстві юстиції України 07.10.2021 за № 1313/36935.

4. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

В Регламенті використано терміни, встановлені в Законі України «Про електронні довірчі послуги» та документах, зазначених у пункті 3 цього Регламенту.

5. ЗАГАЛЬНІ ВІДОМОСТІ

5.1. Ідентифікаційні дані Кваліфікованого Надавача

Країна	Україна
Назва області	Київська
Назва міста	Київ
Повне найменування організації	Товариство з обмеженою відповідальністю «АРТ-МАСТЕР»
Повне найменування Надавача	Кваліфікований Надавач електронних довірчих послуг «MASTERKEY» ТОВ «АРТ-МАСТЕР»
Місцезнаходження організації:	03035, Київ, вул. Сурикова 3, (літ. А)
Код ЄДРПОУ:	30404750
Телефон:	+380 44 206 13 78
Адреса електронної пошти (e-mail):	info@masterkey.ua
Інтернет-адреса офіційного сайту	https://ca.masterkey.ua/

5.2. Порядок внесення змін та доповнень

Внесення змін та доповнень до цього Регламенту здійснюється Надавачем у відповідності до чинного законодавства України.

Надавач має право в односторонньому порядку вносити зміни та доповнення до Регламенту.

Про внесення змін та доповнень до цього Регламенту Надавач повідомляє Заявників, Клієнтів та Користувачів та інших зацікавлених осіб повідомленням на своєму офіційному веб-сайті.

Всі зміни та доповнення, внесені Надавачем до Регламенту, що не пов'язані зі зміною законодавства, набувають чинності з дати, зазначеної у цих змінах та доповненнях, з дня розміщення зазначених змін і доповнень на офіційному веб-сайті Надавача.

Усі зміни та доповнення, що вносяться до Регламенту у зв'язку із змінами законодавства, вступають у силу одночасно із змінами та доповненнями до відповідних нормативних актів.

Усі зміни та доповнення до Регламенту, з моменту їх вступу у дію, однаково поширюються на всіх Клієнтів, що приєдналися до договору про надання електронних довірчих послуг (далі – Договір), в тому числі і на тих, що приєдналися до Договору раніше за дату вступу у дію змін та доповнень.

Якщо Клієнт не погоджується із внесеними до Регламенту змінами та доповненнями, він має право припинити використання сертифіката.

5.3. Порядок публікації

Публічні положення цього Регламенту розповсюджуються в електронній формі: з веб-сайту Надавача за адресою https://ca.masterkey.ua/ та засобами

електронної пошти, а також через поштову адресу: 03035, Київ, вул. Сурикова 3, (літ. А)

5.4. Інформаційно-телекомунікаційна система Надавача

ІТС Надавача створена у вигляді розподіленого багатомашинного комплексу, який реалізує інформаційну технологію та об’єднує програмно-технічний комплекс (далі – ПТК), що використовується під час надання ЕДП, фізичне середовище (інженерні комунікації, обладнання тощо), РС Користувачів, а також оброблювану інформацію.

5.5. Функції ІТС Надавача:

5.5.1. Адміністративні функції:

- реєстрація Заявників;
- надання Заявникам та/або Клієнтам консультацій з питань, пов'язаних з використанням КЕП/УЕП;
- розгляд заяв і скарг Клієнтів;
- передавання документованої інформації, яка підлягає обов'язковому передаванню в разі припинення діяльності Надавача до ЦЗО.

5.5.2. Технічні та технологічні функції:

- забезпечення захисту інформації впродовж експлуатації ІТС;
- генерування ключів Надавача та відповідальних осіб Надавача;
- зберігання ключів Надавача;
- надання допомоги під час генерування ключів Клієнтів, у разі потреби, та вживання заходів щодо забезпечення інформаційної безпеки під час генерування ключів;
- установлення належності Клієнту особистого ключа та його відповідність відкритому ключу;
- засвідчення чинності сертифікатів відкритих ключів Надавача та відкритих ключів послуги фіксування часу в ЦЗО;
- формування сертифікатів сервісу інтерактивного визначення статусу сертифіката (далі – OCSP) Надавача, відповідальних осіб Надавача і Клієнтів;
- ведення реєстру Клієнтів;
- поширення сертифікатів Надавача і Клієнтів у встановленому порядку;
- блокування, скасування та поновлення сертифікатів сервісу OCSP Надавача, формування відповідного запиту до ЦЗО на формування сертифікату формування позначок часу (далі – TSP), відповідальних осіб Надавача і Клієнтів;
- надання послуг інтерактивного визначення статусу сертифіката;
- інші дії, пов'язані з технічною та технологічною підтримкою діяльності Надавача.

Безпосереднє виконання зазначених функцій здійснюється ПТК, при цьому криптографічні перетворення інформації здійснюються з використанням засобів кваліфікованого електронного підпису та печатки, створених з використанням наступних стандартів:

- ДСТУ 4145-2002 - накладання та перевірки електронного підпису;
- ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 – шифрування даних;
- ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 – обчислення імітовставки;
- ДСТУ ГОСТ 34.311-95 та/або ДСТУ 7564:2014 – обчислення геш-функції.

З метою забезпечення безпеки ІТС та оброблюваної у ній інформації, відповідно до законодавства, в ІТС створюється КСЗІ, із підтвердженою відповідністю.

Надавачем, відповідно до Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, затверджених Наказом Адміністрації Держспецзв'язку від 14 травня 2020 року № 269, встановлюються вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника, ВПР та виїзних адміністраторів реєстрації, опису фізичного середовища.

Зазначені вимоги визначаються цим Регламентом, а також іншими нормативними документами Надавача.

6. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ НАДАВАЧ

- Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису та печатки
- Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису та печатки
- Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу.

Під час надання ЕДП Надавачем здійснюються такі процедури:

- реєстрація Користувачів – комплекс заходів з встановлення (ідентифікації) Заявника, підтвердження володіння Заявником особистим ключем, відповідний якому відкритий ключ надається та формування заявки на сертифікацію відкритого ключа;
- сертифікація відкритих ключів – комплекс заходів із контролю результатів реєстрації, формування сертифікату відкритого ключа на підставі заявки, розміщення сертифікату відкритого ключа на інформаційному ресурсі Надавача (за згодою Клієнта) або надання його Клієнту в інший спосіб.
- обслуговування сертифікатів відкритих ключів – комплекс заходів із надання користувачам інформації про статус сертифікату, забезпечення можливості зміни статусу сертифікату відповідно до положень статті 25 Закону України «Про електронні довірчі послуги», забезпечення вільного використання Клієнтем належного йому сертифікату відкритого ключа, надання консультативної та технічної підтримки Клієнтам, забезпечення зміни статусу сертифікату відкритого ключа (за заявкою Клієнта).

Порядок проведення зазначених процедур визначається цим Регламентом, а також іншими нормативними документами Надавача.

Для надання Надавачем ЕДП авторизованим Клієнтам може використовуватися електронний ресурс сервісу «OLS» Надавача, доступ до якого можливо отримати на офіційному сайті Надавача, у розділі: «Подовження дії КЕП», за посиланням: https://ca.masterkey.ua/yak-otrymaty-kep/.

Надавачем, за вимогою Заявника, надаються також ЕДП формування Кваліфікованого сертифікату, що використовується для створення УЕП. Надання таких послуг здійснюється у такому ж порядку, який передбачено для надання ЕДП з формування кваліфікованого сертифікату, з урахуванням вимог та обмежень передбачених постановою Кабінету Міністрів України від 03.03.2020 № 193 та на термін, визначений п. 1. цієї постанови.

7. ПЕРЕЛІК ПОСАД НАЙМАНИХ ПРАЦІВНИКІВ, ОБОВ'ЯЗКИ ЯКИХ БЕЗПОСЕРЕДНЬО ПОВ'ЯЗАНІ З НАДАННЯМ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ТА ФУНКЦІЇ ПРАЦІВНИКІВ

7.1. Склад організаційної структури Надавача

7.1.1. Посадові особи організаційної структури Надавача:

- керівництво Надавача;
- адміністратор реєстрації;
- адміністратор сертифікації;
- адміністратор безпеки та аудиту;
- системний адміністратор (адміністратор системи).

Безпосередньо у обслуговуванні кваліфікованих сертифікатів, задіяні наступні посадові особи:

- адміністратор реєстрації;
- адміністратор сертифікації;

7.1.2. Підрозділ служби захисту інформації

З метою забезпечення вирішення питань, пов'язаних із проектуванням, розробленням і модернізацією, введенням в експлуатацію, обслуговуванням і підтримкою працездатності КСЗІ, а також контролем за станом захищеності інформації, забезпечення повноти та якісного виконання організаційних та технічних заходів із захисту інформації у Надавача створено позаштатний підрозділ служби захисту інформації.

До складу служби захисту інформації Надавача входять працівники, на яких покладено функціональні обов'язки:

- керівника служби захисту інформації;
- адміністратора безпеки та аудиту, у частині, що не суперечить вимогам нормативно-правових актів в сфері ЕДП, без суміщення його посадових обов'язків з іншими посадовими обов'язками, безпосередньо пов'язаними із наданням ЕДП;
- системного адміністратора.

7.2. Функції та завдання організаційних підрозділів та посадових осіб Надавача

7.2.1. Керівництво Надавача

До складу керівництва Надавача входить керівник Надавача та заступник керівника Надавача.

Функції та завдання керівництва Надавача:

- здійснення постійного моніторингу нормативно-правового, організаційного та технічного забезпечення у сфері ЕДП та імплементація відповідних змін у діяльність Надавача;
- визначення основних шляхів розвитку, координація, регламентування, політики та цілей Надавача, контроль та аналіз діяльності посадових осіб Надавача;
- визначення функціоналу структурних підрозділів Надавача;
- забезпечення структурних підрозділів Надавача необхідними ресурсами та матеріалами для досягнення визначених цілей;
- створення умов для безперервної особистої освіти та постійного підвищення кваліфікації найманих працівників Надавача у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних;
- встановлення системи дисциплінарних стягнень за недотримання найманими працівниками Надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері ЕДП і вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо комплексної системи захисту інформації;
- контроль за виконанням зауважень, пропозицій та вимог Клієнтів, направлених на удосконалення роботи Надавача.

7.2.2. Адміністратор реєстрації

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

Функціональні обов'язки адміністратора реєстрації:

- ідентифікація та автентифікація Заявників та Клієнтів;
- перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів, опрацювання відповідних запитів;
- встановлення належності відкритого ключа та відповідного йому особистого ключа Заявників та Клієнтів;
- ведення обліку Клієнтів та передача особових справ Клієнтів, в електронному вигляді, до архіву;
- надання допомоги Клієнтам під час генерації особистих та відкритих ключів, у разі отримання від них відповідного звернення, а також вжиття заходів щодо забезпечення безпеки інформації під час генерації ключів;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів відкритих ключів Клієнтів;
- надання Користувачам консультацій щодо умов та порядку надання ЕДП;
- зберігання та використання носія зі своїм особистим ключем, запобігання доступу до нього інших осіб;
- вирішення спірних питань, що виникають під час роботи з клієнтами, доведення до керівника Надавача інформації про питання, які не можуть бути вирішені власними повноваженнями;
- забезпечення збереження інформації з обмеженим доступом.

Визначені адміністратори реєстрації можуть здійснювати свої повноваження шляхом проведення виїзних реєстрацій.

7.2.3. Адміністратор сертифікації

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

Функціональні обов'язки адміністратора сертифікації:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- зберігання особистих ключів Надавача та їх резервних копій;
- забезпечення використання особистих ключів Надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів Надавача та Клієнтів;
- перевірка запитів про формування, блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів Клієнтів та документів що до них додаються на відповідність вимогам Регламенту роботи Надавача, виконання відповідних дій за запитами;
- участь у знищенні особистих ключів Надавача;
- забезпечення ведення, архівування та відновлення баз даних Надавача;
- забезпечення публікації кваліфікованих сертифікатів відкритих ключів Користувачів та списків відкликаних сертифікатів на офіційному веб-сайті Надавача;
- створення резервних копій кваліфікованих сертифікатів відкритих ключів Клієнтів;
- зберігання кваліфікованих сертифікатів відкритих ключів Клієнтів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІТС;
- забезпечує зберігання носія з особистим ключем Надавача, запобігання доступу до нього інших осіб;
- зберігання та використання носія зі своїм особистим ключем, запобігання доступу до нього інших осіб;
- забезпечення збереження інформації з обмеженим доступом.

7.2.4. Адміністратор безпеки та аудиту.

Адміністратор безпеки та аудиту відповідає за належне функціонування комплексної системи захисту інформації.

Функціональні обов'язки адміністратора безпеки та аудиту:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- контроль за формуванням, обслуговуванням і створенням резервних копій сертифікатів відкритих ключів Надавача, Клієнтів та списків відкликаних сертифікатів;

- контроль за зберіганням особистих ключів Надавача та їх резервних копій, особистих ключів адміністраторів;
- участь у знищенні особистих ключів Надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів ІТС;
- забезпечення спостереження за функціонуванням КСЗІ (реєстрація та моніторинг подій в ІТС);
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС;
- забезпечення режиму доступу до приміщень Надавача, в яких розміщена ІТС;
- ведення журналів обліку адміністратора безпеки та аудиту, визначених документацією щодо КСЗІ;
- проведення перевірок журналів аудиту подій, що реєструють технічні засоби ІТС;
- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо КСЗІ;
- контроль за дотриманням обслуговуючим персоналом Надавача положень внутрішньої організаційно-розпорядчої документації та документації щодо КСЗІ;
- контроль за веденням баз даних Надавача;
- контроль за веденням архіву Надавача;
- забезпечує організацію зберігання та використання в межах ІТС засобів криптографічного захисту інформації;
- забезпечення збереження інформації з обмеженим доступом.

Забороняється суміщення посадових обов'язків адміністратора безпеки та аудиту з іншими посадовими обов'язками, безпосередньо пов'язаними з наданням ЕДП.

Передбачено покладання функцій адміністратора безпеки та аудиту не менш ніж на двох посадових осіб Надавача.

7.2.5. Системний адміністратор

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

Функціональні обов’язки системного адміністратора:
- організація експлуатації та технічного обслуговування ІТС і адміністрування її технічних засобів;
- забезпечення функціонування офіційного веб-сайту Надавача;
- участь у впровадженні та забезпеченні функціонування КСЗІ;
- забезпечення ведення журналів аудиту подій, що реєструють технічні засоби ІТС;
- встановлення, налаштування та забезпечення підтримки працездатності системного та прикладного програмного забезпечення ІТС;
- встановлення та налагодження засобів резервного копіювання ІТС;

- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІТС, у зв'язку із збоями;
- зберігання та використання носія зі своїм особистим ключем, запобігання доступу до нього інших осіб;
- ведення формулярів ІТС;
- забезпечення збереження інформації з обмеженим доступом.

7.2.6. Служба захисту інформації Надавача

Функції та завдання служби захисту інформації наведені у Положенні про Службу захисту інформації Надавача.

7.3. Відокремлені пункти реєстрації

Функції ВПР можуть виконувати як підрозділи або працівники Надавача (далі – ВПР Надавача) так і його Партнери - юридичні особи або ФОП, якими укладено з Надавачем відповідні договори, що містять спеціальні їх обов'язки та повноваження, в тому числі і вимоги щодо захисту інформації (далі – ВПР – представництва Надавача).

До складу ВПР Надавача мають входити лише працівники Надавача.

До складу ВПР – представництва Надавача мають входити працівники або представники відповідних юридичних осіб або ФОП.

7.3.1. ВПР Надавача

На посадових осіб ВПР Надавача можуть бути покладені функції адміністратора реєстрації:
- ідентифікація та автентифікація Заявників та Клієнтів;
- перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів, опрацювання відповідних запитів;
- встановлення належності відкритого ключа та відповідного йому особистого ключа Клієнту;
- ведення обліку Клієнтів;
- надання допомоги Заявникам та Клієнтам під час генерації особистих та відкритих ключів, у разі отримання від них відповідного звернення, а також вжиття заходів щодо забезпечення безпеки інформації під час генерації ключів;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів відкритих ключів Клієнтів;
- надання Користувачам консультацій щодо умов та порядку надання ЕДП;
- зберігання та використання носія зі своїм особистим ключем, запобігання доступу до нього інших осіб;
- ведення обліку Клієнтів та передача особових справ Користувачів до архіву;
- вирішення спірних питань, що виникають під час роботи з клієнтами, доведення до керівника Надавача інформації про питання, які не можуть бути вирішені власними повноваженнями;
- забезпечення збереження інформації з обмеженим доступом.

Функції посадових осіб ВПР Надавача мають виконувати відповідні Посадові особи організаційної структури Надавача, визначені у п. 7.1.1. цього Регламенту.

Визначені адміністратори реєстрації можуть виконувати функції з ідентифікації та автентифікації Клієнтів шляхом проведення виїзних реєстрацій.

7.3.2. ВПР – представництва Надавача

ВПР – представництва Надавача можуть здійснювати функції, аналогічні функціям, покладеним на ВПР Надавача, визначені у п. 7.3.1. цього Регламенту.

Виконання ВПР – представництвом Надавача інших функцій Надавача не припускається.

Функції ВПР – представництва Надавача, на підставі договорів, укладених між Надавачем та відповідними юридичними особами або ФОП, мають виконувати визначені працівники або представники цих юридичних осіб або ФОП.

На підставі положень відповідних договорів, укладених між Надавачем та юридичними особами або ФОП, визначені працівники або представники відповідної юридичної особи або ФОП, можуть бути призначені Уповноваженими особами Надавача.

Визначені адміністратори реєстрації ВПР – представництва Надавача можуть виконувати функції з ідентифікації та автентифікації Заявників шляхом проведення виїзних реєстрацій.

8. ПОЛІТИКА СЕРТИФІКАТА

8.1. Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем

Кваліфіковані сертифікати відкритих ключів, сформованих Надавачем дозволено використовувати для:

- автентифікації;
- перевірки кваліфікованого електронного підпису;
- перевірки кваліфікованої електронної печатки;
- узгодження ключів шифрування.

Вищезазначений перелік не є вичерпним.

Надавачем формуються наступні типи кваліфікованих сертифікатів:

- кваліфіковані сертифікати посадових осіб Надавача, призначені для ідентифікації та автентифікації посадових осіб Надавача та/або перевірки КЕП посадових осіб;
- кваліфіковані сертифікати серверів Надавача, що використовуються при перевірці КЕП на відповідях, які формують сервери ПТК: інформація про статус сертифіката (OCSP) тощо;
- кваліфіковані сертифікати Клієнтів, що використовуються для перевірки КЕП їх власників та/або у якості ідентифікаторів їх власників при забезпеченні доступу до інформаційних ресурсів автоматизованих систем;
- кваліфіковані сертифікати шифрування, що використовуються для підтвердження належності відкритих ключів Клієнтам під час криптографічного захисту інформації шляхом направленого шифрування даних.

8.2. Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем

Обмеження щодо використання сформованих Кваліфікованим Надавачем сертифікатів ключів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України.

Надавач має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери або сфер використання сертифіката доводиться до Користувачів та зазначається у сформованому Надавачем кваліфікованому сертифікаті відкритого ключа.

Не допускається використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем для певної сфери, в інших сферах.

Кваліфіковані сертифікати Надавача та серверів Надавача, а також відповідні їм особисті ключі можуть використовуватись виключно відповідно до їх призначення. Призначення сертифікатів Надавача та сертифікатів

серверів Надавача наводиться у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

Кваліфіковані сертифікати посадових осіб Надавача та відповідні їм особисті ключі можуть використовуватись виключно відповідно до посадових інструкцій їх власників. Інформація стосовно меж використання таких сертифікатів наводиться (за необхідності) у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

Кваліфіковані сертифікати Клієнтів та відповідні їм особисті ключі можуть використовуватись виключно відповідно до призначення пакету послуг, який обирає та отримує Клієнт при обслуговуванні. Інформація стосовного обраного Клієнтом пакету послуг наводиться у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

Кваліфіковані сертифікати шифрування використовуються виключно для підтвердження належності відкритого ключа його власнику під час направленого шифрування даних. Ознака того, що сертифікат використовується у протоколі узгодження ключа, зазначається у розширеному полі сертифіката "Сфера використання відкритого ключа".

Кваліфіковані сертифікати електронної печатки, видані для реєстрації розрахункових операцій юридичним особам та фізичним особам підприємцям відповідно до положень статті 12 Закону України «Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг», та відповідні їм особисті ключі, можуть використовуватись, виключно для застосування в РРО. В означених сертифікатах додатково вказується ознака «для РРО № Х» де Х - порядковий номер РРО.

Надавач має право ініціювати та, за згодою з Заявником, встановлювати інші обмеження сфери використання сформованих ним сертифікатів з занесенням відповідної інформації до сертифіката.

За можливі негативні наслідки використання Клієнтами сертифікатів відкритих ключів і відповідних їм особистих ключів поза визначеною сферою обмежень Надавач відповідальності не несе.

8.3. Перелік інформації, що розміщується Надавачем на своєму офіційному веб-сайті

Електронний інформаційний ресурс (офіційний веб-сайт) Надавача розташований за адресою https://ca.masterkey.ua/ та призначений для розміщення відкритої інформації наступного характеру:

- відомості про Надавача, в тому числі про ВПР та виїзних адміністраторів реєстрації, в обсязі, достатньому для їх однозначного встановлення Заявником (реквізити, адреси, контактні телефони, режими роботи тощо);
- інформація про внесення Надавача до Довірчого списку;

- перелік кваліфікованих електронних довірчих послуг, які надає Надавач;
- сертифікати відкритих ключів серверів Надавача;
- сертифікати відкритих ключів Клієнтів (за згодою Клієнтів);
- списки відкликаних сертифікатів;
- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;
- договори на надання ЕДП, форми та зразки документів, тощо;
- дані про засоби кваліфікованого електронного підпису та печатки, що використовуються під час надання ЕДП;
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів Користувачами;
- дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;
- тарифи та опис пакетів ЕДП, що надаються Надавачем;
- перелік, форми документів, на підставі яких надаються ЕДП, та роз'яснення щодо їх оформлення; посилання на нормативно-правові акти у сфері електронних довірчих послуг та положення цього Регламенту;
- новини, інформаційні повідомлення та інша довідкова інформація, призначені для Клієнтів, Заявників та Користувачів.

Інформація, що публікується на електронному інформаційному ресурсі Надавача, є загальнодоступною. Надавач застосовує організаційні заходи та використовує технічні засоби для забезпечення доступності та захисту від несанкціонованої модифікації цієї інформації.

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

8.4. Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів

Кваліфіковані сертифікати відкритих ключів Надавача публікуються одразу після їх отримання від Центрального засвідчувального органу.

Кваліфіковані сертифікати відкритих ключів серверів Надавача публікуються одразу після їх формування Надавачем.

Кваліфіковані сертифікати відкритих ключів Клієнтів та створювачів електронної печатки, які надали згоду на їх публікацію, публікуються одразу після формування таких сертифікатів.

8.4.1. Порядок публікації сертифікатів ключів Надавача та серверів Надавача

В процесі функціонування Надавач може одночасно використовувати декілька сертифікатів ключів, при цьому усі сертифікати відкритих ключів Надавача повинні бути опубліковані на електронному інформаційному ресурсі Надавача.

Разом з сертифікатом відкритого ключа Надавача на електронному інформаційному ресурсі Надавача публікуються сертифікати відкритих ключів серверів Надавача, зокрема:

– сервера обробки запитів (CMP-сервера);
– сервера позначок часу (TSP-сервера);
– сервера визначення статусу сертифікатів (OCSP-сервера).

8.4.2. Порядок публікації сертифікатів ключів Клієнтів

Публікація сертифікатів відкритих ключів Клієнтів на електронному інформаційному ресурсі Кваліфікованого Надавача здійснюється за згодою Клієнтів. Інформація про необхідність публікації сертифіката ключа кожного окремого Клієнта вноситься у склад реєстраційних даних під час реєстрації Клієнта.

Публікація сертифікатів ключів Клієнтів у інформаційному дереві LDAP-каталогу здійснюється автоматично, після їх формування, з інтервалом синхронізації 30 (тридцять) хвилин.

8.4.3. Порядок публікації списків відкликаних сертифікатів

Публікація СВС на електронному інформаційному ресурсі Надавача (на HTTP-сервері) здійснюється одразу після їх випуску.

Надавач виконує випуск СВС двох типів:

– повний список;
– частковий список.

Повний список випускається не рідше 1 (одного) разу на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані Кваліфікованим Надавачем за весь період його роботи.

Частковий список випускається кожні 2 (дві) години та містить інформацію про усі відкликані сертифікати ключів, статус яких був змінений в інтервалі між часом випуску останнього повного списку та часом формування поточного часткового списку.

У СВС обов’язково зазначається точна дата та час публікації наступного списку.

Новий СВС може бути опублікований до визначеного часу видання наступного списку, вказаного у поточному списку відкликаних сертифікатів.

8.5. Механізм підтвердження володіння Заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа

Підтвердження володіння Заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа забезпечується одним з таких методів:

– візуальним та технічним контролем запису та передачі Надавачу запиту на формування кваліфікованого сертифіката відкритого ключа, особисто Заявником під час генерації пари ключів, одразу після ідентифікації Заявника, за умови його особистої присутності;

–технічним контролем запису та передачі Надавачу запиту на формування кваліфікованого сертифіката відкритого ключа Заявником, під час генерації пари ключів, одразу після ідентифікації Заявника за ідентифікаційними даними, що містяться у раніше сформованому Надавачем кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

При застосуванні будь якого з двох наведених методів, за допомогою засобів електронного підпису Надавача, здійснюється перевірка електронного підпису, створеного за допомогою особистого ключа Заявника на запиті на формування кваліфікованого сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті.

Підтвердження володіння Заявником особистим ключем здійснюється без розкриття особистого ключа.

8.6. Умови встановлення Заявника

На виконання положень Статті 22 Закону України «Про електронні довірчі послуги» під час формування та видачі кваліфікованого сертифіката відкритого ключа Надавач обов'язково здійснює встановлення (ідентифікацію) особи.

Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються.

Ідентифікація фізичної особи, яка вперше звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства України про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

Ідентифікація Заявника — представника державної установи, проведення перевірки цивільної правоздатності та дієздатності державної установи здійснюються за умови подання Надавачу інформації, необхідної для отримання КДП, відповідальним підрозділом (працівником) або Клієнтом особисто.

При цьому, генерація пари ключів (особистого та відкритого) Заявником - представником державної установи здійснюється із використанням засобів кваліфікованого електронного підпису за його особистої присутності у Надавача.

Допускається ідентифікація фізичної особи за ідентифікаційними даними, що містяться у раніше сформованому Надавачем кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифікату.

Ідентифікація іноземців здійснюється відповідно до законодавства України.

Надавач також може здійснювати перевірку чинності документів наданих фізичною особою за даними щодо недійсних документів на інформаційному ресурсі Державної міграційної служби України: https://nd.dmsu.gov.ua.

Для здійснення перевірки цивільної правоздатності та дієздатності юридичної особи Надавач зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься:

– в ЄДР на інформаційному ресурсі - https://usr.minjust.gov.ua/content/free-search;

– в реєстрі платників ПДВ на інформаційному ресурсі - https://cabinet.tax.gov.ua/registers/pdv,

та пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

Надавач, перед формуванням та видачою кваліфікованого сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог Закону України «Про електронні довірчі послуги», а також перевіряє обсяг його повноважень за документом та/або за даними ЄДР, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, Надавачеві подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

Надання ЕДП Надавачем, передбачає проведення ідентифікації Клієнтів під час опрацювання заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

Для ідентифікації особи Заявника, що звернувся до Надавача для отримання ЕДП, Надавач вимагає разом із заявою надати, а Заявник надає оригінали документів що містять інформацію, яка вноситься до кваліфікованого сертифіката відкритого ключа.

Перелік ідентифікаційних даних та механізми їх підтвердження для формування кваліфікованих сертифікатів відкритих ключів електронного підпису чи печатки наведено у Таблицях 1 та 2:

Таблиця 1

Ідентифікаційні дані
та механізми їх підтвердження під час встановлення фізичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Ідентифікаційні дані	**Обов'язковість надання ідентифікаційних даних**	**Механізми підтвердження ідентифікаційних даних**
Прізвище, ім'я, по батькові (за наявності)	Обов'язково	Документальне або електронне (паспорт, посвідка на постійне (тимчасове) місце проживання)
РНОКПП	За наявності	Документальне або електронне (облікова картка платника податків, паспорт)
Серія (за наявності), номер паспорта	Обов'язково	Документальне або електронне (паспорт) та дані інформаційного ресурсу: https://nd.dmsu.gov.ua/
УНЗР	За наявності	Документальне або електронне (паспорт)
Номер телефону	Обов'язково	Технічне (відтворення тексту повідомлення, надісланого надавачем)
Адреса електронної пошти	Обов'язково	Технічне (відповідь на електронний лист, надісланий надавачем)

Таблиця 2

Ідентифікаційні дані
та механізми їх підтвердження під час встановлення юридичних осіб, уповноважені працівники яких вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Ідентифікаційні дані	**Обов'язковість надання ідентифікаційних даних**	**Механізми підтвердження ідентифікаційних даних**
Найменування юридичної особи	Обов'язково	Документальне або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/free-search та платників ПДВ: https://cabinet.tax.gov.ua/registers/pdv
Код ЄДРПОУ	Обов'язково	Документальне або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/free-search)
Юридична адреса	Обов'язково	Документальне або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/free-search)

Повноваження або займана посада	На вимогу Заявника щодо їх включення до сертифікату	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/free-search)

Переліки, форми документів, на підставі яких надаються ЕДП, та роз'яснення щодо їх оформлення публікуються на офіційному веб-сайті Надавача.

Для укладання договорів про надання електронних довірчих послуг Надавач може отримувати від Заявників інші документи, передбачені законодавством.

Для підтвердження належного проведення процедури встановлення Заявника, Надавач забезпечує зберігання електронних копій паперових оригіналів заяв на формування або зміну статусу кваліфікованих сертифікатів відкритих ключів та документів, які надавались Заявниками під час ідентифікації. Копії таких документів (сканкопії/фотокопії) зберігаються в електронному вигляді централізовано в ІТС Надавача, з урахуванням вимог законодавства у сфері архівної справи, захисту інформації, та захисту персональних даних

Заяви та копії документів, які використовуються в процедурі встановлення Заявника, засвідчуються за правилами, наведеними у Таблиці 3:

Таблиця 3

Заяви та копії документів
які використовуються в процедурі встановлення Заявника

Форма документу	**Засвідчення з боку Заявника** засвідчується у першу чергу	**Засвідчення з боку Надавача (адміністратора реєстрації)** засвідчується у другу чергу
	Тип підпису	Тип підпису
Паперова первинна, електронна архівна	Власноручний підпис на паперовому документі	КЕП адміністратора реєстрації на електронній копії паперового документу
Електронна	КЕП або УЕП Клієнта	КЕП адміністратора реєстрації на електронній копії паперового документу

Під час встановлення особи Надавач може використовувати засоби фото або відео фіксації для підтвердження факту пред'явлення Заявником документів, що посвідчують особу. Збереження фото або відео фіксації в ІТС надавача здійснюється з урахуванням положень законодавства України в сфері захисту інформації та захисту персональних даних.

8.7. Механізм автентифікації Користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем

Клієнт може бути автентифікований Надавачем за ідентифікаційними даними, що містяться у раніше сформованому кваліфікованому сертифікаті цього Клієнта, за умов чинності такого сертифіката та незмінності його ідентифікаційних даних на момент звернення для отримання ЕДП.

8.8. Механізм автентифікації Користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа

Перелік та опис механізмів автентифікації Користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа наведено у Таблиці 4:

Таблиця 4

Перелік
механізмів автентифікації Користувачів

Найменування дії зі зміни статусу сертифікату	**Форма звернення**	**Механізми автентифікації**
Блокування кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між Надавачем та Клієнтом здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова	Аналогічний механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Електронна	Аналогічний механізмам підтвердження ідентифікаційних даних Користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем
Скасування кваліфікованого сертифіката відкритого ключа	Письмова	Аналогічний механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Електронна	Аналогічний механізмам підтвердження ідентифікаційних даних Користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем
Поновлення кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між Надавачем та Клієнтом здійснюється під

		час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова	Аналогічний механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Порядок дій посадових осіб Надавача під час процедури встановлення та реєстрації Заявника встановлюється окремими нормативними документами Надавача.

8.9. Опис фізичного середовища

Обладнання забезпечено підключенням до електричної мережі та забезпечено гарантованим безперебійним живлення напругою 220В змінного струму, а також підключено обладнання до мережі Інтернет з використанням захищеного вузлу інтернет-доступу.

ВПР розташовуються в межах контрольованої території приміщень Надавача та партнерів (перелік адрес розміщений на інформаційному ресурсі Надавача: https://ca.masterkey.ua/vpra-info/).

Вхід до приміщень, в яких розміщуються технічні засоби майданчиків обмежений, доступ до них контролюється персоналом Надавача та/або технічними засобами контролю доступу.

Приміщення майданчиків відповідають вимогам Постанови Кабінету Міністрів України від 07.11.2018 № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг» та наказу Адміністрації Держспецзв'язку від 14.05.2020 № 269 «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації».

Розділ приміщень Надавача на функціональні зони за рівнями безпеки приміщень визначається організаційно-розпорядчим документом Надавача.

Для кожного рівня безпеки приміщень визначено мінімально необхідний набір механізмів безпеки, зокрема: контролю доступу, виявлення вторгнень, пожежної сигналізації та пожежогасіння, альтернативних та резервних джерел електроживлення тощо.

Розміщення компонентів ІТС виконується, виходячи з:

- унеможливлення ознайомлення сторонніми особами з інформацією з обмеженим доступом, що обробляється на робочих місцях адміністраторів різних категорій та відображається на їх моніторах;
- обмеження доступу Користувачів до пристроїв комутації та серверів, за виключенням тих, кому надані повноваження з їх адміністрування;
- локалізації технічних засобів у приміщеннях, фізичний доступ до яких є обмеженим;
- технічних характеристик обладнання і вимог щодо його встановлення та умов експлуатації, визначених їх виробником;
- вимог до приміщень та компонентів ІТС Надавача, встановлених Вимогами з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, затверджене наказом Адміністрації Держспецзв'язку від 14.05.2020 № 269 та зареєстровані в Мін'юсті 16.07.20 за № 668/34951.

8.9.2. Контрольно-пропускний режим

В будівлях, де знаходяться технічні засоби майданчиків, функціонує система контролю доступу до контрольованої території майданчиків.

Контрольована територія обмежена системою контролю доступу на вході у відповідне приміщення та зовнішніми стінами.

Доступ в приміщення, які призначені для обслуговування Заявників та Клієнтів – вільний, під контролем працівників Надавача.

8.9.3. Режим доступу до приміщень

В приміщеннях, в яких розташовані компоненти ІТС, діє пропускний та внутрішньо об'єктовий режими. Доступ до компонентів ІТС має лише обслуговуючий персонал. Доступ інших осіб до компонентів ІТС можливий лише в супроводі осіб, яким надано такий доступ. Забезпечується контроль виконання пропускного та внутрішньо об'єктового режимів та протипожежної безпеки в межах контрольованої території, а також цілодобовий контроль доступу в приміщення, в яких розташовані компоненти майданчиків ІТС.

Організація фізичної охорони приміщень, в яких розташовані компоненти Майданчика № 1, пожежної та охоронної сигналізації, систем відеоспостереження, забезпечення електроживлення та інших систем життєзабезпечення, а також пропускного режиму здійснюється в порядку, визначеному внутрішньою нормативно-розпорядчою документацією Надавача.

Організація фізичної охорони серверних приміщень, в яких розташовані компоненти Майданчика № 2, пожежної та охоронної сигналізації, систем відеоспостереження, забезпечення електроживлення та інших систем життєзабезпечення, а також пропускного режиму здійснюється в порядку,

визначеному внутрішньою нормативно-розпорядчою документацією ТОВ «БІ МОБАЙЛ».

8.10. Процедурний контроль

Надавачем утворено систему дисциплінарних стягнень за недотримання найманими працівниками Надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо комплексної системи захисту інформації.

Права та відповідальність найманих працівників Надавача визначено відповідними посадовими інструкціями, а також іншими нормативно-правовими документами Надавача

8.11. Порядок ведення журналів аудиту подій, управління доказами та операційною безпекою

8.11.1. Порядок ведення журналів аудиту подій та управління доказами

Надавачем, за допомогою спеціального ПЗ ПТК, здійснюється автоматична реєстрація та внесення до електронних журналів ПТК таких подій:

- спроби створення, знищення, встановлення паролів, зміни прав доступу в ІТС;
- заміни програмного забезпечення, технічних засобів ІТС;
- технічне обслуговування ІТС;
- генерація, використання, знищення особистих ключів Кваліфікованого надавача;
- формування, блокування, скасування та поновлення сертифікатів відкритих ключів, формування списків відкликаних сертифікатів відкритих ключів;
- спроби несанкціонованого доступу до ІТС;
- надання доступу персоналу до ІТС;
- збоїв в роботі ІТС;
- інші події, необхідні для формування доказової бази при розгляді судових справ.

Реєстрація подій в електронних журналах ПТК здійснюється за такими параметрами:

- дата, час, тип події, результат (успішність/неуспішність) події;
- ідентифікатор Користувача (процесу), що ініціював подію.

Інформація про події, що відбулися також вноситься до журналу аудиту подій, який ведеться у паперовій формі, адміністратором безпеки та аудиту, за тими ж параметрами, що й електронні журнали.

Електронні журнали аудиту подій, що ведуться в ПТК ІТС, переглядаються адміністратором безпеки та аудиту періодично, але не рідше одного разу на тиждень з метою виявлення подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушення безпеки експлуатації ІТС.

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

Журнали аудиту подій, що ведуться в паперовій формі, зберігаються протягом 10 років у місці їх створення, після чого забезпечується їх передача на архівне зберігання.

Електронні резервні копії журналів аудиту подій, сертифікатів відкритих ключів, списків відкликаних сертифікатів на знімних носіях зберігаються в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

Резервне копіювання електронних журналів аудиту здійснюється раз на добу (на резервний сервер Кваліфікованого надавача), резервне копіювання журналів аудиту на знімні носії здійснюється раз на тиждень.

Резервування здійснюється системним адміністратором відповідними засобами, що входять до складу операційної системи персонального комп'ютера, системи керування базами даних та засобами ПТК, під контролем та за участю адміністратора безпеки та аудиту. Факти проведення резервування протоколюються (за період) та засвідчуються підписами відповідальних осіб.

Управління доступом до резервних копій журналів аудиту та контроль за їх зберіганням та застосуванням здійснює адміністратор безпеки та аудиту.

Перегляд журналів аудиту, що ведуться в ПТК ІТС, дозволяється здійснювати лише адміністратору безпеки та аудиту та системному адміністратору, відповідно до функціональних обов’язків.

8.11.2. Управління операційною безпекою

Процедури з управління операційною безпекою передбачають:

- контроль використання носіїв інформації в ІТС, спрямований запобіганню їх викраденню, пошкодженню, використанню понад експлуатаційного терміну, несанкціонованому доступу та використанню;
- контроль встановлення оновлення комп'ютерних програм та оновлень безпеки;
- резервне копіювання даних, необхідних для функціонування ІТС, у територіально відокремлених місцях із забезпеченням захисту цих даних від модифікації та несанкціонованого ознайомлення;
- режим доступу до службових та спеціальних приміщень.

Політикою безпеки заборонено застосування оновлень безпеки, які містять уразливості та є нестабільними. Причини невикористання оновлень безпеки документуються. Політикою безпеки також заборонено оновлення комп'ютерних програм, що застосовуються в ІТС, з неідентифікованих та не автентифікованих джерел.

8.12. Порядок ведення архівів Надавача

Види документів та даних, що підлягають архівуванню, строків зберігання архівів, механізм та порядок зберігання і захисту архівів наведено у Таблиці 5:

Таблиця 5

Види документів та даних, що підлягають архівуванню

Види документів та даних	Форма зберігання	Механізм зберігання
Кваліфіковані сертифікати відкритих ключів Надавача, серверів Надавача, посадових осіб Надавача, Клієнтів та створювачів електронних печаток	Електронна	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Журнали аудиту подій ІТС Надавача	Паперова	Сховище (сейф)
	Електронна	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Укладені договори про надання електронних довірчих послуг	Паперова	Приміщення Надавача, визначене для зберігання архіву
	Електронна	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на формування кваліфікованих сертифікатів відкритих ключів та зміну статусу сертифікатів, копії документів, що використовуються під час реєстрації Заявників	Електронна	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Список відкликаних кваліфікованих сертифікатів відкритих ключів, повний та частковий	Електронна	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації

Усі кваліфіковані сертифікати, списки відкликаних сертифікатів та журнали аудиту подій підлягають постійному зберіганню.

Документи у паперовому та електронному вигляді, мають зберігатися у порядку, встановленому законодавством про архіви та архівні справи.

Надавачем забезпечується фіксація фактів звернення щодо блокування та скасування кваліфікованих сертифікатів відкритих ключів, що відбулись за заявою в усній формі, у відповідному журналі, який зберігається у порядку, встановленому законодавством про архіви та архівні справи.

Для зберігання носіїв з архівними копіями електронних документів виділяється окреме сховище (сейф чи відсік сейфу) з двома екземплярами ключів. Один екземпляр ключа від сховища знаходиться у адміністратора безпеки та аудиту, а другий - в опечатаному конверті зберігається у сховищі (сейфі) керівника Надавача.

Автоматичне резервне копіювання даних забезпечується засобами, що входять до складу ПТК ІТС Надавача. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу, під час найменшого завантаження ПТК.

Резервне копіювання даних на знімні носії інформації виконуватися у ручному режимі. Після створення нової резервної копії, попередня резервна копія стає архівною.

Відновлення даних з резервної копії здійснюються засобами ПТК, шляхом зчитування з останньої (актуальної) резервної копії та запису їх у базу даних сервера.

Знімні носії із архівними копіями зберігаються у конвертах чи упаковках, що засвідчуються підписом адміністратора безпеки та аудиту. При цьому на упаковці вказується обліковий номер копії. Факти створення та використання копій фіксуються у окремому журналі.

Журнали аудиту подій мають зберігатися в приміщенні Надавача. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора. Адміністратор безпеки та аудиту періодично контролює процес створення та зберігання резервних копій.

Знищення архівних документів має здійснюватися комісією, до складу якої обов'язково входить адміністратор безпеки та аудиту. Після завершення процедури знищення архівних документів повинен складатися відповідний акт, який затверджує керівник Надавача.

8.13. Процес, порядок та умови генерації пар ключів Надавача та Користувачів

8.13.1. Порядок генерації та резервного копіювання ключів Надавача, захисту та доступу до особистого ключа Надавача, резервного копіювання особистого ключа Надавача, збереження, доступу та використання резервної копії

Генерації та резервному копіюванню підлягають особистий ключ Надавача, ключ сервера позначок часу (TSP-сервера), ключ сервера обробки запитів (CMP-сервера) та ключ сервера визначення статусу сертифікатів (OCSP-сервера).

Генерація особистих ключів Надавача та особистих ключів серверів Надавача виконується засобами КЕП зі складу ПТК, у спеціальному приміщенні ПТК Надавача адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

Згенерований особистий ключ Надавача під час експлуатації ПТК ІТС знаходиться у постійному запам'ятовуючому пристрої мережного криптомодуля, що є засобом КЕП. Запит на формування сертифіката ключа Надавача, що містить відкритий ключ, записується на локальний диск центрального сервера Кваліфікованого надавача.

Після генерації особистого ключа Надавача виконується генерація особистих ключів серверів Надавача. Запити на формування сертифікатів ключів серверів Надавача, які містять відкриті ключі, записуються на жорсткі диски відповідних серверів.

Після генерації особистого ключа Надавача та особистих ключів серверів Надавача створюється їх резервні копії. Кожна резервна копія особистого ключа Надавача та особистих ключів серверів Надавача завантажується на захищений носій інформації типу ключ електронний «Кристал-1» або «Алмаз-1К». Захищені носії інформації з резервними копіями особистого ключа Надавача та особистих ключів серверів Надавача зберігаються в тубусах у безпечному сховищі Надавача.

Доступ до особистого ключа Надавача має визначений адміністратор сертифікації, який запечатує тубус своєю печаткою.

Доступ до особистих ключів серверів Надавача має адміністратор безпеки та аудиту, який запечатує тубус своєю печаткою.

Резервні копії особистого ключа Надавача та особистих ключів серверів Надавача зберігаються в спеціальному приміщенні Надавача у безпечному сховищі, який запечатується визначеним адміністратором сертифікації. Сформований запит на сертифікат ключа Надавача та сервера позначок часу (TSP) передається до ЦЗО у порядку, встановленому ЦЗО.

Формування сертифіката ключа Надавача виконується у ЦЗО згідно із Регламентом роботи ЦЗО.

Сформовані у ЦЗО сертифікати ключів Надавача та сервера позначок часу (TSP) передаються адміністратору сертифікації Надавача у порядку, встановленому ЦЗО.

Формування сертифікатів ключів інших серверів Надавача виконується засобами ПТК Надавача в спеціальному приміщенні Надавача адміністратором сертифікації у присутності адміністратора безпеки.

Сформовані сертифікати ключів записуються в базу даних відповідного сервера Надавача.

Відомості щодо генерації, резервного копіювання, відновлення та знищення особистого ключа Надавача та особистих ключів серверів Надавача заносяться в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

Після введення в дію нових особистих ключів Надавача та серверів Надавача, особисті ключі, термін дії сертифікатів ключів яких завершився, та їх резервні копії знищуються методом, що не допускає можливості їх відновлення, за участі не менше двох осіб, якими обов'язково повинні бути адміністратор безпеки та аудиту та адміністратор сертифікації.

8.13.2. Порядок позапланової заміни ключів Надавача

У випадку компрометації особистого ключа Надавача або серверів Надавача здійснюється позапланова заміна ключів Надавача.

При компрометації особистого ключа Надавача та/або сервера позначок часу (TSP) кваліфіковані сертифікати Надавача скасовується ЦЗО у порядку передбаченому Регламентом роботи ЦЗО та вноситься до списку (реєстру) відкликаних кваліфікованих сертифікатів ЦЗО.

Сертифікати Надавача, серверів Надавача та всіх Клієнтів скасовуються шляхом занесення в список відкликаних кваліфікованих сертифікатів

Сертифікати всіх Клієнтів, що були сформовані з використанням скомпрометованого ключа Надавача, вважаються нечинними з моменту зміни ЦЗО статусу кваліфікованого сертифіката Надавача на скасований або блокований. Інформація про статус кваліфікованого сертифіката відкритого ключа Надавача розповсюджується ЦЗО у порядку передбаченому Регламентом роботи ЦЗО.

Генерація нових особистих ключів надавача та формування відповідних сертифікатів здійснюється у порядку, визначеному у п. 8.13.1. цього Регламенту.

Новий сертифікат Надавача розміщується на офіційному інформаційному ресурсі Надавача.

Після публікації нового кваліфікованого сертифіката Надавача на офіційному інформаційному ресурсі Надавача, старий особистий ключ Надавача та їх резервні копії знищується у спосіб, що не дозволяє їх відновлення.

Усі кваліфіковані сертифікати Клієнтів, що діяли на момент компрометації ключа Надавача, а також кваліфіковані сертифікати, які були блоковані, повинні бути позапланово замінені.

Під час позапланової заміни Надавач самостійно здійснює виготовлення нових кваліфікованих сертифікатів посадових осіб та Клієнтів, з використанням їх поточних діючих ключових пар. Термін дії нових позапланово сформованих кваліфікованих сертифікатів визначається терміном дії відповідних старих кваліфікованих сертифікатів, що були скасовані внаслідок заміни.

Надавач, шляхом розміщення відповідної інформації на офіційному інформаційному ресурсі Надавача, офіційно оповіщає Користувачів про факт позапланової заміни ключів Надавача та про зміну серійних номерів кваліфікованих сертифікатів Користувачів (формування нових кваліфікованих сертифікатів, підписаних новим ключем Надавача).

СВС підписується новим особистим ключем Надавача.

8.13.3. Процедури отримання Заявником особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її Надавачем

Особистий та відкритий ключі Заявника при отриманні ним ЕДП можуть бути згенеровані Заявником на власному робочому місці або на станції генерації ключів Кваліфікованого Надавача.

Генерація відкритого та особистого ключів Заявника здійснюється з застосуванням засобів кваліфікованого електронного підпису, які мають документи про відповідність або позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

В процесі генерації та впродовж використання особистий ключ Заявника (Клієнта) не покидає меж захищеного носія особистого ключа та захищається паролем і залишається у Клієнта, який несе відповідальність за забезпечення його конфіденційності та цілісності.

Захищеними носіями особистих ключів є носії, що відповідають вимогам статті 19 Закону України «Про електронні довірчі послуги».

Засіб кваліфікованого електронного підпису та печатки за допомогою відповідного особистого ключа створює самопідписані запити на формування кваліфікованих сертифікатів підпису та шифрування, які містять відкриті ключі Користувача та додаткову інформацію для формування кваліфікованих сертифікатів у Кваліфікованого Надавача.

При виборі паролю захисту особистого ключа необхідно враховувати наступні рекомендації:

- довжина паролю повинна містити не менше 8 символів;
- символи паролю не повинні повторюватись;
- пароль не повинен містити підряд більше ніж 2 символи з розкладки

клавіатури;

- в паролі використовувати наступні символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Довжина паролів захисту особистого ключа для НКІ повинна містити кількість символів, передбачену технічною документацією на такі носії.

Після генерації особистого ключа на захищеному носії особистого ключа виводиться вміст простого запиту на формування сертифікату з відкритим ключем КЕП для державних алгоритмів та протоколів. Запити на формування кваліфікованих сертифікатів підпису та шифрування зберігаються Користувачем у форматах: «ПІБ EU-XXXXXXXX.p10» та «ПІБ EU-KEP-XXXXXXXX.p10» відповідно (для електронної печатки замість «ПІБ» зазначається «електронна печатка та ЄДРПОУ юридичної особи»). Розширення файлу запиту (.p10) повинно залишатися без змін.

Запити на формування кваліфікованих сертифікатів підпису та шифрування в «Онлайн-сервісі» має наступний вигляд:

EU-XXXXXXXX.p10 = «_request_sign_yyyymmddxxxxxx

•**.p10**» – унікальне ім’я файлу запиту для формування кваліфікованого сертифіката підпису, що створюється за замовчуванням;

•EU-KEP-XXXXXXXX.p10 = «**_request_crypt_yyyymmddxxxxxx.p10**» – унікальне ім’я файлу запиту для формування кваліфікованого сертифіката шифрування, що створюється за замовчуванням.

Запити на формування кваліфікованих сертифікатів підпису та шифрування ПТК ІТС Кваліфікованого Надавача має наступний вигляд:

•ім’я файлу для запису запиту з відкритим ключем - «**EU-XXXXXXXX.p10**».

•ім’я файлу для запису запиту з відкритим ключем протоколу розподілу - «**EU-KEP-XXXXXXXX.p10**»

Приклад:

ПІБ EU-6E50VH92.p10;

ПІБ EU-KEP-3R15GT23.p10, де:

- «ПІБ» – прізвище, ім’я, по батькові Користувача;
- «EU-6E50VH92.p10» – унікальне ім’я файлу запиту для формування кваліфікованого сертифіката підпису, що створюється за замовчуванням;
- «EU-KEP-3R15GT23.p10» – унікальне ім’я файлу запиту для формування кваліфікованого сертифіката шифрування, що створюється за замовчуванням

Надання Надавачеві сформованих Заявником запитів здійснюється на носії інформації особисто Заявником або його уповноваженою особою після процедури ідентифікації та реєстрації Заявника.

У разі генерації відкритого та особистого ключів Користувача у ВПР ключі генеруються Користувачем особисто на станції генерації ключів, що входить до складу ПТК Кваліфікованого Надавача.

Особистий ключ Користувача генерується на захищений носій особистого ключа, а сформовані запити на формування кваліфікованих сертифікатів передаються на службовому носії інформації на робочу станцію адміністратора реєстрації.

Особисті ключі Користувачів та паролі захисту до них у Кваліфікованого Надавача не зберігаються.

8.13.4. Порядок позапланової заміни особистого ключа Клієнта

Позапланова заміна особистого ключа Клієнта здійснюється в випадку компрометації або підозри компрометації його діючого особистого ключа, втрати носія чи знищення особистого ключа або втрати паролю до особистого ключа.

Для здійснення позапланової заміни особистого ключа та повторного формування сертифіката Клієнт повинен звернутися до Кваліфікованого Надавача із заявою встановленої форми, розміщеної на сайті Кваліфікованого Надавача.

8.14. Механізм надання відкритого ключа Користувача Надавачу для формування кваліфікованого сертифіката відкритого ключа;

Для формування кваліфікованих сертифікатів при отриманні Заявником ЕДП використовуються запити на формування кваліфікованих сертифікатів підпису, які створюються в процесі генерації особистого та відкритого ключів.

Генерація особистих і відкритих ключів виконується при формуванні нового сертифіката ключа, а також при позаплановій заміні особистого ключа Клієнта.

Якщо генерація особистих та відкритих ключів була проведена за межами приміщення Надавача, запити на сертифікацію надаються адміністратору сертифікації особисто Заявником через сервіс «OLS» або виїзним адміністратором, який здійснював реєстрацію.

Підтвердження володіння Користувачем відповідним особистим ключем та його відповідність відкритому ключу здійснюється адміністратором реєстрації без розкриття особистого ключа Користувача, шляхом перевірки кваліфікованого підпису та печатки на запиті за допомогою відкритого ключа, що міститься у запиті.

В процесі генерації ключів створюється особистий та відкритий ключ та запит на формування сертифікату. Запит на формування сертифіката ключа, що передається на сертифікацію до Надавача, є самопідписаним запитом формату PKCS#10. Особистий ключ Надавачу не передається та зберігається у Клієнта.

Під час обробки запиту на формування сертифіката ключа здійснюється перевірка відповідності особистого ключа Клієнта відкритому ключу, який міститься у запиті. Перевірка здійснюється автоматично з використанням програмного забезпечення ПТК ІТС. Формування сертифіката ключа можливе лише за умови позитивного результату перевірки.

8.15. Права та обов’язки Клієнта стосовно користування кваліфікованим сертифікатом та особистим ключем

Клієнт зобов’язаний:

- ознайомитись та дотримуватись умов надання ЕДП, визначених цим Регламентом та відповідними нормативними документами;
- надавати під час реєстрації повну та достовірну інформацію, необхідну для його ідентифікації та формування кваліфікованих сертифікатів;

- зберігати у таємниці особистий ключ та вживати всіх можливих заходів для запобігання його втрати, розкриття, зміни назви, зміни формату чи несанкціонованого використання;
- не розголошувати ключову фразу голосової автентифікації;
- не розголошувати іншим особам пароль захисту захищеного носія особистого ключа, на якому знаходиться особистий ключ;
- використовувати особистий ключ виключно з метою, визначеною у кваліфікованому сертифікаті та додержуватися інших обмежень щодо сфери використання кваліфікованого сертифіката (за наявності);
- використовувати засоби кваліфікованого електронного підпису та печатки для генерації особистих та відкритих ключів, формування та перевірки кваліфікованого електронного підпису та печатки;
- інформувати Кваліфікованого Надавача про події, що трапилися до закінчення строку чинності кваліфікованого сертифіката, зокрема: компрометацію особистого ключа, компрометацію паролю захисту захищеного носія особистого ключа, виявлені неточності або зміну даних, зазначених у кваліфікованому сертифікаті;
- не використовувати особистий ключ у разі його компрометації;
- не використовувати особистий ключ, відповідний до кваліфікованих сертифікатів, заява на скасування чи блокування яких подана до Кваліфікованого Надавача, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування кваліфікованих сертифікатів;
- не використовувати для накладання кваліфікованого підпису та печатки скасований або блокований особистий ключ, відповідний до кваліфікованого сертифіката.

Клієнт має право:
- своєчасно отримувати ЕДП;
- цілодобово користуватись вільним доступом до опублікованих кваліфікованих сертифікатів інших Клієнтів, до даних про статус кваліфікованих сертифікатів, до реєстру кваліфікованих сертифікатів Кваліфікованого Надавача та до нормативних документів у сфері надання ЕДП з використанням телекомунікаційних мереж загального користування;
- одержувати кваліфіковані сертифікати Кваліфікованого Надавача;
- одержувати списки відкликаних сертифікатів, сформовані Кваліфікованим Надавачем;
- застосовувати кваліфікований сертифікат Кваліфікованого Надавача для перевірки кваліфікованих сертифікатів, сформованих Кваліфікованим Надавачем;
- застосовувати списки відкликаних сертифікатів, сформовані Кваліфікованим Надавачем, для перевірки статусу власних кваліфікованих сертифікатів та кваліфікованих сертифікатів інших Користувачів;
- ознайомлюватись з інформацією щодо діяльності Кваліфікованого Надавача у сфері надання ЕДП;
- подавати заяви та скарги;
- здійснювати ініціювання скасування, блокування або поновлення кваліфікованих сертифікатів відповідно до вимог Регламенту;

- вимагати від Кваліфікованого Надавача усунення наслідків порушення умов та вимог Регламенту та договору про надання електронних довірчих послуг;
- вимагати від Кваліфікованого Надавача виконання вимог захисту персональних даних Користувачів;
- оскаржити дії чи бездіяльність Кваліфікованого Надавача у судовому порядку.

9. ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

9.1. Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа

9.1.1. Перелік суб'єктів, уповноважених здійснювати запит на формування кваліфікованого сертифіката відкритого ключа

Запит на формування кваліфікованого сертифіката відкритого ключа формують Заявник, Клієнт, створювач електронних печаток, фізична особа або уповноважений представник юридичної особи, яка отримує ЕДП у Надавача, відповідно до укладеного Договору одночасно з генерацією пари ключів КЕП/УЕП.

Первинну обробку запиту здійснює адміністратор реєстрації під час проведення процедури реєстрації.

Остаточну обробку запиту здійснює адміністратор сертифікації під час проведення процедури сертифікації відкритих ключів.

9.1.2. Порядок подачі та оброблення запиту на формування кваліфікованого сертифіката відкритого ключа

Запит на формування кваліфікованого сертифіката відкритого ключа приймається в обробку після приймання та реєстрації заяви на формування кваліфікованого сертифіката, встановлення (ідентифікації) особи Заявника та підтвердження володіння Заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа відповідно до вимог цього Регламенту.

Обробка запиту на формування кваліфікованого сертифіката відкритого ключа здійснюється засобами ПТК Надавача за участю адміністратора реєстрації або автоматично, із застосуванням сервісу «OLS», при цьому передача сформованих запитів на остаточну обробку адміністратору сертифікації здійснюється захищеними каналами зв'язку, які забезпечують конфіденційність та цілісність даних.

Автоматична обробка запитів не виключає процесів встановлення (ідентифікації) особи Заявника та підтвердження володіння Заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа.

Під час обробки запиту на формування кваліфікованого сертифіката відкритого ключа засобами ПТК Надавача здійснюється перевірка унікальності відкритого ключа в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів та забезпечується унікальність серійного номера кваліфікованого сертифіката електронного підпису чи печатки.

9.1.3. Строки оброблення запиту на формування кваліфікованого сертифіката відкритого ключа

Запит на формування кваліфікованого сертифікату відкритого ключа обробляється у строк, визначений, відповідно до обраного Заявником тарифного плану.

9.2. Порядок надання сформованого кваліфікованого сертифіката відкритого ключа Клієнту

Надання сформованого кваліфікованого сертифіката відкритого ключа Клієнту здійснюється в один із способів:

- надсилання файлу із сформованим кваліфікованим сертифікатом відкритого ключа на адресу електронної пошти, вказану у заяві на формування кваліфікованого сертифіката відкритого ключа;
- запису файлу із сформованим кваліфікованим сертифікатом відкритого ключа на носій інформації, наданий Заявником;
- публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному інформаційному ресурсі Надавача.

Клієнт повинен перевірити свої ідентифікаційні дані, внесені до кваліфікованого сертифіката Надавачем. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки.

Клієнт має використовувати особистий ключ тільки за результатом успішної перевірки сертифікату. Використання Клієнтом особистого ключа є фактом визнання ним правильності даних внесених до кваліфікованого сертифікату відповідного відкритого ключа.

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката та виявлених Клієнтом після отримання сформованого кваліфікованого сертифіката, власник такого сертифіката особисто (або через довірену особу, тільки для юридичних осіб) звертається до Надавача для скасування цього сертифіката та формування нового кваліфікованого сертифіката у встановленому порядку.

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката відкритого ключа та виявлених Надавачем до моменту надання сформованого сертифіката Заявнику, Надавачем здійснюється переформування сертифікату із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення встановленого строку чинності особистого ключа та відповідного йому відкритого ключа.

Порядок дій, у разі виявлення помилок, під час формування кваліфікованих сертифікатів визначається окремою інструкцією, яку видає Надавач

9.3. Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа Клієнта на офіційному веб-сайті надавача

Публікація сформованого кваліфікованого сертифіката відкритого ключа Клієнта, за умови надання ним згоди публікацію, здійснюється у порядку визначеному п. 8.4.2. цього Регламенту.

Згода на публікацію кваліфікованих сертифікатів відкритих ключів надаються Заявниками під час подання заяв на формування сертифікатів

9.4. Умови використання кваліфікованого сертифіката відкритого ключа Клієнта та його особистого ключа

Сфери та умови використання кваліфікованого сертифіката відкритого ключа Клієнта та його особистого ключа та обмеження щодо їх використання наведено в п.п. 8.1., 8.2. цього Регламенту.

Положення, що описують умови використання кваліфікованого сертифіката відкритого ключа Клієнта та його особистого ключа, а також наслідки їх неправильного використання зазначаються у договорі про надання електронних довірчих послуг.

9.5. Процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для Клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем

9.5.1. Повторне формування сертифіката ключа

Повторне формування сертифіката ключа здійснюється за зверненням Клієнта у разі:

– наближення строку завершення чинності сертифіката, з генерацією нових відкритого та особистого ключів;

– зміни відомостей, зазначених у сертифікаті ключа, впродовж дії договору про обслуговування сертифіката, необхідність генерації нових відкритого та особистого ключів встановлює Клієнт;

– прийняття Клієнтом такого рішення, необхідність генерації нових відкритого та особистого ключів встановлює Клієнт.

При повторному формуванні сертифіката відкритого ключа старий сертифікат скасовується.

Обслуговування Клієнтів при повторному формуванні сертифікатів може здійснюватися за процедурами, ідентичними процедурам при первинному формуванні сертифіката, або за наявності чинного сертифікату, в автоматизованому режимі (з використанням сервісу «OLS» Надавача).

9.5.2. Автоматизоване обслуговування Клієнтів при повторному формуванні сертифікатів

Клієнти, які установленим порядком пройшли реєстрацію та володіють чинними, незаблокованими та не анульованими сертифікатами, можуть в автоматизованому режимі здійснити переоформлення таких сертифікатів, та/або здійснювати повторне формування сертифікатів, пов’язане з закінченням терміну дії чинних сертифікатів, шляхом розміщення на електронному ресурсі сервісу «OLS» Надавача електронних документів та електронних копій документів, виготовлених скануванням оригіналів документів на паперових носіях.

При наданні послуги щодо повторного формування сертифіката у разі, коли термін дії чинного сертифіката закінчується, Надавачу надаються:

– заява-реєстр на надання послуги у вигляді електронного документа;

–договір на отримання послуги у вигляді електронного документа або заповнену заяву - приєднання до Договору у вигляді електронного документа;

– запит на формування нового сертифіката у форматі PKCS#10.

Форми та зміст зазначених документів розміщено на офіційному сайті Надавача.

На всі електронні документи, що надсилаються Клієнтом Надавачу, має бути накладено КЕП/УЕП Користувача з використанням особистого ключа, що відповідає чинному сертифікату, термін дії якого закінчується, та/або який підлягає переоформленню.

На всі електронні копії документів, на оригінали яких на паперових носіях нанесено підпис Клієнта, повинний накладатись КЕП/УЕП Клієнта.

Шляхом накладання КЕП/УЕП на електронні документи та електронні копії документів, що надаються Надавачу, Клієнт засвідчує достовірність та актуальність на момент відправки зазначених документів усіх реєстраційних даних, що в них містяться, та реєстраційних даних, що надавались Надавачу Клієнтом під час первинного формування сертифіката. Автентифікація Клієнта виконується шляхом перевірки КЕП/УЕП Клієнта на документах.

У разі, коли Клієнтом виступає посадова особа юридичної особи, а оригінали документів на паперових носіях, електронні копії яких надсилаються Надавачу, підписуються керівником цієї юридичної особи, на електронні копії таких документів накладається КЕП/УЕП зазначеного керівника.

Запит на формування нового сертифіката містить згенерований та засвідчений КЕП/УЕП Клієнта новий відкритий ключ. Підтвердження володіння Клієнтом відповідним новим особистим ключем виконується установленим порядком.

При наданні ЕДП, пов’язаних із повторним формуванням сертифіката ключа, формування нового пакету електронних документів Клієнта не є обов’язковим, дозволяється актуалізувати надані Заявником раніше документи та долучати електронні копії нових документів до бази даних, сформованої при первинному формуванні сертифіката.

9.6. Управління статусом сертифікатів

Управління статусом сертифікатів відкритих ключів полягає в його скасуванні, блокуванні та поновленні чинності.

Скасування, блокування та поновлення чинності сертифіката відкритого ключа виконує виключно Надавач.

Клієнт, статус кваліфікованого сертифіката електронного підпису чи печатки якого було змінено на скасований чи блокований, повинен бути поінформований Надавачем про зміни статусу негайно після завершення відповідних процедур.

Зміна статусу сертифікату здійснюється у порядку, передбаченому статтею 25 Закону України «Про електронні довірчі послуги».

Подання заявки на зміну статусу сертифіката відкритого ключа може виконувати його власник, з застосуванням засобу КЕП придбаного у Надавача з використанням сервісу «OLS» Надавача.

Дані про зміну статусу сертифікату автоматично вносяться до СВС.

9.6.1. Обставини скасування сертифікатів

Скасування сертифіката є достроковим припиненням його чинності. Скасовані сертифікати поновленню не підлягають.

Особистий ключ, сертифікат якого скасований, не може бути використаний Клієнтом для накладання КЕП/УЕП.

У випадку, коли необхідно терміново припинити чинність сертифіката, Клієнт має право заблокувати сертифікат за заявою в усній формі, а потім подати відповідну письмову заяву про скасування сертифіката.

9.6.2. Підстави для скасування сертифіката

Підставами для скасування сертифіката є:

- отримання від Клієнта заяви на скасування сертифіката;
- компрометації особистого ключа (факт або обґрунтована підозра того, що особистий ключ став відомий іншим особам, втрата можливості подальшого використання особистого ключа, зокрема, втрата або пошкодження носія ключової інформації тощо);
- необхідність зміни відомостей, що зазначені у сертифікаті;
- виявлення помилок у реквізитах сертифіката;
- смерть Клієнта або оголошення його померлим за рішенням суду;
- визнання Клієнта недієздатним за рішенням суду;
- припинення діяльності суб'єкта господарювання, реквізити якого зазначені в сертифікаті Клієнта;
- закінчення строку чинності сертифіката ключа;
- виявлення факту надання Клієнтом недостовірних даних;
- виявлення факту порушень вимог законодавства та даного Регламенту під час формування та обслуговування сертифіката;
- набрання законної сили рішенням суду про скасування сертифіката;
- розірвання Клієнтом трудового договору або аналогічного документу, укладеного між Клієнтом та роботодавцем – суб'єктом господарювання, реквізити якого зазначені в сертифікаті ключа Клієнта (за зверненням роботодавця);
- припинення (розірвання) відповідного договору про надання електронних довірчих послуг або порушення суттєвих умов цього договору.

9.6.3. Порядок скасування сертифікатів

Скасування сертифіката можуть ініціювати:

- Клієнт;
- Посадова особа Надавача або Уповноважена особа Надавача, яка має відповідні повноваження, за умови встановлення факту надання Клієнтом, під час формування кваліфікованого сертифікату, недостовірних ідентифікаційних даних або за рішенням суду.

Для скасування сертифіката ключа ініціатором скасування подається заява в письмовій формі або у формі електронного документа установленої форми.

Зразок заповнення заяви на скасування сертифіката розміщується на сайті Кваліфікованого Надавача.

Заява щодо скасування повинна містити наступні відомості:

- ідентифікаційні дані Клієнта;
- серійний номер сертифіката, що скасовується;
- причина скасування сертифіката;
- дата та підпис Клієнта, відбиток печатки Клієнта (за наявності), КЕП/УЕП Клієнта – для заяви в електронній формі.

У разі скасування сертифіката посадовою особою Кваліфікованого Надавача складається акт у довільній формі, у якому вказуються ідентифікаційні дані та серійний номер сертифікату, що скасовується, а також причина його скасування. Акт підписується зазначеною посадовою особою та затверджується керівником Надавача.

Заява на скасування сертифікату, у формі електронного документу, формується Клієнтом на електронному ресурсі сервісу «OLS» Надавача та підписується електронним підписом Заявника.

Письмова заява на скасування сертифіката підписується особистим підписом Клієнта та засвідчується печаткою (за наявності).

Прийняття та опрацювання заяв на скасування сертифіката ключа здійснюються посадовими особами Надавача цілодобово.

Розгляд та опрацювання заяви на скасування сертифіката та інформування Заявника/Клієнта про скасування здійснюється протягом двох годин з моменту надходження заяви до Надавача.

Часом скасування сертифіката встановлюється час зміни статусу сертифіката у реєстрі сертифікатів Надавача.

9.6.4. Обставини блокування сертифікатів

Блокування сертифіката - це тимчасове припинення його чинності.

Особистий ключ, сертифікат якого заблокований, не може бути використаний Клієнтом для накладання КЕП/УЕП.

Надавач має право блокувати сертифікат з подальшим його скасуванням у випадку несплати послуг Надавачу відповідно до договору про надання електронних довірчих послуг.

9.6.5. Підстави для блокування сертифікатів

Підставами для блокування сертифіката є:
- заява, отримана від Клієнта;
- підозра на компрометацію відповідного особистого ключа;
- набрання законної сили рішенням суду про блокування сертифіката;
- виявлення факту порушень вимог законодавства та цього Регламенту під час формування та обслуговування сертифіката;
- інші підстави, передбачені Договором та чинним законодавством України.

9.6.6. Порядок блокування сертифікатів

Блокування сертифіката можуть ініціювати:
- Клієнт;
- Заявник;
- Посадова особа Надавача або Уповноважена особа Надавача, яка має відповідні повноваження, за умови встановлення факту надання Клієнтом, під

час формування кваліфікованого сертифікату, недостовірних ідентифікаційних даних або за рішенням суду.

Блокування сертифіката ключа здійснюється на підставі заяви, поданої ініціатором блокування в усній формі, або заяви, поданої Клієнтем у письмовій формі чи у вигляді електронного документа.

Прийняття і опрацювання заяв на блокування сертифікатів ключів здійснюється цілодобово.

Розгляд та опрацювання заяви на блокування сертифіката, інформування Заявника/Клієнта про блокування здійснюється протягом двох годин з моменту надходження заяви до Надавача.

Часом блокування сертифіката встановлюється час зміни статусу сертифіката у реєстрі сертифікатів Надавача.

Заява в усній формі подається до Надавача в режимі телефонного зв'язку за номером, розміщеним на сайті Надавача.

При поданні заяви на блокування сертифіката необхідно повідомити Надавачу наступну інформацію:

- ідентифікаційні дані Клієнта;
- серійний номер сертифіката;
- фраза-пароль для голосової автентифікації (для заяви в усній формі).

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу фрази – пароля та ідентифікаційних даних Клієнта з інформацією, вказаною в заявці).

Електронна заява на блокування сертифіката повинна підписуватись власником сертифіката з використанням КЕП/УЕП і подаватись до Надавача засобами електронних комунікацій на електронну адресу, вказану на сайті Надавача, або розміщується на електронному ресурсі сервісу «OLS» Надавача.

Письмова заява на блокування сертифіката має засвідчуватись особистим підписом та печаткою (за наявності) Заявника/ Клієнта.

Зразок оформлення заяви на блокування сертифіката розміщується на сайті Надавача.

У разі блокування сертифіката посадовою особою Надавача складається акт у довільній формі, у якому вказуються ідентифікаційні дані та серійний номер сертифіката, що блокується, а також причина його блокування. Акт підписується зазначеною посадовою особою та затверджується керівником Надавача.

9.6.7. Обставини поновлення сертифікатів

Поновлення сертифіката можливе лише для заблокованих сертифікатів, термін дії яких не закінчився. Скасовані сертифікати поновленню не підлягають.

9.6.8. Підстави для поновлення сертифікатів

Надавач поновлює заблокований сертифікат в наступних випадках;

- встановлення недостовірності відомостей про компрометацію відповідного особистого ключа;
- набрання законної сили рішенням суду про поновлення сертифіката;
- в інших випадках, передбачених Договором та чинним законодавством

України.

9.6.9. Порядок поновлення сертифікатів

Поновлення заблокованого сертифіката можуть ініціювати:

- Клієнт;
- Посадова особа Надавача або Уповноважена особа Надавача, яка має відповідні повноваження, за рішенням суду.

Поновлення сертифіката ключа здійснюється на підставі заяви, поданої Клієнтом в усній формі, або заяви, поданої Клієнтом у письмовій формі.

При поданні заяви на поновлення сертифіката Клієнт повинен повідомити Надавача наступну інформацію:

- ідентифікаційні дані Клієнта;
- серійний номер сертифіката;
- фраза-пароль для голосової автентифікації (для заяви в усній формі).

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу фрази – пароля та ідентифікаційних даних Клієнта з інформацією, вказаною в заявці).

Письмова заява повинна засвідчуватись особистим підписом Клієнта та печаткою (за наявності).

Зразок заповнення заяви розміщується на сайті Надавача.

Прийняття заяв на поновлення сертифіката ключа здійснюються Надавачем цілодобово.

Опрацювання письмової заяви на поновлення чинності сертифіката та інформування Заявника/Клієнта про поновлення здійснюється протягом двох годин з моменту отримання заяви Надавачем.

Часом поновлення чинності сертифіката вважається час зміни його статусу у реєстрі сертифікатів Надавача.

9.6.10. Частота формування списку відкликаних сертифікатів та строки його дії.

Порядок формування та публікації СВС, а також строки його наведено у п. 8.4.3 цього Регламенту.

9.6.11. Розповсюдження інформації про статус сертифікатів ключів

Для розповсюдження інформації про статус сертифікатів ключів Клієнтів використовується механізм СВС та механізм визначення статусу сертифіката ключа в режимі реального часу за протоколом OCSP.

У разі скасування (блокування, поновлення) сертифіката ключа, оновлений список відкликаних сертифікатів випускається та публікується не пізніше 2 (двох) годин після надходження запиту на відкликання сертифіката ключа до Кваліфікованого Надавача. Після отримання заяви вносяться зміни до списків відкликаних сертифікатів, доступних Користувачам. Часом отримання заяви вважається час її опрацювання.

Надавач надає усім Користувачам послугу інтерактивного визначення статусу сертифіката. Послуга надається шляхом відправлення запиту за протоколом HTTP на OCSP-сервер Кваліфікованого Надавача.

Послуга інтерактивного визначення статусу сертифіката надається

цілодобово.

9.7. Особливості поводження з тестовими сертифікатами

Формування та обслуговування тестових сертифікатів відкритих ключів здійснюється за умови дотримання вимог спільного наказу Міністерства цифрової трансформації України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.09.2020 № 140/614.

9.8. Строк закінчення дії кваліфікованого сертифіката відкритого ключа Користувача

Строк дії сертифікату відкритого ключа не може перевищувати 2 років.

Надавач зберігає сертифікат ключа та пов'язану з ним інформацію про його статус постійно. За запитом Користувачів Надавач надає доступ до необхідного сертифіката ключа та інформацію про його статус.

10. ОПИС ПРОЦЕДУР ТА ПРОЦЕСІВ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

10.1. Надання засобів КЕП

Для надання ЕДП послуг Надавачем використовуються засоби КЕП, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

Засоби КЕП можуть надаватися Надавачем у вигляді апаратно-програмних засобів, інформацію щодо яких наведено у розділі: https://ca.masterkey.ua/aparatni-zasoby/, на офіційному веб-сайті Надавача, або окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків.

Надання Надавачем окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватися шляхом передачі цих засобів на носіях інформації безпосередньо Клієнту, шляхом надання доступу до електронного ресурсу сервісу «OLS» Надавача, через офіційний веб-сайт Надавача.

При отриманні ЕДП послуг з використанням мобільних технологій забезпечення Клієнтів SIM-картками, які є засобом КЕП та захищеним носієм особистих ключів, здійснюється постачальниками послуг MobileID з дотриманням вимог законодавства щодо захисту інформації.

10.2. Надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу

КДП з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається Клієнтам при створенні КЕП. Зазначена КДП включає:

- формування кваліфікованої електронної позначки часу;
- передачу кваліфікованої електронної позначки часу Користувачу.

Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, та цілісності електронних даних, з якими ці дата та час пов’язані.

Формування та перевірка кваліфікованої електронної позначки часу здійснюється з використанням засобів КЕП. Перевірка кваліфікованої електронної позначки часу може проводитися будь-яким Користувачем з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

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

- отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити

Надавача;

- перевіряє КЕП, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката Надавача;
- перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана.

Кваліфікована електронна позначка часу вважається недійсною у разі:

- недотримання вимоги щодо точності часу в ПТК Надавача;
- використання скасованого або блокованого кваліфікованого сертифіката Надавача на момент формування кваліфікованої електронної позначки часу.

Кваліфікована електронна позначка часу повинна забезпечувати:

- зв’язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;
- точність часу в програмно-технічному комплексі кваліфікованого Надавача електронних довірчих послуг, що синхронізується із Всесвітнім координованим часом (UTC) з точністю до секунди.

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) погоджується Надавачем із ЦЗО.