Прим. № _

ПОГОДЖЕНО

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

О.В.Потій

"17" 07 2023 р.

ЗАТВЕРДЖУЮ

ТОВ «Вчасно Сервіс»
Директор

С.С. Кривошеєв

"5" 09 2023 р.

РЕГЛАМЕНТ

КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ
ТОВ "ВЧАСНО СЕРВІС"

На 44 аркушах

2023 р.

до вх 6693/ВС

ЗМІСТ

ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

У цьому Регламенті скорочення мають наступні значення:

OCSP	–	Online Certificate Status Protocol
TSP	–	Time Stamp Protocol
CMP	–	Certificate Management Protocol
СВС		Список відкликаних сертифікатів
ВЗІ	–	Відповідальний за захист інформації
ВПР	–	Відокремлений пункт реєстрації
ЄДР	–	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄДДР	–	Єдиний державний демографічний реєстр
ІКС	–	Інформаційно-комунікаційна система
ЕДП	–	Електронні довірчі послуги(а)
КЗІ	–	Криптографічний захист інформації
НКІ	–	Носій ключової інформації - засіб кваліфікованого електронного підпису чи печатки, у вигляді апаратно-програмного або апаратного пристрою, який реалізує функцію зберігання особистого ключа кваліфікованого електронного підпису чи печатки
ОС	–	Операційна система
ПЗ	–	Програмне забезпечення
СПЗ	–	Спеціалізоване програмне забезпечення
СЗІ	–	Служба захисту інформації
РНОКПП	–	Реєстраційний номер облікової картки платника податків
УНЗР	–	Унікальний номер запису в ЄДДР
ЦОД	–	Центр обробки даних

У цьому Регламенті терміни вживаються в наступних значеннях:

автентифікація – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних;

блокування сертифіката відкритого ключа – тимчасове зупинення чинності сертифіката відкритого ключа;

веб-сайт – сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу;

відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

відокремлений пункт реєстрації (ВПР) – територіальний підрозділ кваліфікованого надавача електронних довірчих послуг або юридична чи фізична особа, яка на підставі наказу надавача

електронних довірчих послуг (його керівника) або договору, укладеного з ним, що здійснює реєстрацію Заявників. Безпосереднє управління відокремленим пунктом реєстрації здійснюється Надавачем;

відповідальні працівники Надавача – обслуговуючий персонал Надавача та відокремленого пункту реєстрації, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;

довірчий список – перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються;

договір про надання електронних довірчих послуг (надалі – Договір) – окремий договір про надання електронних довірчих послуг або анкета-заява про приєднання, що розміщенні на веб-сайті, відповідно до якого надаються кваліфіковані електронні довірчі послуги;

електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги;А

електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;

електронна позначка часу – електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;

електронна послуга – будь-яка послуга, що надається через інформаційно-телекомунікаційну систему;

електронні дані – будь-яка інформація в електронній формі;

засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;

засіб кваліфікованого електронного підпису чи печатки (надалі – засіб) – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам Закону України від 05.10.2017 № 2155-VIII «Про електронні довірчі послуги» (надалі – Закон);

засіб удосконаленого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки;

захищений носій особистих ключів – засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання;

Заявник – фізична особа, у тому числі іноземець, фізична особа - підприємець, уповноважений представник юридичної особи, фізичної особи - підприємця, іноземної юридичної особи, що звернулись до надавача для отримання кваліфікованих електронних довірчих послуг;

ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;

ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

інформаційно-комунікаційна система (ІКС) – сукупність інформаційних та комунікаційних систем Надавача, які у процесі обробки інформації діють як єдине ціле та об'єднують програмно-технічний комплекс, що використовується під час надання кваліфікованих електронних довірчих послуг, фізичне середовище, інформацію, що обробляється в зазначених системах;

кваліфікована електронна довірча послуга (КЕД послуга) – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють кваліфікованому надавачу електронних довірчих послуг щодо надання такої послуги;

кваліфікована електронна печатка – удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;

кваліфікований електронний підпис (КЕП) – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

кваліфікована електронна печатка та кваліфікований електронний підпис – надалі разом - КЕП

кваліфікований надавач електронних довірчих послуг (Надавач) – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам Закону та відомості про яку внесені до Довірчого списку;

кваліфікований сертифікат відкритого ключа (надалі – кваліфікований сертифікат) – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам Закону;

компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;

користувач – підписувач, створювач електронних печаток, відправник та отримувач електронних даних, фізична або юридична особа, що є резидентом або нерезидентом, яка отримує електронні довірчі та інші послуги у Надавача згідно укладеного Договору;

надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг;

особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

офіційний інформаційний ресурс Надавача – офіційний веб-сайт Надавача, що розміщений за електронною адресою: ca.vchasno.ua;

пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення;

перевірка – процес засвідчення справжності і підтвердження того, що електронний підпис чи печатка є дійсними;

підписувач – фізична особа (представник юридичної особи), яка створює електронний підпис;

поновлення сертифіката відкритого ключа – відновлення чинності попередньо заблокованого сертифіката відкритого ключа;

програмно-технічний комплекс (надалі – ПТК), що використовується під час надання електронних довірчих послуг – апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов'язаних з наданням електронних довірчих послуг;

реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів – електронна база даних, в якій містяться відомості про сертифікати відкритих ключів, сформовані надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом, їх статус та списки відкликаних сертифікатів відкритих ключів;

сертифікат відкритого ключа – електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту;

скасування сертифіката відкритого ключа – зупинення чинності сертифіката відкритого ключа;

створювач електронної печатки – юридична особа, яка створює електронну печатку, (фізична особа – підприємець, яка створює електронну печатку для застосування в програмних реєстраторах розрахункових операцій);

схема електронної ідентифікації – система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб;

уповноважений представник юридичної особи – відповідальний підрозділ або працівник, що забезпечує організацію використання кваліфікованих електронних довірчих послуг в установі.

Система Вчасно.КЕП – ІКС кваліфікованого надавача електронних довірчих послуг ТОВ «Вчасно Сервіс» , що містить у своєму складі засоби КЕП.

Система Вчасно.КЕП призначена для:

- взаємодії користувачів електронних довірчих послуг, найманих працівників ТОВ «Вчасно Сервіс» та уповноважених осіб його ВПР з програмно-технічним комплексом КНЕДП ТОВ «ВЧАСНО СЕРВІС»;
- внесення (підтвердження) ідентифікаційних даних користувачів електронних довірчих послуг;
- самостійної генерації користувачами електронних довірчих послуг особистих ключів, в т.ч. для їх подальшого зберігання у Системі *Вчасно.КЕП*;
- взаємодії з Єдиним державним веб-порталом електронних послуг «Портал Дія» та іншими державними та приватними користувачами електронних довірчих послуг.

Функціонал Системи передбачає розмежування ролей та прав доступу.

Інші терміни застосовуються у значеннях, наведених у Законі України від 05.10.2017 № 2155-VIII «Про електронні довірчі послуги», Вимогах у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07.11.2018 № 992 (надалі – Вимоги), Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджених постановою Кабінету Міністрів України від 19.09.2018 № 749 (надалі – Порядок), наказі Мінінстерства цифрової трансформації України та Адміністрації державної служби спеціально зв'язку та захисту інформації «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг» від 30.09.2020 № 140/614 інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Статус Регламенту

Цей Регламент кваліфікованого надавача електронних довірчих послуг ТОВ «ВЧАСНО СЕРВІС» (надалі – Надавач) визначає організаційно-методологічні, технічні та технологічні умови діяльності Надавача під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Цей Регламент розроблено відповідно до:

- Закону України від 05.10.2017 № 2155-VIII «Про електронні довірчі послуги»;
- Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07.11.2018 № 992;
- Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, затверджених наказом 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";
- Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджених постановою Кабінету Міністрів України від 19.09.2018 № 749;
- Наказу Мінінстерства цифрової трансформації України та Адміністрації державної служби спеціально зв'язку та захисту інформації «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг» від 30.09.2020 № 140/614
- інших нормативно-правових актів сфери надання електронних довірчих послуг.

Цей Регламент не визначає та не розглядає відносини між Надавачем та Користувачами, які є співробітниками Надавача. Ці відносини регулюються внутрішніми документами Надавача.

Будь-яка зацікавлена особа може ознайомитися з Регламентом на офіційному інформаційному ресурсі Надавача.

1.2 Застосування Регламенту

Норми цього Регламенту поширюються на:

- працівників Надавача;
- працівників відокремлених пунктів реєстрації Надавача;
-
- заявників;
- підписувачів;
- створювачів електронної печатки.

Вимоги Регламенту є обов'язковими до виконання працівниками Надавача та працівниками відокремлених пунктів реєстрації.

Визнання вимог Регламенту заявниками, підписувачами та створювачами електронних печаток є обов'язковою умовою та підставою для укладання з ними договору про надання електронних довірчих послуг.

Цей Регламент є обов'язковим для всіх Користувачів Надавача та є засобом офіційного повідомлення та інформування всіх сторін у взаєминах, що виникають у процесі надання кваліфікованих електронних довірчих послуг.

Норми даного Регламенту є обов'язковими для Користувача та Надавача з моменту подачі Користувачем заяви до Надавача на отримання кваліфікованого сертифіката відкритого ключа.

Положення цього Регламенту поширюються в електронній формі шляхом розміщення на офіційному інформаційному ресурсі Надавача.

Вимоги цього Регламенту застосовуються протягом строку дії Договору на обслуговування, якщо інше не зазначено у Регламенті.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Регламентом, застосовуються правила міжнародного договору.

1.3 Зміни (доповнення) Регламенту

Внесення змін та доповнень до цього Регламенту здійснюється надавачем відповідно до Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 7 листопада 2018 року № 992.

Про внесення змін та доповнень до цього Регламенту, Надавач повідомляє заявників, підписувачів, створювачів електронних печаток та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному веб-сайті Надавача.

Всі зміни та доповнення, внесені Надавачем до Регламенту, що не пов'язані зі зміною законодавства, набувають чинності через 10 (десять) календарних днів з дня розміщення зазначених змін і доповнень на офіційному веб-сайті Надавача.

Всі зміни та доповнення, внесені надавачем до регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом в силу відповідних нормативно-правових актів, але не раніше моменту опублікування змін на офіційному веб-сайті надавача.

Усі зміни та доповнення до Регламенту, з моменту їх вступу у дію, однаково поширюються на всіх Користувачів, що приєдналися до Регламенту, в тому числі і на тих, що приєдналися до Регламенту раніше за дату вступу у дію змін та доповнень.

Якщо, Користувач не згоден із внесеними змінами та доповненнями, він має право припинити використання послуг.

1.4 Ідентифікаційні дані Надавача

Повне найменування організації: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ВЧАСНО СЕРВІС».

Скорочене найменування: ТОВ «ВЧАСНО СЕРВІС».

Код ЄДРПОУ: 41231992.

Юридична адреса: Україна, 02121, місто Київ, Харківське шосе, будинок 201-203, літера 4Г, приміщення 604 .

Номери телефонів/факсів: +380443920300, +380676592623.

Веб-сайт: https://vchasno.ua. https://cap.vchasno.com.ua

Електронна пошта: support.cap@vchasno.ua.

2 ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

Надавач забезпечує надання таких кваліфікованих електронних довірчих послуг:

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

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

3.1 Склад організаційної структури Надавача

До складу організаційної структури Надавача, входять такі посадові особи:

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

Безпосередньо у обслуговуванні кваліфікованих сертифікатів, задіяні наступні посадові особи:

- адміністратор реєстрації;
- адміністратор сертифікації;
- системний адміністратор;
- адміністратор безпеки та аудиту.

3.1.1 Відокремлені пункти реєстрації

До складу організаційної структури відокремленого пункту реєстрації, задіяної в обслуговуванні Користувачів Надавача, входять:

- відповідальний за захист інформації в ВПР (керівник пункту);
- адміністратор реєстрації.

3.1.2 Підрозділ служби захисту інформації

З метою забезпечення вирішення питань, пов'язаних із проектуванням, розробленням і модернізацією, введенням в експлуатацію, обслуговуванням і підтримкою працездатності комплексної системи захисту інформації, 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 Надавача (керівник служби захисту інформації);
- адміністратора безпеки та аудиту;
- адміністратора сертифікації;
- системного адміністратора.

Відповідальні за захист інформації на відокремленому пункті реєстрації функціонально підпорядковуються керівнику служби захисту інформації.

3.2 Функції та завдання організаційних підрозділів та посадових осіб Надавача

3.2.1 Керівництво Надавача

До складу керівництва Надавача входить керівник Надавача .

Функції та завдання керівництва Надавача:

- визначення та підтримка в актуальному стані політики та цілей Надавача;
- визначення основних шляхів розвитку, координація, регламентування, контроль та аналіз діяльності Надавача;
- визначення цілей структурних підрозділів Надавача;
- забезпечення структурних підрозділів Надавача необхідними ресурсами для досягнення визначених цілей;
- забезпечення 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 чіткої системи дисциплінарних стягнень за недотримання найманими працівниками Надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг і вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо комплексної системи захисту інформації;
- контроль за виконанням зауважень, пропозицій та вимог Користувачів, направлених на удосконалення роботи Надавача.

3.2.2 Адміністратор реєстрації

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

Функції та завдання адміністратора реєстрації:

- ідентифікація та автентифікація Заявників;
- реєстрація Користувачів;
- отримання та перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;
- встановлення належності відкритого ключа та відповідного йому особистого ключа Заявнику;
- ведення обліку Користувачів;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів;
- надання допомоги Користувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вжиття заходів щодо забезпечення безпеки інформації під час генерації;
- надання Користувачам консультацій щодо умов та порядку надання КЕД послуг;
- підтвердження запитів на формування сертифікатів для Заявників;
- формування запитів на зміну статусу сертифікатів для Користувачів в системі Надавача;

3.2.3 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.

Основними обов'язками адміністратора сертифікації є:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- зберігання особистих ключів Надавача та їх резервних копій;
- формування сертифікатів серверів Надавача;
- формування сертифікатів для персоналу Надавача (адміністратора сертифікації, адміністраторів реєстрації, віддалених адміністраторів реєстрації);
- опрацювання запитів на формування та зміну статусу сертифікатів для користувачів;
- формування списків відкликаних сертифікатів;
- забезпечення використання особистих ключів Надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів Надавача та користувачів;
- перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів Надавача на відповідність вимогам регламенту роботи Надавача;
- участь у знищенні особистих ключів Надавача;
- забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів Користувачів;
- забезпечення публікації кваліфікованих сертифікатів відкритих ключів Користувачів та списків відкликаних сертифікатів на офіційному веб-сайті Надавача;
- створення резервних копій кваліфікованих сертифікатів відкритих ключів Користувачів;
- зберігання кваліфікованих сертифікатів відкритих ключів Користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІКС Надавача.

З метою контролю якості здійснення процедури ідентифікації адміністратор сертифікації вибірково здійснює підтвердження особистої присутності Заявників під час процедури первинної ідентифікації користувачів. Для цього, можуть використовуватися засоби відеозв'язку та відеозапису, за

умови, що Заявник надав згоду на використання засобів відеозв'язку або відеозапису для забезпечення власної ідентифікації Надавачем.

3.2.4 Системний адміністратор Надавача

Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу (надалі - технічні засоби) ІКС Надавача.

Основними обов'язками системного адміністратора є:

- організація експлуатації та технічного обслуговування ІКС Надавача і адміністрування її технічних засобів;
- налаштування програмного забезпечення (надалі - ПЗ) ПТК Надавача (у частині, що не стосується параметрів безпеки);
- налаштування ІКС ПТК Надавача (у частині, що не стосується параметрів безпеки);
- контроль працездатності ПЗ та ПТК Надавача;
- технічне обслуговування та адміністрування ПТК Надавача
- формування та ведення резервних копій загальносистемного та спеціального програмного забезпечення ПТК Надавача;
- забезпечення функціонування офіційного інформаційного ресурсу Надавача;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації;
- ведення журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;
- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІКС Надавача;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІКС Надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІКС Надавача, у зв'язку із збоями.

3.2.5 Адміністратор безпеки та аудиту

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

Основними обов'язками адміністратора безпеки та аудиту є:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- контроль за формуванням, обслуговуванням і створенням резервних копій кваліфікованих сертифікатів відкритих ключів Надавача, користувачів 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 ІКС Надавача;
- забезпечення спостереження за функціонуванням комплексної системи захисту інформації (реєстрація подій в ІКС Надавача, моніторинг подій тощо);
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІКС Надавача;
- забезпечення режиму доступу до приміщень Надавача, в яких розміщена ІКС Надавача;
- ведення журналів обліку адміністратора безпеки та аудиту, визначених документацією щодо комплексної системи захисту інформації;
- проведення перевірок журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;
- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо комплексної системи захисту інформації;
- контроль за дотриманням найманими працівниками Надавача положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо комплексної системи захисту інформації;
- контроль за веденням баз даних та архіву Надавача.

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

Штатним розкладом Надавача передбачено дві посади адміністратора безпеки.

3.2.6. Служба захисту інформації Надавача

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

3.3 Відокремлені пункти реєстрації

Надавач має відокремлені пункти реєстрації без правового статусу юридичної особи, що реалізують функції Надавача з реєстрації Користувачів та їх подальшого обслуговування на відповідній території. В ролі ВПР можуть виступати представництва (відділення, філії, підрозділи) Надавача.

ВПР можуть відряджати адміністраторів реєстрації до Користувачів. ВПР діють на підставі цього Регламенту. ВПР надає консультаційні послуги за зверненнями Користувачів.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «ВЧАСНО СЕРВІС».

Перелік ВПР Надавача, відомості при виїзних адміністраторів реєстрації та відомості про місця розташування ВПР публікуються на офіційному інформаційному ресурсі Надавача. Для взаємодії з Надавачем, ВПР використовують програмні або програмно-технічні засоби, які надаються Надавачем.

Функціональне управління відокремленими пунктами здійснюється Надавачем

До складу працівників відокремлених пунктів реєстрації входять працівники, які здійснюють реєстрацію підписувачів з дотриманням вимог Закону України «Про електронні довірчі послуги» та законодавства у сфері захисту інформації.

На працівників відокремлених пунктів реєстрації Надавача покладено функціональні обов'язки:

- віддаленого адміністратора реєстраціїВПР;
- відповідального за захист інформації на ВПР ;
- відповідальний за системне адміністрування в ІКС ВПР.

Віддалений адміністратор реєстрації ВПР (в т.ч. виїзні адміністратори реєстрації) відповідають за виконання функцій та несуть обов'язки адміністратора реєстрації, визначені у цьому Регламенті.

З числа віддалених адміністраторів реєстрації на відокремленому пункті реєстрації призначаються відповідальні за захист інформації.

Функції та завдання відокремлених пунктів реєстрації:

- ідентифікація та автентифікація заявників, які звернулися до Надавача з метою формування сертифіката;
- перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу Користувача;
- укладення договорів про надання КЕД послуг;
- ведення реєстрації Користувачів (Заявників) у базі даних, передання даних для реєстрації Надавачу;
- отримання від Користувачів заявок на формування, скасування, блокування та поновлення сертифікатів ключів та передавання цих даних Надавачу;
- надання допомоги Користувачам під час генерації особистих та відкритих ключів а також електронних запитів на формування кваліфікованих сертифікатів відкритих ключів Користувачів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;
- перевірка правомірності звернень про блокування, поновлення та скасування сертифікатів;
- надання Користувачам консультацій щодо умов та порядку надання КЕД послуг;
- забезпечення захисту інформації у відокремленому пункті реєстрації.

На ВЗІ у межах ВПР покладається виконання таких функцій:

- організація розмежування доступу до ресурсів ВПР;

- забезпечення спостереження за функціонуванням комплексної системи захисту інформації у ВПР;
- забезпечення режиму доступу до приміщень ВПР;
- ведення журналів обліку, визначених документацією щодо комплексної системи захисту інформації у ВПР;
- контроль за дотриманням працівниками ВПР положень внутрішньої організаційно-розпорядчої документації та документації щодо комплексної системи захисту інформації.

4 ПОЛІТИКА СЕРТИФІКАТА

4.1 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.

Для ідентифікації сфери використання відкритих ключів, під час формування кваліфікованого сертифіката відкритого ключа надавач встановлює розширення сертифіката "Призначення відкритого ключа" ("keyUsage"), зазначені у Таблиці 1.

Таблиця 1 – Призначення відкритого ключа

Сфера використання кваліфікованого сертифіката відкритого ключа	«Призначення відкритого ключа» ("keyUsage")
Автентифікація	digitalSignature + nonRepudiation або keyAgreement
Перевірка кваліфікованого електронного підпису	digitalSignature + nonRepudiation
Перевірка кваліфікованої електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

Для використання сертифікатів у сфері криптографічного захисту інформації з метою узгодження ключів шифрування, та інших сферах, повинні використовуватися різні сертифікати з різними ключовими парами.

Надавач формує кваліфіковані сертифікати відкритого ключа з розширеннями сертифіката digitalSignature + nonRepudiation або keyAgreement за умов, що такі відкриті ключі належать до різних ключових пар.

Для сфери перевірки кваліфікованої електронної печатки, під час формування кваліфікованого сертифіката відкритого ключа надавач встановлює додаткове розширення "Уточнене призначення відкритого ключа" "extendedKeyUsage" із об'єктним ідентифікатором 1.2.804.2.1.1.1.3.9.

В сертифікатах електронних печаток юридичних осіб та фізичних осіб - підприємців, призначених для використання в програмних реєстраторах розрахункових операцій відповідно до Закону України № 128-IX «Про внесення змін до Закону України «Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг» та інших законів України щодо детінізації розрахунків у сфері торгівлі та послуг», додатково вказується ознака «Для РРО № X», де X – номер реєстратора розрахункових операцій

У випадках, передбачених вимогами до окремо визначених ІКС, окрім ознаки того, що генерація особистого ключа відбулася з використанням захищеного носія особистого ключа (id-etsi-qcs 4), для ідентифікації типу захищеного носія особистого ключа, під час формування кваліфікованого сертифіката відкритого ключа надавач встановлює додаткове розширення "Уточнене призначення відкритого ключа" "extendedKeyUsage" та умовне позначення типу такого носія у додаткових даних підписувача.

4.2 Обмеження щодо використання кваліфікованих сертифікатів відкритих 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 із відповідним розширенням сертифіката, в інших сферах.

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

До інформації, вільний доступ до якої забезпечує Надавач через офіційний веб-сайт належать:

- відомості про Надавача;
- відомості про ВПР і виїзних адміністраторів реєстрації.
- дані про внесення відомостей про Надавача до Довірчого списку;
- регламент роботи Надавача;
- кваліфіковані сертифікати відкритих ключів Надавача;
- перелік кваліфікованих електронних довірчих послуг, які надає Надавач;
- дані про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;
- форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги
- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;
- 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;
- перелік актів законодавства у сфері електронних довірчих послуг.

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

4.4 Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів

4.4.1 Публікація чинних кваліфікованих 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 підписувачів та створювачів електронної печатки, які надали згоду на їх публікацію, публікуються одразу після формування таких сертифікатів.

4.4.2 Списки відкликаних сертифікатів

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

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

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

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

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів відкритих ключів підписувачів та створювачів електронної печатки.

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

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

4.4.3 Публікація сертифікатів Надавача та серверів Надавача

Після формування сертифіката Надавача та отримання його від ЦЗО виконується його публікація на офіційному інформаційному ресурсі.

Окрім власного сертифіката Надавача виконується публікація сертифікатів серверів Надавача:

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

Публікація сертифікатів серверів Надавача виконується після формування сертифіката відповідного сервера.

4.5 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:

- візуальним та/або 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

або:

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 кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката. В обох випадках за допомогою засобів кваліфікованого електронного підпису Надавача здійснюється перевірка удосконаленого 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.

Умови подання запиту на сертифікацію встановлено пунктом 5.1 цього Регламенту.

4.6 Умови встановлення Заявника

Відповідно до статті 22 Закону України «Про електронні довірчі послуги» під час формування та видачі кваліфікованого сертифіката відкритого ключа надавач 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 особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється в один із таких способів:

1) за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством порядку з Єдиного державного демографічного реєстру, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи;

2) за ідентифікаційними даними особи, що міститься у кваліфікованому сертифікаті електронного підпису чи печатки, раніше сформованого (сформованої) та виданого (виданої), за умови чинності такого сертифіката.

За бажанням, заявник, використовуючи систему Вчасно.КЕП, може завантажити власні документи, які посвідчують особу, підтверджують громадянство України, повноваження чи спеціальний статус особи, для здійснення Надавачем попередньої верифікації таких документів.

Ідентифікація іноземців здійснюється відповідно до законодавства, в тому числі за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства.

Для підтвердження ідентифікаційних даних фізичної особи чи уповноваженого представника юридичної особи надавач використовує результати перевірки відомостей (даних) про особу, отримані з Єдиного державного демографічного реєстру, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

У разі відсутності в іноземців та осіб без громадянства документів, що підтверджують ідентифікаційні дані, виданих відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, їх ідентифікація здійснюється за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства..

Під час перевірки цивільної правоздатності та дієздатності юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки) чи фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) Надавач використовує інформацію про юридичну особу чи фізичну особу - підприємця, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, (і перелік яких публікує на своєму офіційному веб-сайті центральний засвідчувальний орган), а також пересвідчується, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

Перевірка цивільної правоздатності та дієздатності міжнародних організацій, відомості про яких не внесені до Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань або торговельного, банківського чи судового реєстру, що ведеться іноземною державою, за місцезнаходженням штаб-квартири міжнародної організації здійснюється з використанням інформації з міжнародного договору або іншого офіційного документа, на підставі якого створена та/або діє міжнародна організаціяВ тому числі, повноваження представника юридичної особи підтверджуються накладенням кваліфікованого електронного підпису керівника (уповноваженої особи) такої юридичної особи на заяву про формування кваліфікованих сертифікатів особи в системі Вчасно.КЕП.

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

Надання кваліфікованих електронних довірчих послуг надавачем передбачає опрацювання заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

Ідентифікацію фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, може бути здійснена ВПР (юридичною чи фізичною особою-підприємцем), які виконують повноваження на підставі договору, укладеного з Надавачем за умови дотримання вимог статті 22 Закону України «Про електронні довірчі послуги».

Підставою для здійснення ідентифікації заявника є заява - документ за встановленою формою, що формується заявником в онлайн-сервісі «Вчасно.КЕП та разом із документами, що підтверджують його повноваження відповідно до встановленого переліку, надаються Надавачу для внесення ідентифікаційних даних та проведення реєстрації Користувача. Строк дії заяви становить 48 (сорок вісім) годин з моменту її остаточного заповнення.

Для ідентифікації особи заявника, що звернувся до надавача для отримання кваліфікованих електронних довірчих послуг і не має діючого кваліфікованого сертифіката електронного підпису,

надавач вимагає разом із заявою надати, а заявник надає оригінали документів (в тому числі в електронній формі засобами Порталу Дія) та документи, що підтверджують його повноваження як працівника юридичної особи або фізичної особи – підприємця, 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 2 та 3.

Таблиця 2 – 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, діючий кваліфікований сертифікат електронного підпису)
РНОКПП	За наявності	Документальне або електронне (облікова картка платника податків, паспорт, діючий кваліфікований сертифікат електронного підпису)
Серія (за наявності), номер паспорта або УНЗР	Обов'язково	Документальне або електронне (паспорт, ID картка)
Номер телефону	Обов'язково	Технічне (відтворення тексту SMS, або введення паролю до «хмарного» ключа через повідомлення, надісланого надавачем)
Адреса електронної пошти	Обов'язково	Технічне (відповідь на електронний лист, надісланий надавачем)

Таблиця 3 – 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 (отримання інформації в електронному вигляді з ЄДР, діючий кваліфікований сертифікат електронного підпису)
Код ЄДРПОУ або код чи номер запису торговельного, банківського, судового реєстрів, які ведуться країною резидентства іноземної юридичної особи	Обов'язково	Документальне або технічне (отримання інформації в електронному вигляді з ЄДР, діючий кваліфікований сертифікат електронного підпису)
Місцезнаходження	Обов'язково	Документальне або технічне (отримання інформації в електронному вигляді з ЄДР, діючий кваліфікований сертифікат електронного підпису)

Повноваження або займана посада	На вимогу заявника про їх включення до сертифіката	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або технічне (інформація з ЄДР)

Переліки, форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги, та роз'яснення щодо їх оформлення публікуються на офіційному веб-сайті надавача.

Для укладання договорів про надання кваліфікованих електронних довірчих послуг надавач може отримувати від заявників інші документи, передбачені законодавством.

Заявник безумовно погоджується з тим, що для отримання кваліфікованих електронних довірчих послуг, зокрема формування, перевірки та підтвердження чинності сертифіката електронного підпису чи печатки, його персональні дані (в т.ч. сканкопії або фотокопії документів, які використовувались для ідентифікації особи) та інші документи та дані заявника, які надаються для отримання послуг, будуть передані для подальшої обробки та зберігання в електронному вигляді до програмно-технічного комплексу Надавача з використанням системи Вчасно.КЕП. Обробка та збереження даних здійснюється відповідно до вимог Закону України «Про захист персональних даних».

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 ІКС Надавача або в паперовому вигляді в архівних приміщеннях Надавача, або відокремлених пунктів реєстрації Надавача; з урахуванням вимог законодавства у сфері архівної справи, захисту інформації, та захисту персональних даних.

У разі, якщо заява на реєстрацію (для формування кваліфікованих сертифікатів відкритих ключів заявника) створена в електронному вигляді, перед початком процесу формування кваліфікованих сертифікатів заявника, Надавач повинен отримати згоду такого заявника щодо прийняття ним умов та порядку надання послуг Надавачем. Такою згодою заявник та Надавач вважають OTP (one time password), який використовується, зокрема, для верифікації мобільного номеру телефону заявника та звіряється ПТК Надавача перед формуванням кваліфікованих сертифікатів відкритих ключів. Надавач забезпечує зберігання такої заяви разом з іншими документами, які надавалися заявником в процесі ідентифікації та/або верифікації для отримання кваліфікованих електронних довірчих послуг, в т.ч. з використанням системи Вчасно.КЕП.

Заяви та копії документів, які використовуються в процедурі встановлення заявника, засвідчуються за правилами, наведеними у Таблиці 4

Таблиця 4 – заяви та копії документів які використовуються в процедурі встановлення заявника

Форма документа	Засвідчення з боку заявника		Засвідчення з боку надавача (адміністратора реєстрації, в т.ч. віддаленого та/або виїзного)	
	Тип підпису	Черга засвідчення	Тип підпису	Черга засвідчення
Паперова первинна, електронна архівна	Власноручний підпис на паперовому документі	Перша	Власноручний підпис адміністратора реєстрації	Друга

Електронна	Кваліфікований електронний підпис та/або електронний підпис, отриманий за допомогою засобів відтворення власноручного підпису з використанням інтерактивних сенсорних дисплеїв	Перша	Кваліфікований електронний підпис адміністратора реєстрації або виїзного адміністратора реєстрації на електронному документі, в підсистемі створення облікових записів користувачів	Друга
	Кваліфікована електронна печатка технічного адміністратора Порталу Дія (засвідчення інформації отриманої з Порталу Дія (е-паспорт, е- паспорт для виїзду за кордон тощо)	Перша	Кваліфікована електронна печатка Надавача на електронному документі, в підсистемі створення облікових записів користувачів	Друга
	ОТР (для засвідчення заявником заяв на реєстрацію, створених в електронному вигляді відповідно до п.1 ст.639, п.1 ст.640, п.2 ст.642, ст. 633, 638 Цивільного Кодексу України)	Перша	Кваліфікований електронний підпис адміністратора реєстрації або виїзного адміністратора реєстрації в підсистемі створення облікових записів користувачів на електронній копії паперового документу	Друга

Засвідчення надавачем заяв та копій документів без завершення встановлення особи заявника та без належного засвідчення документів не допускається.

Під час встановлення особи Надавач може використовувати засоби відео-, фотофіксації факту пред'явлення заявником документів, що посвідчують особу. Збереження документів, відео-, фотодокументів в ІКС надавача здійснюється після їх засвідчення шляхом створення кваліфікованого електронного підпису адміністратора реєстрації з урахуванням положень законодавства в сфері захисту інформації та захисту персональних даних. Відео-, фотофіксація здійснюється за умови, що Заявник надав згоду на використання засобів відео зв'язку або відеозапису для забезпечення факта присутності Заявника.

4.7 Механізм ідентифікації Заявників та автентифікації Користувачів, які мають чинний кваліфікований сертифікат відкритого ключа

Для ідентифікації заявника, який має діючий кваліфікований сертифікат електронного підпису чи печатки, використовуються дані такого сертифікату та підтверджуються шляхом накладання кваліфікованого електронного підпису на завку про формування кваліфікованих сертифікатів особи в системі Вчасно.КЕП та засвідчення таким підписом копій документів.

Користувач може бути автентифікований Надавачем за ідентифікаційними даними, що містяться у раніше сформованому Надавачем або іншим кваліфікованим надавачем електронних довірчих, за умови

дотримання вимог статті 22 Закону України «Про електронні довірчі послуги» кваліфікованому сертифікаті цього Користувача, за умов чинності такого сертифіката та незмінності його ідентифікаційних даних на момент звернення для отримання КЕД послуги.

4.8 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 5

Таблиця 5 – перелік механізмів автентифікації користувачів

Тип операції (причина подання заяв)	Форма подання заяв	Механізми підтвердження ідентифікаційних даних
Блокування кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між користувачем та Надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Електронна в системі Вчасно.КЕП	Аналогічні механізмам підтвердження ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем
Скасування кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між користувачем та Надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Електронна в системі Вчасно.КЕП	Аналогічні 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 користувачем та Надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова паперова	Аналогічними механізмами підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

4.9 Опис фізичного середовища

Серверна частина ІКС ТОВ "ВЧАСНО СЕРВІС" розміщена в центрі обробки даних (далі – ЦОД) ТОВ «ГІГАЦЕНТР УКРАЇНА» за адресою: 03022, м. Київ, вул. Васильківська, 37-В.

Неконтрольований доступ сторонніх осіб до апаратури та обладнання серверної частини ІКС ТОВ "ВЧАСНО СЕРВІС" в робочий та неробочий час неможливий.

Приміщення Надавача розділено на функціональні зони з дотриманням вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 14.05.2020 № 269, зареєстрованим в Мінюсті 16.07.2020 за № 668/34951.

Приміщення також обладнані пожежними датчиками та засобами пожежогасіння.

Стіни, підлога та стеля серверного приміщення збудовані з капітальних негорючих матеріалів стійких до проникнення зі зломом.

Робочі станції найманих працівників надавача ІКС ТОВ "ВЧАСНО СЕРВІС" розміщується у приміщенні, що розташована за адресою: м. Київ, Харківське шосе 201-203, секція Б, каб. 115, 116.

Охорона та пропускний режим будівлі цілодобово забезпечується охороною.

Режим доступу до службових приміщень визначається керівництвом, доступ співробітникам надається згідно з їх службовими обов'язками.

Безконтрольний доступ сторонніх осіб до апаратури та обладнання РС обслуговуючого персоналу ІКС ТОВ "ВЧАСНО СЕРВІС" в робочий та неробочий час виключений.

4.10 Управління операційною безпекою

Процедури з управління операційною безпекою передбачають:

- контроль використання носіїв інформації в ІКС, 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 ІКС, 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 заборонено оновлення комп'ютерних програм, що застосовуються в ІКС, з неідентифікованих та неавтентифікованих джерел.

4.11 Управління доказами та архівами

Процедури з управління доказами та архівами передбачають ведення журналів аудиту подій, у яких реєструються події таких типів:

- спроби створення, знищення, встановлення паролів, зміни прав доступу в ІКС тощо;
- заміна технічних засобів ІКС та пар ключів;
- формування, блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів, формування списків відкликаних сертифікатів відкритих ключів;
- спроби несанкціонованого доступу до ІКС;
- надання доступу персоналу до ІКС;
- зміни системних конфігурацій та технічне обслуговування ІКС;
- збої в роботі ІКС;
- інші події, необхідні для збору доказів.

Типи подій, частота перегляду, строки зберігання журналів аудиту подій, методи захисту та резервного копіювання журналів аудиту подій, перелік найманих працівників Надавача, що можуть здійснювати перегляд журналів аудиту подій наведено у Таблиці 6

Таблиця 6 – типи подій

Тип події	Частота перегляду	Строк зберіганн я	Форма ведення	Метод захисту	Доступ на перегляд
Спроби створення, знищення, встановлення паролів, зміни прав доступу в ІКС тощо	не менше 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС Надавача	Адміністрат ор безпеки та аудиту
Заміна технічних засобів ІКС та пар ключів;	За необхідності	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІКС Надавача/ зберігання у сховищах (сейфах)	Адміністрат ор безпеки та аудиту
Внесення, модифікація та видалення реєстраційних даних підписувачів	не менше 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС Надавача	Адміністрат ор безпеки та аудиту
Формування, блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів, формування списків відкликаних сертифікатів відкритих ключів	не менше 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС Надавача	Адміністрат ор безпеки та аудиту
Створення резервних копій та відновлення реєстру кваліфікованих сертифікатів та списків відкликаних сертифікатів та іншої важливої інформації	не менше 1 раз на добу	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІКС Надавача/ зберігання у сховищах (сейфах)	Адміністрат ор безпеки та аудиту

Тип події	Частота перегляду	Строк зберіганн я	Форма ведення	Метод захисту	Доступ на перегляд
Отримання персоналом доступу до автоматизованої системи Надавача та її складових частин (вхід до операційної систему тощо)	не менше 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС Надавача/	Адміністрат ор безпеки та аудиту
Спроби несанкціонованого доступу до ІКС	не менше 1 раз на добу	Постійно	Електронн а	засобами ОС/ засобами ПЗ ІКС Надавача	Адміністрат ор безпеки та аудиту
Зміни системних конфігурацій та технічне обслуговування ІКС	За необхідності	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІКС Надавача/ зберігання у сховищах (сейфах)	Адміністрат ор безпеки та аудиту
Збої у роботі ІКС	не менше 1 раз на добу	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІКС Надавача/ зберігання у сховищах (сейфах)	Адміністрат ор безпеки та аудиту

Усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час події, а також ідентифікувати суб'єкта, що її ініціював або брав у ній участь.

Журнали аудиту подій резервуються та переглядаються адміністратором безпеки та аудиту не рідше одного разу на тиждень, в рамках чого перевіряється наявність несанкціонованої модифікації та вивчаються події.

Час, що зазначається у журналі аудиту подій, синхронізований із Всесвітнім координованим часом з точністю до секунди.

Журнали аудиту подій повинні бути захищені від неавторизованого перегляду, модифікації і знищення шляхом впровадження комплексної системи захисту інформації з підтвердженою відповідністю.

Записи подій у журналах аудиту подій у паперовій формі повинні бути завірені і підписані адміністратором безпеки.

Надавач зберігає журнали аудиту подій на місці їх створення протягом 10 років, після чого забезпечує їх передачу на архівне зберігання.

4.12 Порядок ведення архівів Надавача

4.12.1 Документи, які підлягають архівному зберіганню

Види документів та даних, що підлягають архівуванню, строки зберігання архівів, механізм та порядок зберігання і захисту архівів наведено у Таблиці 7.

Таблиця 7 – види документів та даних, що підлягають архівуванню

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Кваліфіковані сертифікати відкритих ключів Надавача	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів Надавача серверів Надавача (OCSP, TSP, CMP)	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів адміністраторів Надавача	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів підписувачів та створювачів електронних печаток	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Журнали аудиту подій ІКС Надавача	Паперова	> 10 років з моменту внесення останнього запису, після чого забезпечує їх передачу на архівне зберігання	Сховище (сейф)
	Електронна	> 10 років з моменту досягнення максимальної кількості записів, після чого забезпечує їх передачу на архівне зберігання	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Укладені договори про надання послуг	Паперова	> 3 років після закінчення строку дії договору	Архівне приміщення Надавача
	Електронна	> 3 років після закінчення строку дії договору	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Документи та копії документів, що використовуються під час реєстрації заявників	Паперова	> 3 років після закінчення строку дії договору	Архівне приміщення Надавача або відокремленого пункту реєстрації Надавача
	Електронна	> 3 років після закінчення строку дії договору	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на формування кваліфікованих сертифікатів відкритих ключів	Паперова	> 3 роки після закінчення строку дії договору	Архівне приміщення Надавача або відокремленого пункту реєстрації Надавача
	Електронна	> 3 роки після закінчення строку дії договору	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на блокування кваліфікованих сертифікатів відкритих ключів	Паперова	> 3 роки після закінчення строку дії договору	Архівне приміщення Надавача або відокремленого пункту реєстрації Надавача
	Електронна	> 3 роки після закінчення строку дії договору	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на скасування кваліфікованих сертифікатів відкритих ключів	Паперова	> 3 роки після закінчення строку дії договору	Архівне приміщення Надавача або відокремленого пункту реєстрації Надавача
	Електронна	> 3 роки після закінчення строку дії договору	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на поновлення кваліфікованих сертифікатів відкритих ключів	Паперова	> 3 роки після закінчення строку дії договору	Архівне приміщення Надавача або відокремленого пункту реєстрації Надавача

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Список відкликаних кваліфікованих сертифікатів відкритих ключів, повний та частковий	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації

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.

Засоби, що входять до складу центрального серверу ІКС Надавача, забезпечують автоматичне резервне копіювання даних. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу, під час найменшого завантаження центрального серверу.

Додатково може виконуватися резервне копіювання даних на оптичні носії, або інші з'ємні носії інформації у ручному режимі. Після створення нової резервної копії, попередня резервна копія стає архівною.

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

З'ємні носії 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 не менше 10 років. 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 входить адміністратор безпеки та аудиту (а також, за необхідності, адміністратор сертифікації). Після завершення процедури знищення архівних документів повинен складатися відповідний акт, який затверджує керівник Надавача.

4.13 Процес, порядок та умови генерації пар ключів Надавача та Користувачів

4.13.1 Порядок планової заміни ключів Надавача та працівників Надавача

В Надавача використовуються пари (особистих та відкритих) ключів, а саме особисті та відкриті ключі (поточний та попередній) для накладання та перевірки КЕП на сертифікатах серверів Надавача, Користувачів та СВС.

Не пізніше завершення половини строку дії поточної пари ключів (особистий та відкритий ключі) здійснюється генерація нової пари ключів (особистий та відкритий ключі) та формування відповідного сертифікату Надавача. При цьому поточний особистий ключ Надавача стає попереднім, а новий поточним.

Поточний особистий ключ Надавача та попередній особистий ключ Надавача повинні генеруватися, зберігатися і застосовуватися в апаратному або апаратно-програмному засобі, що є засобом КЕП, що входить до складу ПТК Надавача, та використовуватися для накладання КЕП на сертифікати серверів Надавача, Користувачів та СВС.

Апаратні або апаратно-програмні засоби КЗІ із особистими ключами Надавача чи серверів Надавача застосовуються лише у екранованій серверній шафі у спеціальному приміщенні Надавача (серверному приміщенні).

У разі здійснення резервного копіювання особисті ключі надавача переносяться на зовнішній засіб кваліфікованого електронного підпису чи печатки, який є апаратно-програмним або апаратним пристроєм у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

Умови забезпечення захисту резервних копій особистих ключів надавача під час їх зберігання є не гіршими, ніж умови забезпечення захисту особистих ключів, що використовуються.

Факти резервного копіювання та відновлення попереднього особистого ключа Надавача з одного засобу КЕП до іншого засобу КЕП реєструються адміністратором безпеки та аудиту у відповідному журналі обліку.

Після введення в дію нових особистих ключів, 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 .

Процедура планової заміни ключів Надавача здійснюється в наступному порядку:

- адміністратор безпеки та аудиту разом з адміністратором сертифікації генерують новий особистий і відповідний йому відкритий ключ;
- адміністратор сертифікації ініціює процес засвідчення чинності відкритого ключа Надавача у центральному засвідчувальному органі;
- новий сертифікат Надавача розміщується на офіційному інформаційному ресурсі Надавача.

Процедура планової заміни ключів уповноважених осіб Надавача здійснюється в наступному порядку:

- уповноважена особа Надавача генерує нові особисті та відповідний їм відкриті ключі;
- адміністратор сертифікації або уповноважена особа Надавача формує нові сертифікати ключів підпису та протоколу узгодження ключів шифрування посадової особи Надавача;
- старі особисті ключі уповноваженої особи Надавача знищуються у спосіб, що унеможливлює відновлення, а старі сертифікати публікуються у списку відкликаних кваліфікованих сертифікатів.

Перевірка КЕП на документах, підписаних за допомогою старого особистого ключа уповноваженої особи, здійснюється шляхом застосування відповідного йому скасованого сертифіката ключа, який зберігається в реєстрі сертифікатів ключів Надавача.

4.13.2 Порядок позапланової заміни ключів Надавача та посадових осіб Надавача

У випадку компрометації особистого ключа Надавача або ключів уповноважених осіб Надавача виконується позапланова заміна ключів.

У випадку компрометації особистого ключа Надавача кваліфікований сертифікат відкритого ключа Надавача скасовується Центральним засвідчувальним органом шляхом внесення до списку (реєстру) відкликаних кваліфікованих сертифікатів.

Надавачем, після усунення причин та наслідків компроментації особистого ключа, що в т.ч. призвели до скасування кваліфікованого сертифіката відкритого ключа, виконується процедура позапланової зміни ключів та сертифікатів Надавача:

- адміністратор безпеки та аудиту разом з адміністратором сертифікації генерують новий особистий і відповідний йому відкритий ключ;
- адміністратор сертифікації ініціює процес засвідчення чинності відкритого ключа Надавача у центральному засвідчувальному органі;
- новий сертифікат Надавача розміщується на офіційному інформаційному ресурсі Надавача.

Усі кваліфіковані сертифікати уповноважених осіб Надавача та користувачів Надавача, що діяли на момент компрометації особистого ключа Надавача, а також кваліфіковані сертифікати, які були блоковані, повинні бути позапланово замінені.

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

.Сертифікати всіх Користувачів Надавача, що були сформовані з використання скомпрометованого ключа Надавача, вважаються нечинними з моменту зміни центральним засвідчуваним органом статусу кваліфікованого сертифіката Надавача на скасований або блокований. Інформація про статус кваліфікованого сертифіката відкритого ключа Надавача розповсюджується центральним засвідчуваним органом в режимі реального часу за протоколом визначення статусу сертифіката, а також шляхом публікації списків відкликаних кваліфікованих сертифікатів.

Сертифікати всіх Користувачів Надавача скасовуються шляхом внесення в список відкликаних кваліфікованих сертифікатів.

Під час позапланової заміни Надавач самостійно здійснює формування нових кваліфікованих сертифікатів посадових осіб та користувачів, 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).

Список відкликаних кваліфікованих сертифікатів підписується новим особистим ключем Надавача.

У випадку компрометації особистого ключа уповноваженої посадової особи Надавача сертифікат уповноваженої посадової особи Надавача скасовується шляхом внесення до списку відкликаних сертифікатів Надавача.

Після скасування сертифіката уповноваженої посадової особи Надавача а також усунення причин, що призвели до такого скасування , виконується процедура позапланової зміни ключів уповноваженої посадової особи Надавача. Процедура позапланової заміни ключів уповноваженої посадової особи Надавача виконується в порядку, що визначено у процедурі планової зміни ключів уповноваженої посадової особи Надавача даного Регламенту.

4.13.3 Порядок генерації відкритих і особистих ключів та формування кваліфікованих сертифікатів Користувачів Надавача

Процедура формування особистого та відкритого ключів виконується Користувачем на підставі заяви про реєстрацію та формування кваліфікованого сертифіката, опублікованих на офіційному сайті Надавача та/або за допомогою системи Вчасно.КЕП. Формування кваліфікованих сертифікатів Користувачів здійснюється Надавачем на підставі договору.Адміністратор реєстрації виконує процедуру ідентифікації Користувача (Заявника) або його уповноваженої особи (тільки для юридичних осіб). Порядок і умови здійснення ідентифікації описані в пункті 4.6 Регламенту.Генерація особистого та відкритого ключів Користувача виконується при формуванні нового кваліфікованого сертифіката , а також плановій та позаплановій замінах особистого ключа Користувача.

Відкритий та особистий ключі Користувача можуть бути згенеровані за допомогою засобу КЕП:

- самостійно, на особистому обладнанні;
- на робочій станції генерації ключів Користувачів у Надавача або ВПР;
- самостійно у «хмарному» сховищі ключів Надавача.

Після позитивної ідентифікації Користувача або його уповноваженої особи, адміністратор реєстрації:

- приймає заяву про реєстрацію та формування кваліфікованого сертифіката,

- виконує перевірку заяви, документів та запиту на формування сертифіката відкритого ключа.

- виконує перевірку факту володіння Заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа

- опрацьовує запит на формування сертифікату відкритого ключа або відмовляє в наданні послуги.

В разі відмови у реєстрації та формуванні кваліфікованого сертифіката, заява про реєстрацію та формування кваліфікованого сертифіката разом з додатками повертається (в тому числі за допомогою системи Вчасно.КЕП) Заявнику з відміткою адміністратора реєстрації про причини відмови.

Формування паперової копії відображення даних кваліфікованого сертифіката здійснюється на замовлення Користувача та засвідчуються власноручним підписом адміністратора реєстрації та штампом Надавача.

По завершенні процедури формування ключів та кваліфікованого сертифіката Користувачу Надавача надаються:

- Кваліфікований сертифікат відкритого ключа, який може надаватися шляхом публікації на офіційному ресурсі Надавача або відправленням на електронну пошту Користувача, або записом на електронний носій інформації, за умови надання такого носія.
- паперова копія відображення даних кваліфікованого сертифіката відкритого ключа на паперовому носії (на вимогу Користувача).

Після отримання кваліфікованого сертифіката, Користувач або довірена особа повинні перевірити достовірність відомостей викладених в ньому. При виявлені недостовірних даних або помилок, Користувач або довірена особа повідомляють про це адміністратора реєстрації

Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе Користувач.

Надавач здійснює обслуговування кваліфікованого сертифіката Користувача згідно з Договором про надання КЕД послуг.

Повторне формування кваліфікованого сертифікату у разі передчасного (протягом строку дії сертифікату ключа) скасування сертифікату через компрометацію особистого ключа, пошкодження носія особистого ключа або зміни даних Користувача зазначених у сертифікаті здійснюється за додаткову плату згідно з діючими тарифами, або відповідно до умов договору.

4.13.3.1 Генерація ключів на особистому обладнані Користувача

Відкритий та особистий ключі Користувача може бути згенеровані за допомогою засобу КЕП самостійно, на особистому обладнанні.

Особистий ключ Користувача генерується засобами КЕП та захищається паролем. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе Заявник.

Передача Користувачем запиту на сертифікацію до Надавача здійснюється на носії інформації або завдяки сервісу Надавача, що відповідає профілям захисту для кваліфікованого електронного підпису, особисто Користувачем.

При отриманні відкритого ключа у відповідному форматі від Користувача, адміністратор реєстрації перевіряє формат наданого відкритого ключа засобами технічних засобів Надавача, і у разі його невідповідності – відмовляє у формуванні сертифіката ключа. При цьому надані раніше документи повертаються Заявнику з позначкою адміністратора реєстрації на заяві.

Обробка запиту на формування сертифіката відкритого ключа Користувача, який має чинний кваліфікований сертифікат відкритого ключа, , здійснюється після перевірки факту володіння Заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа. Перевірка здійснюється з використанням технічних засобів Надавача, автоматично, шляхом перевірки підпису, накладеного на запит на формування сертифіката, з використанням відкритого ключа, що міститься у запиті. Тобто запит на формування сертифіката є самопідписаним. Формування сертифіката ключа Користувача можливе за умов успішної перевірки запиту.

4.13.3.2 Генерація ключів на робочій станції генерації ключів у Надавача

Користувач виконує генерацію особистого і відкритого ключів засобами КЕП та формує запит на формування кваліфікованого сертифіката у відповідному форматі, що містить відкритий ключ Користувача для формування сертифіката у Надавача.

Унікальність відкритого ключа Користувача в реєстрі чинних, блокованих та скасованих сертифікатів, унікальність розпізнавального імені Користувача та унікальність реєстраційного номеру сертифіката в межах Надавача забезпечується адміністратором реєстрації за допомогою засобів ПТК Надавача.

Адміністратор реєстрації виконує процедуру перевірки унікальності відкритого ключа Користувача в реєстрі чинних, блокованих та скасованих кваліфікованих сертифікатів, включає дані про обмеження використання КЕП, та за вимог Користувача включає до кваліфікованого сертифіката додаткові дані. Ці дані (атрибути) не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів

Сформований запит на формування сертифіката передається на з'ємному носії інформації або за допомогою ІКС Надавача на робочу станцію адміністратора реєстрації. Адміністратор реєстрації опрацьовує запит та передає адміністратору сертифікації для продальшого опрацювання..

Кваліфікований сертифікат в електронній формі може експортуватись на з'ємний носій інформації Користувача та включається у список (реєстр) Надавача.

4.13.3.3 Генерація ключів з використанням «хмарного» сховища

У разі генерації ключових даних Заявником у «хмарному» сховищі Надавача, яке являє собою засіб КЕП, що реалізує зберігання множини особистих ключів КЕП (наприклад, у мережному криптомодулі), така генерація ініціюється Заявником самостійно після ідентифікації у «хмарному» сховищі на основі атрибутів захисту від доступу сторонніх осіб до використання особистого ключа (пароль, PIN-код або біометричні дані особи, що є володільцем особистого ключа). Після отримання запитів на на сертифікацію з «хмарного» сховища, а також ідентифікаційних даних Заявника адміністратор реєстрації Надавача опрацьовує запити на сертифікацію Заявника.

Невід'ємною умовою надання доступу до операцій з особистим ключем у «хмарному» сховищі є проходження Користувачем багатофакторної автентифікації з використанням механізмів, оцінених під час проведення державної експертизи комплексної системи захисту інформації в ІКС Надавача.

Подання та оброблення запитів на сертифікацію, поданих до Надавача, здійснюється відповідно до пункту 5.1 цього Регламенту.

Генерацію та/або управління парою ключів від імені підписувача може здійснювати виключно Надавач. Під час управління парою ключів підписувача Надавач може здійснювати резервне копіювання особистого ключа підписувача з метою його зберігання за умови дотримання таких вимог:

- рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки основного особистого ключа;
- кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

4.14 Процедури отримання Користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги

Отримання Користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги Надавачем, здійснюється через отримання та/або використання засобу електронного підпису, в один із наступних способів:

- отримання особистого ключа в складі засобу електронного підпису Користувача, у тому числі НКІ
- отримання особистого ключа на договірних засадах через доступ і відповідне використання частини ресурсу засобу кваліфікованого електронного підпису, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережний криптомодуль – засіб КЕП).

Фактичне отримання Користувачем особистого ключа відбувається у момент генерації особистого ключа особисто або у момент ініціювання генерації на засобі КЕП, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки). Не допускається формування

Надавачем кваліфікованих сертифікатів відкритих ключів до моменту фактичного отримання особистого ключа Користувачем.

4.15 Механізм надання відкритого ключа Користувача Надавачу для формування кваліфікованого сертифіката відкритого ключа

Відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа у складі запиту на формування кваліфікованого сертифіката відкритого ключа, який являє собою файл формату PKCS#10, що містить відкритий ключ заявника і додаткову інформацію для формування сертифіката.

Формування запиту передбачає створення удосконаленого електронного підпису за допомогою особистого ключа з однієї пари з відкритим ключем.

Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа описаний у положеннях сертифікаційних практик цього Регламенту.

4.16 Порядок захисту та доступу до особистого ключа Надавача

Даний порядок є обов'язковим до виконання усім персоналом Надавача, які надалі називаються – користувачами комплексу.

4.16.1 Порядок обліку носіїв ключової інформації та ключових даних

Всі НКІ мають бути промарковані та поставлені на облік до початку їх використання, про що робиться відповідний запис до журналу обліку НКІ.

Для забезпечення ідентифікації НКІ можуть використовуватися наявні ідентифікаційні дані у маркуванні – заводські чи серійні номери або надані інвентарні номери. Інвентарні номери НКІ повинні бути зазначені на наліпках, які наклеюються на корпус носія або прикріплюються у вигляді ярликів.

НКІ однозначно ідентифікується за його типом та ідентифікаційними даними. Всі дії (операції) з НКІ повинні реєструватися у журналі обліку. Всі операції з резервними НКІ повинні реєструватися у журналі обліку так само, як і зі звичайними носіями.

Всі операції з ключовими даними повинні реєструватися у журналів обліку ключових даних.

4.16.2 Порядок зберігання носіїв ключової інформації

НКІ повинні зберігатися у безпечних сховищах, що знаходяться у спеціальних приміщеннях Надавача. Кожен НКІ повинен зберігатися у конверті (коробці, тубусі) разом із обліковою карткою - у вигляді ключового документа.

Конструкція безпечного сховища повинна передбачати індивідуальні відсіки для кожної уповноваженої посадової особи, яка згідно з посадовими обов'язками виконує роботи з критичною для надавача інформацією (в т.ч. НКІ)

Облікова картка ключового документа заповнюється адміністратором безпеки та аудиту підписується керівником профільного підрозділу Надавача. До облікової картки вноситься інформація про НКІ, ключові дані, що зберігаються на НКІ, а також, за наявності, пароль доступу до НКІ чи інші ідентифікаційні дані, які необхідні для автентифікації у НКІ (наприклад, інформація про електронні ключі автентифікації для криптомодулів, тощо).

НКІ з копіями особистого ключа надавача та особистих ключів серверів ІКС Надавача (OCSP, TSP, CMP) зберігаються у безпечних сховищах, що знаходяться у спеціальних приміщеннях Надавача в запечатаних конвертах чи коробках, які опечатуються печаткою керівника профільного підрозділу надавача чи адміністратора безпеки та аудиту. Умови забезпечення захисту резервних копій особистих ключів Надавача під час їх зберігання повинні бути не гіршими, ніж умови забезпечення захисту особистих ключів, що використовуються

4.16.3 Заходи безпеки під час генерації ключових даних Надавача

Генерація ключових даних (особистих ключів та відкритих ключів) здійснюється згідно з експлуатаційною документацією на відповідні технічні засоби комплексу, на яких здійснюється генерація.

Генерація особистих ключів Надавача та особистих ключів серверів ІКС Надавача (OCSP, TSP, CMP) здійснюються у спеціальному приміщенні Надавача адміністратором сертифікації під контролем

адміністратора безпеки та аудиту.

Генерація особистих ключів посадових осіб Надавача здійснюється на робочих станціях у службових приміщеннях Надавача.

Під час генерації особистих ключів Надавача та особистих ключів серверів ІКС Надавача (OCSP, TSP, CMP) двері повинні бути зачиненими, а всі дії проводитись або у середині приміщення за допомогою термінала або за допомогою віддаленого термінала на робочій станції адміністратора безпеки та аудиту.

Усі особисті ключі у ПТК захищаються на паролях. Паролі повинні відповідати наступним вимогам:

- алфавіт символів пароля – англійські букви "a" – "z", "A" – "Z", цифри "0" – "9" та символи "-", "+" (потужність алфавіту – 2^6 , 6 біт/символ);
- довжина пароля – мінімальна 8, максимальна 42 символи (48-252 біт, потужність системи паролів 2^{46} -2^{252}).

У випадку, якщо для зберігання та використання особистих ключів використовуються мережні криптомодулі, має забезпечуватися взаємна автентифікації криптомодулів та програмних комплексів (складових частин комплексу ІКС Надавача). Алгоритм (протокол) взаємної автентифікації повинен реалізовуватися відповідними бібліотеками підтримки (програмними компонентами), які є складовою частиною криптомодулів. Інтерфейси бібліотек підтримки криптомодулів повинні відповідати вимогам Стандартів, що визначають вимоги до засобів кваліфікованого електронного підпису чи печатки, а саме Профілів захисту для пристроїв створення безпечного підпису, відповідно до виконуваних ними функцій.

4.16.4 Порядок знищення ключових даних

4.16.4.1 Порядок та підстави знищення ключових даних

Знищення особистих ключів Надавача, його серверів та посадових осіб здійснюється згідно з експлуатаційною документацією на відповідні НКІ чи криптомодулі, у яких вони зберігалися та використовувалися. Процедури знищення особистих ключів повинні забезпечувати неможливість відновлення ключів після знищення.

Факти знищення особистих ключів, серверів ІКС Надавача (OCSP, TSP, CMP) та адміністраторів, а також їх резервних копій заносяться до журналу обліку ключових даних. За фактом знищення особистих ключів складаються акти.

4.16.4.2 Знищення особистого ключа Надавача

Підставою для знищення особистого ключа Надавача є:

- закінчення терміну дії кваліфікованого сертифікату відкритого ключа Надавача;
- компрометація особистого ключа Надавача.

Знищення особистих ключів здійснюється штатними програмними засобами, які постачаються разом з комплексом та НКІ.

Резервна копія особистого ключа Надавача повинна бути знищена разом із особистим ключем, який був у використанні після введення нового особистого ключа Надавача.

Знищення резервної копії особистого ключа Надавача на НКІ здійснюється шляхом форматування та/або перезапису НКІ у відповідності з експлуатаційною документацією на НКІ, або шляхом механічного пошкодження НКІ, якщо процедура безпечного очищення НКІ не передбачена виробником.

4.17 Порядок та умови резервного копіювання особистого ключа Надавача, збереження, доступу та використання резервної копії

Відновлення особистого ключа здійснюється шляхом запису його резервної копії в засіб КЕП у ручному режимі, відповідно до експлуатаційної документації на засоби КЕП.

У разі здійснення резервного копіювання особисті ключі Надавача повинні бути перенесені на зовнішній засіб КЕП, який є апаратно-програмним або апаратним пристроєм у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

Резервне копіювання та відновлення особистих ключів Надавача здійснюються адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

Умови забезпечення захисту резервних копій особистих ключів надавача під час їх зберігання є не гіршими, ніж умови забезпечення захисту особистих ключів, що використовуються.

Факти резервного копіювання особистих ключів Надавача та серверів ІКС Надавача (OCSP, TSP, CMP) заносяться до журналу обліку ключових даних.

Факти відновлення особистих ключів Надавача та серверів ІКС Надавача (OCSP, TSP, CMP) з резервних копій або застосування (переходу до використання) резервних засобів КЕП з особистими ключами заносяться до журналу обліку ключових даних. За фактом відновлення особистих ключів чи застосування резервних копій складаються акти.

Резервна копія особистого ключа Надавача може бути застосована з дозволу керівника Надавача у випадку виходу з ладу засобу КЕП, в якому зберігався та використовувався особистий ключ для відновлення ключа у відремонтованому або заміненому мережному криптомодулі.

Резервні копії особистих ключів серверів ІКС Надавача (OCSP, TSP, CMP) можуть бути застосовані у випадку виходу з ладу засобу КЕП з особистими ключами серверів чи мережних криптомодулів, в яких вони зберігалися та використовувалися для заміни основного засобу КЕП чи відновленні ключів у відремонтованому або заміненому засобі КЕП.

4.18 Управління інцидентами

Процедури з управління інцидентами в ІКС Надавача передбачають:

- виконання заходів, визначених Порядком координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженим наказом Адміністрації Держспецзв'язку від 10 червня 2008 року № 94, зареєстрованим в Міністерстві юстиції України 07 липня 2008 року за № 603/15294;
- інформування контролюючого органу про порушення вимог з безпеки та захисту інформації, визначені в абзаці одинадцятому частини другої статті 13 Закону України "Про електронні довірчі послуги", протягом 24 годин після виявлення порушення;
- інформування користувачів, яким надаються послуги, про порушення безпеки, які спричиняють на них негативний вплив, протягом двох годин після виявлення порушення.

4.19 Вимоги до поводження з персональними даними користувачів

Справи підписувачів зберігаються у приміщеннях та сховищах із забезпеченням розмежування доступу персоналу надавача або ВПР відповідно до посадових обов'язків.

Дозволяється тимчасове зберігання (протягом робочого дня) справ підписувачів у місці їх реєстрації у разі забезпечення їх захисту від несанкціонованого доступу (зберігання зачиненими у вогнестійкій шафі, сейфі).

У разі реалізації механізмів автентифікації підписувачів за ключовою фразою дані фраз ключової автентифікації повинні зберігатися в ІКС надавача із забезпеченням доступу до такої інформації виключно персоналу надавача, відповідального за управління статусами сертифікатів відкритих ключів підписувачів.

4.20 Вимоги до процедур встановлення заявника, ВПР та виїзних адміністраторів реєстрації

Процедури встановлення особи-заявника повинні використовувати наявні сервіси перевірки чинності документів та ідентифікаційної інформації про особу.

Під час ідентифікації особи використовується сервіс «Перевірки за базою недійсних документів» Державної міграційної служби України та ЄДР.

Верифікація даних ID-картки здійснюється одним із таких способів:

- без залучення додаткових пристроїв шляхом візуального зіставлення однакової інформації (значення "УНЗР", "документ № ", "дата народження", "строк дії"), яка надрукована в зоні візуальної перевірки та машинозчитувальній зоні;

– шляхом автоматизованого зчитування інформації з використанням апаратних та програмних засобів (зчитувачів), які мають інтерфейс, опублікований на офіційному веб-сайті державного підприємства "Поліграфічний комбінат "Україна".

4.21 Вимоги до публікації на офіційному веб-сайті надавача ідентифікаційних даних про ВПР та виїзних адміністраторів реєстрації

На веб-сайті Надавача публікуються наступні ідентифікаційні дані про ВПР:

– офіційна назва;
– код ЄДРПОУ;
– фізична адреса;
– веб-сайт;
– засоби зв'язку (телефон, електронна пошта, тощо).
– графік роботи

На веб-сайті Надавача публікуються наступні ідентифікаційні дані про виїзних адміністраторів реєстрації:

– прізвище, ім'я, по батькові;
– засоби зв'язку (телефон, електронна пошта, тощо).

5 ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

5.1 Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа

Перелік суб'єктів, уповноважених здійснювати запит на формування кваліфікованого сертифіката відкритого ключа зазначений у визначені поняття «Користувач».

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 програмними засобами ІКС Надавача за участю адміністратора реєстрації, працівника ВПР Надавача на якого покладено обов'язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку 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 ІКС 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.

Строк оброблення запиту на формування кваліфікованого сертифіката відкритого ключа, поданого разом із заявою на реєстрацію, становить не більше однієї години.

5.2 Порядок надання сформованного кваліфікованого сертифіката відкритого ключа Користувачу

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

– шляхом надсилання файлу із сформованим кваліфікованим сертифікатом відкритого ключа на адресу електронної пошти, вказану у заяві на формування кваліфікованого сертифіката відкритого ключа;

- шляхом запису файлу із сформованим кваліфікованим сертифікатом відкритого ключа на носій інформації, наданий заявником;
- шляхом публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному веб-сайті Надавача, у разі отримання згоди на таку публікацію від Користувача.

Користувач повинен перевірити свої ідентифікаційні дані, внесені до кваліфікованого сертифіката Надавачем. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки. Користувач повинен використовувати особистий ключ тільки за результатом успішної перевірки сертифіката. Використання Користувачем особистого ключа є фактом визнання ним правильності даних внесених до кваліфікованого сертифіката відповідного відкритого ключа.

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

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката відкритого ключа та виявлених Надавачем до моменту надання сформованого сертифіката заявнику, посадовою особою Надавача здійснюється переформування сертифіката із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років.

Працівник Надавача, який здійснив повторне формування кваліфікованого сертифіката, складає акт, в якому зазначається дата та час скасування кваліфікованого сертифіката, ідентифікаційні дані Користувача, що зазначені у заяві про реєстрацію та невідповідні ідентифікаційні дані Користувача, що містяться в кваліфікованому сертифікаті. Акт складається в електронній формі, підписується посадовою особою Надавача, що здійснила повторне формування кваліфікованого сертифіката, та адміністратором сертифікації, після цього долучається до особової справи Користувача.

5.3 Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа Користувача на офіційному веб-сайті Надавача

Сформований Надавачем кваліфікований сертифікат Користувача, який надав згоду на його публікацію, публікується у порядку розповсюдження (публікації) інформації Надавачем, встановленим у пункті 4.4.1 Регламенту.

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

5.4 Умови використання кваліфікованого сертифіката відкритого ключа Користувача та його особистого ключа

Умови використання Користувачем особистого ключа та власного кваліфікованого сертифіката, а також сертифікатів інших Підписувачів визначені у пункті 4.1 цього Регламенту.

Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа, а також відомості про наслідки їх неправильного використання зазначаються у договорі про надання кваліфікованої електронної довірчої послуги.

5.5 Процедура подачі запиту на формування кваліфікованого сертифіката для Користувачів, які мають чинний кваліфікований сертифікат відкритого ключа

Запит на формування нового кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа подається разом із заявою про формування нового кваліфікованого сертифіката відкритого ключа.

Автентифікація Користувача виконується шляхом перевірки його КЕП на відповідній електронній заяві.

Програмні засоби ІКС Надавача із інтегрованими засобами кваліфікованого електронного підпису чи печатки, розміщені на офіційному веб-сайті Надавача, забезпечують:

- перевірку чинності кваліфікованого сертифіката відкритого ключа користувача;
- автоматичне формування заяви про формування нового кваліфікованого сертифіката

відкритого ключа із використанням ідентифікаційних даних, внесених до попереднього сертифіката;

- створення кваліфікованого електронного підпису чи печатки до цієї заяви із використанням засобу КЕП з особистим ключем Користувача;
- ініціювання процесу генерації нової ключової пари та формування запиту на формування кваліфікованого сертифіката відкритого ключа у форматі PKCS#10;
- передачу запиту на формування нового кваліфікованого сертифіката відкритого ключа разом із заявою про формування нового кваліфікованого сертифіката відкритого ключа на обробку до ІКС Надавача.

Створення заяви про формування нового кваліфікованого сертифіката відкритого ключа, запиту на формування нового кваліфікованого сертифіката відкритого ключа та їх передача на обробку до ІКС Надавача здійснюється із забезпеченням цілісності та конфіденційності інформації за допомогою засобів кваліфікованого електронного підпису чи печатки.

5.6 Обставини скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа

До переліку суб'єктів, уповноважених подавати запит на скасування (блокування та поновлення) кваліфікованого сертифіката відкритого ключа формування кваліфікованого сертифіката відкритого ключа належать фізичні та юридичні особи, які подають до Надавача заяви або надають інформацію, що підтверджує підстави для зміни статусу сертифіката, передбачені статтею 25 Закону України «Про електронні довірчі послуги».

Перелік підстав для зміни статусу сертифіката із зазначенням суб'єктів подання запитів на зміну статусу та форм підтвердження підстав наведено у Таблиці 8.

Таблиця 8 – перелік підстав для зміни статусу сертифіката

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
Подання користувачем електронних довірчих послуг заяви	+	+	+	Заява користувача (уповноваженого представника юридичної особи)
Смерть фізичної особи - підписувача	+			Документальне підтвердження
Припинення діяльності створювача електронної печатки	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
Зміни ідентифікаційних даних користувача електронних довірчих послуг	+			Документальне або технічне (в т.ч.отримання інформації в електронному вигляді з ЄДР) підтвердження
Припинення підприємницької діяльності фізичної або юридичної особи	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
Надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних	+			Документальне підтвердження

Факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг	+			Заява користувача або документальне підтвердження
Повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг		+		Заява користувача або документальне підтвердження
Повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або контролюючим органом, який раніше повідомив про цю підозру			+	Заява користувача або документальне підтвердження
Набрання законної сили рішенням суду	+	+	+	Документальне підтвердження
Порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг		+		Документальне підтвердження
Усунення порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг			+	Документальне підтвердження

Заява про скасування (блокування, поновлення) кваліфікованого сертифіката електронного підпису чи печатки подається Надавачеві у спосіб, що забезпечує підтвердження особи користувача (уповноваженого представника юридичної особи), в тому числі через Систему Вчасно.КЕП.

Перелік та опис механізмів автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа наведено у Таблиці 5 цього Регламенту.

Надавач здійснює цілодобовий прийом та перевірку заяв користувачів в електронній формі про скасування, блокування та поновлення їх кваліфікованих сертифікатів відкритих ключів.

Заяви в усній формі про поновлення сертифікатів відкритих ключів оброблюються цілодобово.

Заяви в усній формі про блокування сертифікатів відкритих ключів, а також всі заяви в паперовій формі приймаються та оброблюються в робочий час Надавача

5.6.1 Скасування

Скасування кваліфікованого сертифіката Користувача виконується Надавачем на підставі заяви, яка надходить установленим порядком до пунктів реєстрації Надавача в паперовій формі чи у вигляді електронного запиту. Також скасування сертифіката можуть ініціювати посадова особа Надавача на підставах визначених в Таблиці 8.

Заява щодо скасування повинна містити наступні відомості:

- ідентифікаційні дані Користувача ;

- серійний номер сертифіката, що скасовується;

- причина скасування сертифіката;

- дата та підпис Користувача (уповноваженого представника юридичної особи), відбиток печатки Користувача (за наявності), КЕП/УЕП Користувача – для заяви в електронній формі.

Електронний запит на скасування сертифіката формується Користувачем (або уповноваженим представником юридичної особи) через Систему Вчасно.КЕП та передається у ПТК Надавача у вигляді HTTP-запиту. Електронний запит на скасування сертифіката засвідчується КЕП користувача (уповноваженого представника юридичної особи). Обробка електронного запиту та інформування Користувача про скасування здійснюються в режимі реального часу, цілодобово.

Прийняття та опрацювання заяв в паперовій формі на скасування сертифіката ключа здійснюються посадовими особами в робочий час Надавача 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 кваліфікованого сертифіката встановлюється час офіційного повідомлення Користувача про скасування його кваліфікованого сертифіката, шляхом публікації СВС.

5.6.2 Блокування

Блокування кваліфікованого сертифіката Користувача виконується Надавачем на підставі заяви, яка надходить установленим порядком до пунктів реєстрації Надавача в усній або паперовій формі чи у вигляді електронного запиту через систему Вчасно.КЕП.

Заява в усній формі подається Надавачу по телефону. Заявник повинен повідомити адміністратору реєстрації Надавача наступну інформацію:

- ідентифікаційні дані власника сертифіката;
- ключову фразу парольної автентифікації;
- реєстраційний номер сертифіката.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу парольної фрази переданої в заяві з інформацією з реєстру Користувачів). Обробка усної заяви на блокування сертифіката та інформування Користувача здійснюється протягом часу не більше 2 (двох) годин з моменту подачі заяви. Подача і обробка усної заяви здійснюється у робочий час.

Електронний запит на блокування сертифіката формується Користувачем (або уповноваженим представником юридичної особи) через систему Вчасно.КЕП та передається у ПТК Надавача у вигляді HTTP-запиту. Електронний запит на блокування сертифіката засвідчується власним КЕП Користувача (уповноваженого представника юридичної особи). Обробка електронного запиту та інформування Користувача про блокування здійснюються в режимі реального часу, цілодобово.

Кваліфікований сертифікат користувача скасовується Надавачем в автоматичному режимі через 7 (сім) робочих днів з моменту блокування, якщо впродовж цього часу Користувачем не було надано заяву на відновлення кваліфікованого сертифіката в усній або паперовій формі.

Заява про блокування кваліфікованого сертифіката на паперовому носії засвідчується власноручним підписом Користувача. Подання та розгляд заяви про блокування кваліфікованого сертифіката Користувача на паперовому носії виконується в пункті реєстрації Надавача тільки у робочий час.

Користувач повинен внести до заяви про блокування в паперовій формі, наступні відомості:

- ідентифікаційні дані Користувача кваліфікованого сертифіката;
- унікальний реєстраційний номер кваліфікованого сертифіката;
- -
- дату та час подання заяви.

Опрацювання письмової заяви про блокування кваліфікованого сертифіката та повідомлення Користувача про блокування кваліфікованого сертифіката повинні бути виконані не пізніше 2-х годин, після подання заяви до Надавача.

Часом блокування кваліфікованого сертифіката встановлюється час внесення його до списку заблокованих кваліфікованих сертифікатів Надавача.

5.6.3 ПоновленняЗаблокований кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин поновлюється Надавачем у раз настання обставин передбачених в таблиці 8:

- поновлення чинності сертифіката ключа можливе лише для сертифікатів, що заблоковані і термін блокування не скінчився;
- скасовані сертифікати поновленню не підлягають.

Для здійснення процедури поновлення кваліфікованого сертифіката Користувач подає заяву до пунктів реєстрації Надавача в усній або паперовій формі чи у вигляді електронного запиту через систему Вчасно.КЕП

Заява в усній формі подається цілодобово по каналам зв'язку, що повідомляються Надавачем Користувачам в тому числі шляхом розміщення на офіційному веб-сайті Надавача. Заява в усній формі про поновлення кваліфікованого сертифіката приймається тільки у випадку позитивної автентифікації (збігу парольної фрази переданої в заяві з інформацією з реєстру Користувачів). Обробка заяви в усній формі на поновлення сертифіката та інформування Користувача здійснюється протягом часу не більше 2 (двох) годин з моменту подачі заяви.

Для Користувачів, що маю діючий кваліфікований сертифікат електронного підпису, можливе подання електронного запиту на поновлення сертифікату. Електронний запит підписується кваліфікованим електронним підписом Користувача (уповноваженого представника юридичної особи), та приймається в обробку за умови позитивної ідентифікації особи за таким сертифікатом. Електронний запит на поновлення сертифіката формується Користувачем (або уповноваженим представником юридичної особи) через систему Вчасно.КЕП та передається у ПТК Надавача у вигляді HTTP-запиту. Обробка електронного запиту та інформування Користувача про поновлення здійснюються в режимі реального часу, цілодобово.Заява про поновлення кваліфікованого сертифіката на паперовому носії засвідчується власноручним підписом Користувача. Подання та розгляд письмової заяви про поновлення кваліфікованого сертифіката Користувача виконується Надавачем в робочий час.Опрацювання та виконання заяви на паперовому носії здійснюється не пізніше 2-х годин, після подання заяви до Надавача
.

Користувач повинен внести до заяви, наступні відомості:

- ідентифікаційні дані Користувача кваліфікованого сертифіката;
- унікальний реєстраційний номер кваліфікованого сертифіката;
- дату та час подання заяви.

5.7. Частота формування списку відкликаних сертифікатів та строки його дії

Повний та частковий СВС формуються згідно положень наведених у п. 4.4.2 цього Регламенту.

Строки дії СВС зазначається у самих СВС та вказується на початок формування даного СВС та наступного.

5.8. Інформація про статус кваліфікованого сертифіката відкритого ключа у режимі реального часу

Інформація про зміну статусу кваліфікованого сертифіката розповсюджується шляхом формування та публікації Надавачем списків відкликаних сертифікатів та за он-лайн протоколом визначення статусу сертифіката (OCSP).

У випадку компрометації або загрози компрометації особистого ключа Користувач повинен виконати процедуру блокування або скасування кваліфікованого сертифіката.

5.9 Строк закінчення дії кваліфікованого сертифіката відкритого ключа Надавача та Користувача

5.9.1 Строки дії сертифікатів ключів Надавача

Максимальний термін дії сертифікатів ключів Надавача не більший ніж 5 (п'ять) років, сертифікатів ключів його уповноважених посадових осіб — не більше ніж 2 (два) роки.

Початком строку дії особистого ключа Надавача вважається дата та час формування кваліфікованих сертифікатів для відповідної ключової пари

Після закінчення терміну чинності сертифіката Надавача особистий ключ Надавача та всі його резервні копії знищуються методом, що не допускає можливості їх відновлення.

Після закінчення терміну чинності сертифікатів уповноважених посадових осіб Надавача, відповідні ключі знищуються методом, що не допускає можливості їх відновлення.

5.9.2 Строки дії ключів Користувачів

Строк дії ключів визначається строком дії кваліфікованого сертифікату відкритого ключа.

Максимальний строк дії (чинності) кваліфікованого сертифікату відкритого ключа Користувачів становить не більше ніж 2 (два) роки.

Дата та час початку та закінчення строку дії кваліфікованого сертифіката відкритого ключа Користувача зазначається у сертифікаті із точністю до однієї секунди.

Зі закінченням строку чинності кваліфікованого сертифіката відкритого ключа Користувача, такий кваліфікований сертифікат автоматично скасовується.

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

6.1 Надання засобів КЕП

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

Засоби КЕП надаються Надавачем у вигляді апаратно-програмних засобів, окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, або доступу до частини ресурсу засобу кваліфікованого електронного підпису чи печатки, який знаходиться у Надавача та реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережний криптомодуль).

Надання Надавачем засобів КЕП окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватися шляхом передачі цих засобів на носіях інформації безпосередньо Користувачеві або шляхом надання доступу через офіційний інформаційний ресурс Надавача, або завдяки сервісам Надавача.

Надавач забезпечує надання Користувачам засобів КЕП для ініціювання генерації ключів, а також створення, перевірки та підтвердження КЕП шляхом розміщення відповідних інсталяційних пакетів на офіційному веб-сайті Надавача або завдяки сервісам Надавача.

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

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається Користувачам при створенні КЕП, та 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 Центральним засвідчувальним органом.

6.3 Припинення діяльності Надавача

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

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

Центральний засвідчувальний орган скасовує виданий ним кваліфікований сертифікат відкритого ключа Надавача у день, визначений Надавачем як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, чи у день набрання законної сили відповідним рішенням суду.