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

_____ **О.М. Чаузов**

"10" ____ 2019 р.

ЗАТВЕРДЖУЮ
Директор ТОВ «Арт-мастер»

_____ **В.О. Ковальська**

"06" ____ 2019 р.

РЕГЛАМЕНТ РОБОТИ

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

Київ-2019

Зміст

1. СФЕРА ЗАСТОСУВАННЯ

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

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

Вимоги Регламенту є обов'язковими для юридичних та фізичних осіб – представників органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій незалежно від їх організаційно-правової форми та форми власності, що задіяні у впровадженні та забезпеченні функціонування систем електронного документообігу з моменту їх звернення до Кваліфікованого надавача за отриманням установленим порядком зазначеної послуги до завершення терміну дії підписаного між ними відповідного договору.

Визнання вимог цього Регламенту користувачами електронних довірчих послуг є обов'язковою умовою та підставою для укладання Кваліфікованим надавачем договорів про надання кваліфікованих електронних довірчих послуг.

Положення цього Регламенту поширюються в електронній формі шляхом розміщення на офіційному електронному інформаційному ресурсі Кваліфікованого надавача. Будь-яка заінтересована особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі Кваліфікованого надавача.

Суб'єктами правових відносин у сфері електронних довірчих послуг, що обумовлюються цим регламентом є Центральний засвідчувальний орган (далі – ЦЗО), Кваліфікований надавач, підписувачі та користувачі.

2. НОРМАТИВНІ ПОСИЛАННЯ

В документі є посилання на такі нормативно-правові документи:

- Закон України «Про електронні довірчі послуги» від 05.10.2017р. № 2155-VIII;
- Закон України «Про електронні документи та електронний документообіг» від 22.05.2003р. № 851-VI;
- Закон України «Про захист персональних даних» від 1.06.2010 р. № 2297 - VI;
- Постанова Кабінету Міністрів України від 7.11. 2018 р. № 992 «Про затвердження Вимог у сфері електронних довірчих послуг».

3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

В Регламенті використано терміни, встановлені в Законі України «Про електронні довірчі послуги» та документах, зазначених у пункті 2 цього Регламенту.

4. ПОЗНАЧКИ ТА СКОРОЧЕННЯ

ВПР - віддалений (відокремлений) пункт реєстрації;
ЕДП - електронна довірча послуга;
ЄДДР - єдиний державний демографічний реєстр;
ЄДР - єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань;
ЄДРПОУ - єдиний державний реєстр підприємств та організацій України;
ІТС - інформаційно-телекомунікаційна система;
КЕП - кваліфікований електронний підпис;
КЗІ - криптографічній захист інформації;
КСЗІ - комплексна система захисту інформації;
НД ТЗІ - нормативний документ з технічного захисту інформації;
НКІ - носій ключової інформації;
ПІБ - прізвище ім’я по батькові;
ПТК - програмно-технічний комплекс;
РС - робоча станція;
СВС - список відкликаних сертифікатів;
СЗІ - служба захисту інформації;
СКБД - система керування базами даних;
ОС - операційна система;
ЦЗО - центральний засвідчувальний орган;
ЦПХ - цивільно-правового характеру (договір);
СМР - сервер обробки запитів;
HTTP - Hyper Text Transfer Protocol (протокол прикладного рівня, що використовується для передавання гіпертексту);
LDAP - Lightweight Directory Access Protocol (полегшений протокол доступу до директорій/протоколів);
NTP - Network Time Protocol (мережевий протокол синхронізації внутрішнього годинника комп'ютера);
OCSP - Online Certificate Status Protocol (протокол визначення статусу сертифіката ключа);
OLS - Online Service;
PKCS - Public Key Cryptography Standards (стандарти криптографії з відкритими ключами);
TSP - Time Stamp Protocol (протокол фіксування часу);
URL - Unique Resource Locator (унікальна адреса інформаційного ресурсу в телекомунікаційній мережі);
UTC - Coordinated Universal Time (всесвітній координований час).

5. ЗАГАЛЬНІ ПОЛОЖЕННЯ

5.1. Ідентифікаційні дані Кваліфікованого надавача

Країна	Україна
Назва області	Київська
Назва міста	Київ
Повне найменування організації	Товариство з обмеженою відповідальністю «Арт-мастер»
Повне найменування Кваліфікованого надавача	Кваліфікований надавач електронних довірчих послуг «MASTERKEY» ТОВ «АРТ-МАСТЕР»
Місцезнаходження організації:	03035, Київ, вул. Сурикова 3, (літ. А)
Код ЄДРПОУ:	30404750
Телефон:	+380 44 206 13 78
Факс:	+380 44 206 13 79
Адреса електронної пошти (e-mail):	info@masterkey.ua

5.2. Порядок внесення змін та доповнень

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

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

Про внесення змін та доповнень до цього Регламенту Кваліфікований надавач повідомляє користувачів та інших зацікавлених осіб офіційним повідомленням.

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

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

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

5.3. Порядок публікації

Положення цього Регламенту розповсюджується в електронній формі: з веб-сайту Кваліфікованого надавача за адресою https://www.masterkey.ua та засобами електронної пошти від уповноваженої особи Кваліфікованого надавача, а також через поштову адресу: 03035, Київ, вул. Сурикова 3, (літ. А)

6. КВАЛІФІКОВАНІ ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ, ЩО НАДАЮТЬСЯ КВАЛІФІКОВАНИМ НАДАВАЧЕМ

6.1. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису та печатки

Кваліфікована електронна довірча послуга щодо створення, перевірки та підтвердження кваліфікованого електронного підпису та печатки, яка надається Кваліфікованим надавачем, включає надання користувачам електронних довірчих послуг засобів кваліфікованого електронного підпису та печатки для генерації пар ключів, створення кваліфікованих електронних підписів та печаток, перевірки кваліфікованих електронних підписів та печаток, а також зберігання особистого ключа кваліфікованого електронного підпису та печатки.

Окрім зазначеного, Кваліфікований надавач надає технічну підтримку та обслуговування зазначених засобів кваліфікованого електронного підпису та печатки.

Надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів та печаток передбачає, що така послуга:

- надається виключно Кваліфікованим надавачем;

- відповідає усім вимогам до перевірки кваліфікованих електронних підписів та печаток;

- дає змогу отримувати результати перевірки із застосуванням кваліфікованого електронного підпису та печатки Кваліфікованого надавача автоматизованим способом, який є надійним, ефективним та захищеним.

Під час надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів та печаток Кваліфікований надавач повинен забезпечити:

- використання підписувачем та створювачем електронної печатки виключно засобу кваліфікованого електронного підпису та печатки, та кваліфікованого сертифіката електронного підпису та печатки;

- захист обміну інформацією між підписувачем та створювачем електронної печатки, та Кваліфікованим надавачем засобами телекомунікаційних мереж загального користування;

- створення умов для генерації пари ключів підписувача або створювача електронної печатки;

- надання допомоги підписувачу та створювачу електронної печатки під час генерації ними пари ключів у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

- унікальність пари ключів підписувача та створювача електронної печатки;

- зберігання на захищеному носії особистого ключа підписувача та створювача електронної печатки;

- захист від доступу сторонніх осіб до параметрів особистого ключа підписувача та створювача електронної печатки під час використання засобу кваліфікованого електронного підпису та печатки.

У разі, коли пара ключів була згенерована заявником поза приміщенням Кваліфікованого надавача, Кваліфікований надавач перевіряє достатність обсягу цивільної правоздатності і дієздатності заявника, формує та надає заявнику кваліфікований сертифікат

відкритого ключа після перевірки факту володіння ним особистим ключем, який відповідає згенерованому відкритому ключу.

Перевірка факту володіння заявником особистим ключем здійснюється без розкриття його особистого ключа, яким заявник підписує запит на формування сертифіката.

Кваліфікований надавач, який здійснює управління парою ключів підписувача або створювача електронної печатки, у разі обґрунтованої необхідності може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки за умови, що рівень безпеки резервної копії особистого ключа відповідає рівню безпеки оригінального особистого ключа, а кількість резервних копій не перевищує обґрунтованої мінімально - необхідної потреби.

Кваліфікований електронний підпис та печатка повинні відповідати таким вимогам:

- встановлювати однозначний зв'язок з підписувачем та створювачем електронної печатки;

- надавати можливість можливість здійснення електронної ідентифікації підписувача та створювача електронної печатки;

- забезпечувати одноосібний контроль підписувача або створювача електронної печатки за відповідним особистим ключем;

- виявляти будь-які зміни пов'язаних електронних даних, на які накладено кваліфікований електронний підпис та печатку.

Перевірка кваліфікованого електронного підпису та печатки може ініціюватись та здійснюватись будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого електронного підпису та печатки.

Кваліфікований електронний підпис та печатка вважаються такими, що пройшли перевірку та отримали підтвердження, якщо:

- перевірку кваліфікованого електронного підпису та печатки проведено засобом кваліфікованого електронного підпису та печатки;

- перевіркою встановлено, що відповідно до вимог Закону України «Про електронні довірчі послуги» на момент створення кваліфікованого електронного підпису та печатки був чинним кваліфікований сертифікат електронного підпису та печатки підписувача та створювача електронної печатки;

- за допомогою кваліфікованого сертифіката електронного підпису та печатки здійснено ідентифікацію підписувача та створювача електронної печатки;

- під час перевірки за допомогою кваліфікованого сертифіката електронного підпису та печатки отримано підтвердження того, що особистий ключ, який належить підписувачу та створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису та печатки;

- під час перевірки підтверджено цілісність електронних даних в електронній формі, з якими пов'язаний цей кваліфікований електронний підпис та печатка.

Відповідність засобів кваліфікованого електронного підпису та печатки зазначеним вимогам підтверджується документами про відповідність або позитивними експертними висновками за результатами їх державної експертизи у сфері криптографічного та технічного захисту інформації.

6.2. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису та печатки

Формування кваліфікованого сертифіката електронного підпису та печатки заявника здійснюється Кваліфікованим надавачем на основі ідентифікаційних даних особи, одержаних від заявника під час його ідентифікації та перевірки достатності обсягу його цивільної правоздатності та дієздатності.

В процесі надання електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису та печатки Кваліфікований надавач повинен забезпечити:

- унікальність серійного номера кваліфікованого сертифіката електронного підпису та печатки заявника щодо інших кваліфікованих сертифікатів електронного підпису та печатки, сформованих цим самим Кваліфікованим надавачем;

- збереження усіх сформованих ним кваліфікованих сертифікатів електронного підпису та печатки, а також їх резервних копій;

- створення умов для генерації пари ключів особисто підписувачем та створювачем (уповноваженим представником створювача) електронної печатки за допомогою засобу кваліфікованого електронного підпису та печатки;

- формування кваліфікованих сертифікатів електронного підпису та печатки, та надання їх отримувачу електронної довірчої послуги;

- скасування, блокування та поновлення кваліфікованих сертифікатів електронного підпису та печатки у порядку та за умов, наведених у підрозділах 9.13 та 9.14 цього Регламенту;

- перевірку та підтвердження чинності кваліфікованих сертифікатів електронного підпису та печатки шляхом надання третім особам інформації про їхній статус та відповідність вимогам Закону України «Про електронні довірчі послуги»;

- надання доступу до сформованих кваліфікованих сертифікатів електронних підписів та печаток шляхом їх розміщення на офіційному веб-сайті Кваліфікованого надавача, за умови згоди підписувача та створювача електронної печатки на публікацію кваліфікованого сертифіката електронного підпису та печатки;

- цілісність та походження інформації про статус кваліфікованих сертифікатів електронного підпису та печатки.

Повторне формування кваліфікованого сертифіката електронного підпису та печатки користувача Кваліфікований надавач здійснює у порядку та за умов, наведених у підрозділах 9.10 та 9.11 цього Регламенту.

6.3. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу.

Позначка часу - сукупність електронних даних, створена за допомогою технічних засобів ПТК ІТС, яка підтверджує наявність електронного документа (електронних даних) на певний момент часу.

Послуга фіксування часу - процедура засвідчення наявності електронного документа (електронних даних) на певний момент часу шляхом додання до нього або логічного поєднання з ним позначки часу.

Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає формування кваліфікованої електронної позначки часу та її надання користувачеві.

Послуга фіксування часу надається Кваліфікованим надавачем усім користувачам за їх запитами.

Зазначена послуга надається шляхом надсилання Кваліфікованим надавачем відповідного запиту на TSP-сервер.

Сформовані позначки часу засвідчуються КЕП TSP-сервера.

Формат запиту на TSP-сервер Кваліфікованого надавача та відповіді TSP-сервера відповідають вимогам спільного наказу Міністерства юстиції України та Державної служби спеціального зв'язку та захисту інформації від 20.08.2012 № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису».

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.

Послуга фіксування часу надається цілодобово.

Під час формування кваліфікованої електронної позначки часу підписувач та Кваліфікований надавач з використанням засобів кваліфікованого електронного підпису та печатки вчиняють наступні дії:

1. Підписувач обчислює геш-значення електронних даних, на які необхідно сформувати кваліфіковану електронну позначку часу, та створює запит на формування кваліфікованої електронної позначки часу, який містить:

- обчислене геш-значення;

- об’єктний ідентифікатор політики формування позначки часу (необов’язково);

- ідентифікатор алгоритму гешування, що використовувався;

- унікальний ідентифікатор запиту (необов’язково);

- необов’язкові розширення;

- підписувач передає сформований запит Кваліфікованому надавачу.

2. Кваліфікований надавач перевіряє правильність формату запиту та здійснює його обробку, формує кваліфіковану електронну позначку часу та відповідь, що містить кваліфіковану електронну позначку часу, або відповідь з інформацією про відмову у формуванні кваліфікованої електронної позначки часу.

Кваліфікований надавач надсилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, в якій зазначені такі дані:

- об’єктний ідентифікатор політики формування кваліфікованої електронної позначки часу, що була використана;

- геш-значення електронних даних, для яких було сформовано кваліфіковану електронну позначку часу;

- серійний номер кваліфікованої електронної позначки часу;

- час формування кваліфікованої електронної позначки часу;

- додаткову інформацію про кваліфіковану електронну позначку часу;

- кваліфікований електронний підпис та печатку Кваліфікованого надавача, накладені на кваліфіковану електронну позначку часу.

Підписувач після отримання відповіді від Квалифікованого надавача вчиняє такі дії:

- перевіряє результат обробки запиту;

- перевіряє відповідність імені чи найменування суб’єкта, що наклав кваліфікований електронний підпис та печатку на кваліфіковану електронну позначку часу, імені чи найменуванню Кваліфікованого надавача;

- перевіряє відповідність призначення кваліфікованого сертифіката відкритого ключа Кваліфікованого надавача (для формування позначки часу);

- перевіряє чинність кваліфікованого сертифіката відкритого ключа Кваліфікованого надавача;

- перевіряє кваліфікований електронний підпис та печатку, що був накладений на кваліфіковану електронну позначку часу;

- перевіряє відповідність електронних даних та даних, для яких була сформована кваліфікована електронна позначка часу (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу);

- додає кваліфіковану електронну позначку часу до електронних даних.

Перевірка кваліфікованої електронної позначки часу може ініціюватись та проводитись будь-якою особою з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

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

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

- перевіряє кваліфікований електронний підпис та печатку, накладені на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката відкритого ключа Кваліфікованого надавача;

- перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу).

Кваліфікована електронна позначка часу вважається недійсною у разі недотримання вимоги щодо точності часу в програмно-технічному комплексі Кваліфікованого надавача та використання скасованого або блокованого кваліфікованого сертифіката відкритого ключа Кваліфікованого надавача на момент формування кваліфікованої електронної позначки часу.

Коректність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в засобі кваліфікованого електронного підпису та печатки, забезпечує протокол фіксування часу.

Механізм синхронізації часу із Всесвітнім координованим часом (далі - UTC) в програмно-технічному комплексі Кваліфікованого надавача та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із UTC, який розроблено Кваліфікованим надавачем та погоджено із ЦЗО.

Програмний комплекс сервера синхронізації часу реалізовано у вигляді системної служби. Встановлення параметрів та запуск програмного комплексу сервера синхронізації часу здійснюється локально, а запуск NTP- сервера виконується автоматично при завантаженні операційної системи (далі - ОС).

Комплекс засобів синхронізації часу забезпечує отримання сигналів синхронізації часу з NTP-сервера ІТС ЦЗО, резервних NTP-серверів, синхронізованих з державним еталоном одиниць часу і частоти, та синхронізацію системного часу на технічних засобах ПТК Кваліфікованого надавача.

До складу клієнтської частини комплексу входять програмні компоненти клієнта синхронізації часу - штатні NTP-клієнти різних ОС, під керуванням яких функціонують робочі станції (далі – РС) та сервери Кваліфікованого надавача.

Штатні NTP-клієнти ОС реалізовані у вигляді системних служб [ОС Microsoft Windows] або демонів (ОС FreeBSD). Запуск NTP-клієнтів виконується автоматично ОС при її завантаженні.

До складу комплексу входять його компоненти:

– NTP-сервер ІТС ЦЗО (основний);

– NTP-сервери ІТС ЦЗО (резервні);

– NTP-сервер Кваліфікованого надавача;

– засоби та обладнання каналоутворення;

– РС системного адміністратора Кваліфікованого надвача - внутрішній резервний NTP-сервер синхронізації часу ПТК Кваліфікованого надавача;

– РС та сервери Кваліфікованого надавача із штатними програмними NTP-серверами та NTP-клієнтами ОС.

Сервер взаємодії Кваліфікованого надавача виступає в ролі клієнта NTP-сервера ЦЗО або в ролі клієнта резервного NTP-сервера ЦЗО, та є основним NTP-сервером для ПТК Квіліфікованого надавача. В разі виходу з ладу основного NTP-сервера ЦЗО, в якості NTP-сервера виступають резервні NTP-сервери ЦЗО.

У разі недоступності NTP-сервера ІТС ЦЗО синхронізація часу здійснюється із підключенням до резервних NTP-серверів, синхронізованими з державним еталоном одиниць часу і частоти, що вказані у параметрах NTP-сервера Кваліфікованого надавача, або з резервним NTP-сервером для сервера взаємодії Кваліфікованого надавача.

Резервний NTP-сервер Кваліфікованого надавача у якості джерела точного часу використовує GPS – приймач, який підключено до РС адміністратора системи.

Позначки точного часу отримуються у всесвітній шкалі UTC із точністю до 1 (однієї) секунди.

Основним джерелом часу для засобів Кваліфікованого надавача є NTP-сервер сервера взаємодії Кваліфікованого надавача. Всі РС та сервери підключаються до NTP-сервера Кваліфікованого надавача та синхронізують системний годинник у відповідності до значення часу, що отримується від нього.

Штатні програмні NTP-клієнти операційної системи налагоджуються на всіх РС та серверах ЛОМ на отримання часу від NTP-сервера Кваліфікованого надавача за протоколом NTP. NTP-клієнти здійснюють підключення до NTP-сервера та отримують значення точного часу і виконують встановлення власного системного часу (системного годинника).

Синхронізація часу здійснюється не рідше одного разу кожних 15 хвилин.

7. СУБ'ЄКТИ ТА ОБ'ЄКТИ ОБСЛУГОВУВАННЯ ЗАЯВНИКІВ

7.1. Інформаційно-телекомунікаційна система Кваліфікованого надавача електронних довірчих послуг

ІТС Кваліфікованого надавача створена у вигляді розподіленого багатомашинного комплексу, який реалізує інформаційну технологію та об'єднує обчислювальну систему, фізичне середовище (приміщення, інженерні комунікації та обладнання), а також персонал та оброблювану інформацію.

До складу ІТС входять наступні технічні засоби:

– сервери віртуалізації (центральні сервери, сервери взаємодії, сервер резервного копіювання тощо);

– робочі станції (далі – РС) адміністраторів (адміністратора безпеки та аудиту, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації) в тому числі РС адміністраторів віддалених (відокремлених) пунктів реєстрації;

– внутрішнє комунікаційне обладнання та обладнання каналоутворення;

– РС генерації ключів користувачів (ізольовані).

Сервери ІТС, об'єднані в єдине віртуальне середовище, під управлінням гіпервізора, що входить до складу програмного забезпечення системи віртуалізації, реалізують виконання регламентних процедур та механізмів, пов'язаних з обслуговуванням кваліфікованих сертифікатів, зокрема:

– реєстрацію заявників;

– сертифікацію відкритих ключів підписувачів;

– управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;

– надання послуг фіксування часу;

– надання користувачам засобів КЕП та шифрування даних, а також засобів генерації особистих та відкритих ключів;

– надання допомоги під час генерації особистих та відкритих ключів користивачами;

– надання консультаційних послуг КЕП за зверненнями підписувачів.

Безпосереднє виконання зазначених функцій здійснюється програмно-технічним комплексом (далі – ПТК), при цьому криптографічні перетворення інформації здійснюються з використанням засобів кваліфікованого цифрового підпису та печатки, створених з використанням наступних стандартів:

– ДСТУ 4145-2002 - накладання та перевірки електронного підпису;

– ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 – шифрування даних;

– ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 – обчислення імітовставки;

– ГОСТ 34.311-95 та ДСТУ 7564:2014 – обчислення геш-функції.

7.2. Наймані працівники, чиї обов'язки пов'язані з наданням кваліфікованих довірчих послуг.

В сфері застосування цього Регламенту під найманими працівниками Кваліфікованого надавача маються на увазі посадові особи Кваліфікованого надавача та його структурних підрозділів, досвід роботи яких та кваліфікація відповідають «Вимогам у сфері електронних довірчих послуг», Постанова Кабінету Міністрів України від 7 листопада 2018 р. № 992 "Про затвердження Вимог у сфері електронних довірчих послуг".

Найманими працівниками Кваліфікованого надавача, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, є:

1) адміністратор реєстрації;

2) адміністратор сертифікації;

3) адміністратор безпеки та аудиту;

4) системний адміністратор.

7.2.1. Адміністратор реєстрації

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

Основними обов'язками адміністратора реєстрації є:

1) ідентифікація та автентифікація заявників;

2) перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;

3) встановлення належності відкритого ключа та відповідного йому особистого ключа заявнику;

4) ведення обліку користувачів.

7.2.2. 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 Кваліфікованого надавача, а також створення їх резервних копій.

Основними обов'язками адміністратора сертифікації є:

1) участь у генерації пар ключів Кваліфікованого надавача та створенні резервних копій особистих ключів Кваліфікованого надавача;

2) зберігання особистих ключів Кваліфікованого надавача та їх резервних копій;

3) забезпечення використання особистих ключів Кваліфікованого надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів Кваліфікованого надавача та користувачів;

4) перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів Кваліфікованого надавача на відповідність вимогам регламенту роботи Кваліфікованого надавача;

5) участь у знищенні особистих ключів Кваліфікованого надавача;

6) забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів підписувачів;

7) забезпечення публікації кваліфікованих сертифікатів відкритих ключів користувачів та списків відкликаних сертифікатів на офіційному веб-сайті Кваліфікованого надавача;

8) створення резервних копій кваліфікованих сертифікатів відкритих ключів підписувачів;

9) зберігання кваліфікованих сертифікатів відкритих ключів підписувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІТС Кваліфікованого надавача.

7.2.3. Адміністратор безпеки та аудиту

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

Основними обов'язками адміністратора безпеки та аудиту є:

1) участь у генерації пар ключів Кваліфікованого надавача та створенні резервних копій особистих ключів Кваліфікованого надавача;

2) контроль за формуванням, обслуговуванням і створенням резервних копій кваліфікованих сертифікатів відкритих ключів Кваліфікованого надавача, користувачів та списків відкликаних сертифікатів;

3) контроль за зберіганням особистих ключів Кваліфікованого надавача та їх резервних копій, особистих ключів адміністраторів;

4) участь у знищенні особистих ключів Кваліфікованого надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;

5) організація розмежування доступу до ресурсів ІТС Кваліфікованого надавача;

6) забезпечення спостереження за функціонуванням комплексної системи захисту інформації або системи управління інформаційною безпекою (реєстрація подій в ІТС Кваліфікованого надавача, моніторинг подій тощо);

7) забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою після збоїв, відмов, аварій ІТС Кваліфікованого надавача;

8) забезпечення режиму доступу до приміщень Кваліфікованого надавача, в яких розміщена ІТС Кваліфікованого надавача;

9) ведення журналів обліку адміністратора безпеки та аудиту, визначених документацією на комплексну систему захисту інформації або звітності, що передбачена системою управління інформаційною безпекою;

10) проведення перевірок журналів аудиту подій, що реєструють технічні засоби ІТС Кваліфікованого надавача;

11) проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації Кваліфікованого надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою;

12) контроль за дотриманням найманими працівниками Кваліфікованого надавача положень внутрішньої організаційно-розпорядчої документації Кваліфікованого надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою;

13) контроль за веденням баз даних Кваліфікованого надавача;

14) контроль за веденням архіву Кваліфікованого надавача.

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

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

7.2.4. Адміністратор системи

Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу (далі – технічні засоби) ІТС Кваліфікованого надавача.

Основними обов’язками системного адміністратора є:

1) організація експлуатації та технічного обслуговування ІТС Кваліфікованого надавача і адміністрування її технічних засобів;

2) забезпечення функціонування офіційного веб-сайту Кваліфікованого надавача;

3) участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою;

4) ведення журналів аудиту подій, що реєструють технічні засоби ІТС Кваліфікованого надавача;

5) встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІТС Кваліфікованого надавача;

6) встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІТС Кваліфікованого надавача;

7) забезпечення актуалізації баз даних, створюваних та оброблюваних в ІТС Кваліфікованого надавача, у зв'язку із збоями.

7.3. Підписувачі та користувачі

Послугами Кваліфікованого надавача користуються підписувачі та користувачі.

Підписувачі мають договірні відносини з Кваліфікованим надавачем, на законних підставах володіють особистими ключами, мають відповідні відкриті ключі та сформовані Кваліфікованим надавачем сертифікати відкритих ключів.

У договорі про надання послуг повинні бути визначені:

- обов'язки сторін, у тому числі ті, що стосуються використання засобів кваліфікованого електронного підпису (далі – КЕП);
- умови надання доступу користувачам до сертифіката підписувача (умови публікації сертифіката);
- обмеження щодо використання сертифіката.

Форми та зразки договорів для різних категорій підписувачів розміщені на офіційному сайті Кваліфікованого надавача.

Користувачі не мають договірних відносин з Кваліфікованим надавачем, однак, при цьому, можуть використовувати загальнодоступну інформацію з електронного інформаційного ресурсу Кваліфікованого надавача, а також користуватися низкою послуг Кваліфікованого надавача, що не потребують автентифікації.

7.4. Віддалені (відокремлені) пункти реєстрації

Для здійснення заходів, спрямованих на обслуговування заявників в різних регіонах можуть утворюватись віддалені (відокремлені) пункти реєстрації та/або відряджатись адміністратори реєстрації для надання клієнтам таких послуг.

Впровадження ВПР передбачається підпунктом 5 пункту 1 Статті 1 Закону України «Про електронні довірчі послуги» і може утворюватись як філія чи підрозділ Кваліфікованого надавача, або функціонувати на підставі договору, укладеного, Кваліфікованим надавачем з фізичною особою, з фізичною особою – підприємцем або з юридичною особою.

Завдання і функції, що покладаються на ВПР, можуть виконуватися як в повному обсязі вимог статті 7.2 Регламенту, так і частково.

В залежності від обсягу завдань і функцій, покладених на конкретного ВПР, вони можуть виконуватися як з доступом до ресурсів ПТК ІТС, так і без такого доступу.

У разі надання ВПР доступу до електронного ресурсу ПТК ІТС обслуговування заявників виконують наймані працівники Кваліфікованого надавача, а покладений на них обсяг завдань і функцій визначається посадовими інструкціями. Відповідальність за виконання вимог стосовно захисту інформації покладається на Кваліфікованого надавача.

У разі відсутності доступу ВПР до ПТК ІТС зазначені вимоги не застосовуються, а функції та завдання ВПР, в тому числі завдання захисту інформації, можуть виконувати спеціально уповноважені на такі дії фізичні особи, фізичні особи - підприємці або посадові особи юридичних осіб (далі – уповноважені особи).

Свою діяльність уповноважені особи здійснюють на підставі та в обсязі договорів цивільно-правового характеру, корпоративних та дилерських договорів тощо, які укладають фізичні особи, фізичні особи - підприємці чи юридичні особи з Кваліфікованим надавачем.

Об’єктом захисту у цьому випадку є персональні дані, що надаються заявником для здійснення процедур його обслуговування уповноваженою особою, а відповідальність за їх захист згідно з вимогами статті 24 Закону України «Про захист персональних даних» покладається на ВПР.

Послуги можуть надаватися ВПР як у приміщеннях, що належать/використовуються Кваліфікованим надавачем, так і в інших приміщеннях.

Інформація про місця розташування ВПР та їх контактні дані публікуються на сайті Кваліфікованого надавачача.

8. ПОЛІТИКА СЕРТИФІКАТА

8.1. Типи сертифікатів та сфери їх використання

В ПТК ІТС формуються наступні типи сертифікатів:

- сертифікат Кваліфікованого надавача, призначений для перевірки підпису на сертифікатах та на списках відкликаних сертифікатів;
- сертифікати посадових осіб Кваліфікованого надавача, призначені для ідентифікації та автентифікації посадових осіб Кваліфікованого надавача та/або перевірки КЕП посадових осіб;
- сертифікати серверів Кваліфікованого надавача, що використовуються при перевірці КЕП на відповідях, які формують сервери ПТК: позначки часу (TSP), інформація про статус сертифіката (OCSP) тощо;
- сертифікати підписувачів Кваліфікованого надавача, що використовуються для перевірки КЕП їх власників та/або у якості ідентифікаторів їх власників при забезпеченні доступу до інформаційних ресурсів автоматизованих систем;
- сертифікати шифрування, що використовуються для підтвердження відповідності відкритих ключів підписувачам під час криптографічного захисту інформації шляхом направленого шифрування даних.

8.2. Обмеження щодо використання сертифікатів ключів

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

Кваліфікований надавач має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання сертифіката ключа заноситься до сформованого сертифіката ключа у вигляді уточненого призначення ключа.

Сертифікати Кваліфікованого надавача та серверів Кваліфікованого надавача, а також відповідні їм особисті ключі можуть використовуватись виключно відповідно до їх призначення.

Призначення сертифікатів Кваліфікованого надавача та серверів Кваліфікованого надавача наводиться у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

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

Сертифікати підписувачів та відповідні їм особисті ключі можуть використовуватись виключно відповідно до призначення пакету послуг, який обирає та отримує підписувач при обслуговуванні.

Інформація стосовного обраного підписувачем пакету послуг наводиться у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

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

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

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

8.3. Електронний інформаційний ресурс Кваліфікованого надавача

Електронний інформаційний ресурс Кваліфікованого надавача розташований за адресою www.masterkey.ua та призначений для розміщення відкритої інформації наступного характеру:

– відомості про Кваліфікованого надавача, в тому числі про ВПР (реквізити, адреси, контактні телефони тощо) та інформація щодо внесення Кваліфікованого надавача до Довірчого списку;

– довідкова інформація (режими роботи Кваліфікованого надавача, положення цього Регламенту тощо);

– договори на надання електронних довірчих послуг, форми та зразки документів, тощо;

– сертифікати ключів Кваліфікованого надавача;

– сертифікати ключів серверів Кваліфікованого надавача;

– сертифікати ключів підписувачів (за згодою підписувачів);

– списки відкликаних сертифікатів;

– реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

– дані про засоби кваліфікованого електронного підпису та печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;

– опис пакетів електронних довірчих послуг, що надаються Кваліфікованим надавачем, тарифи;

– перелік актів законодавства у сфері електронних довірчих послуг;

– новини та інформативні повідомлення для посадових осіб Кваліфікованого надавача, підписувачів, користувачів та заявників.

Технічною основою електронного інформаційного ресурсу Кваліфікованого надавача є сервери взаємодії, що входять до складу ПТК ІТС.

Довідкова інформація розміщується на HTTP-сервері сервера взаємодії у вигляді набору веб-сторінок.

Сертифікати ключів Кваліфікованого надавача, ключів серверів Кваліфікованого надавача та ключів підписувачів, а також списки відкликаних сертифікатів розміщуються у складі веб-сторінок на HTTP-сервері сервера взаємодії та у інформаційному дереві LDAP-каталогу на LDAP-сервері сервера взаємодії.

Доступ до HTTP-сервера здійснюється за адресою www.masterkey.ua за протоколом HTTP.

Інформація, що публікується на електронному інформаційному ресурсі Кваліфікованого надавача, є загальнодоступною. Кваліфікований надавач застосовує організаційні заходи та використовує технічні засоби захисту від несанкціонованої модифікації цієї інформації.

8.4. Порядок публікації сертифікатів ключів Кваліфікованого надавача та серверів Кваліфікованого надавача

В процесі функціонування Кваліфікований надавач може одночасно використовувати декілька особистих сертифікатів ключів, при цьому усі використовувані Кваліфікованим надавачем сертифікати повинні бути опубліковані на електронному інформаційному ресурсі Кваліфікованого надавача.

Публікація на електронному інформаційному ресурсі Кваліфікованого надавача кожного з використовуваних сертифікатів здійснюється одразу після завершення його формування.

Окрім особистого сертифіката ключа Кваліфікованого надавача на електронному інформаційному ресурсі Кваліфікованого надавача виконується публікація сертифікатів ключів серверів Кваліфікованого надавача, зокрема:

– сервера обробки запитів (CMP-сервера);

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

8.5. Порядок публікації сертифікатів ключів підписувачів

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

Публікація сертифікатів ключів підписувачів у інформаційному дереві LDAP-каталогу здійснюється автоматично з інтервалом синхронізації 15 (п’ятнадцять) хвилин.

8.6. Порядок публікації списків відкликаних сертифікатів

Публікація списків відкликаних сертифікатів на електронному інформаційному ресурсі Кваліфікованого надавача (на HTTP-сервері) здійснюється одразу після їх випуску.

Кваліфікований надавач виконує випуск списків відкликаних сертифікатів двох типів:
– повний список;
– частковий список.

Повний список випускається 1 (один) раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані Кваліфікованим надавачем за весь період його роботи.

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

У списках відкликаних сертифікатів обов’язково зазначається точна дата та час публікації наступного списку відкликаних сертифікатів.

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

8.7. Порядок генерації ключів підписувачів

Відкритий та особистий ключі заявника можуть бути згенеровані заявником на власному робочому місці або на станції генерації ключів Кваліфікованого надавача.

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

В процесі генерації та впродовж використання особистий ключ заявника не покидає меж захищеного носія ключової інформації, захищається паролем і залишається у користувача, який несе відповідальність за забезпечення його конфіденційності та цілісності.

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

При виборі паролю захисту особистого ключа необхідно враховувати наступні рекомендації:
– довжина паролю повинна містити не менше 8 символів;
– символи паролю не повинні повторюватись;
– пароль не повинен містити підряд більше ніж 2 символи з розкладки клавіатури;
– в паролі використовувати наступні символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Після запису особистого ключа на НКІ виводиться вміст простого запиту на формування сертифікату з відкритим ключем КЕП для державних алгоритмів та протоколів.

Запити на формування кваліфікованих сертифікатів підпису та шифрування зберігаються користувачем у форматах: «ПІБ EU-XXXXXXXX.p10» та «ПІБ EU-KEP-XXXXXXXX.p10» відповідно (для електронної печатки замість «ПІБ» зазначається «електронна печатка та ЄДРПОУ юридичної особи»). Розширення файлу запиту (.p10) повинно залишатися без змін.

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

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

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

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

Приклад:

ПІБ EU-6E50VH92.p10;

ПІБ EU-KEP-3R15GT23.p10, де:

– «ПІБ» – прізвище, ім'я, по батькові користувача;

– «EU-6E50VH92.p10» – унікальне ім'я файлу запиту для формування кваліфікованого сертифіката підпису, що створюється за замовчуванням;

– «EU-KEP-3R15GT23.p10» – унікальне ім'я файлу запиту для формування кваліфікованого сертифіката шифрування, що створюється за замовчуванням.

Надання до ВПР сформованих користувачем запитів здійснюється на носії інформації особисто користувачем або уповноваженою особою після процедури ідентифікації та реєстрації заявника.

У разі генерації відкритого та особистого ключів користувача у ВПР ключі генеруються користувачем особисто на станції генерації ключів, що входить до складу ПТК Кваліфікованого надавача.

Особистий ключ користувача генерується на захищений носій особистого ключа та залишається у користувача, а сформовані запити на формування кваліфікованих сертифікатів передаються через службовий носій інформації на робочу станцію адміністратора реєстрації.

Особисті ключі користувачів та паролі захисту до них у Кваліфікованого надавача не зберігаються.

Строк дії особистого ключа користувача становить 1 (один) рік. Початком строку дії особистого ключа вважається дата та час формування кваліфікованого сертифіката, що містить відкритий ключ, відповідний до особистого.

8.8. Порядок подання запиту на сертифікацію

Для формування кваліфікованих сертифікатів використовуються запити на формування кваліфікованих сертифікатів підпису та шифрування, які створюються в процесі генерації особистого та відкритого ключів.

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

Якщо генерація особистих та відкритих ключів була проведена за межами приміщення Кваліфікованого надавача, запити на сертифікацію адміністратору реєстрації надаються користувачем особисто або відповідальною особою.

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

Відкритий і особистий ключі підписувача можуть генеруватись на робочій станції генерації ключів підписувачів у відповідному приміщенні Кваліфікованого надавача або на робочій станції підписувача виключно з використанням засобів КЕП. Відповідальність за конфіденційність особистого ключа під час генерації на робочій станції підписувача повністю несе підписувач.

В процесі генерації ключів створюється особистий ключ, що записується на носій ключової інформації, та запит на формування сертифіката ключа. Запит на формування сертифіката ключа, що передається на сертифікацію до Кваліфікованого надавача, є самопідписаним запитом формату PKCS#10, який засвідчується КЕП за допомогою особистого ключа заявника.

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

8.9. Права та обов'язки підписувача стосовно користування кваліфікованим сертифікатом та особистим ключом ЕДП

Підписувач зобов'язаний:

– ознайомитись та дотримуватись умов надання ЕДП, визначених цим Регламентом та відповідними нормативними документами;

– надавати під час реєстрації повну та достовірну інформацію, необхідну для його ідентифікації та формування кваліфікованих сертифікатів;

– зберігати у таємниці особистий ключ та вживати всіх можливих заходів для запобігання його втрати, розкриття, зміни назви, зміни формату чи несанкціонованого використання;

– не розголошувати іншим особам пароль захисту особистого ключа та ключову фразу голосової автентифікації;

– не розголошувати іншим особам пароль захисту захищеного носія, на якому знаходиться особистий ключ;

– використовувати особистий ключ виключно з метою, визначеною у кваліфікованому сертифікаті та додержуватися інших обмежень щодо сфери використання кваліфікованого сертифіката (за наявності);

– використовувати засоби кваліфікованого електронного підпису та печатки для генерації особистих та відкритих ключів, формування та перевірки кваліфікованого електронного підпису та печатки;

– інформувати Кваліфікованого надавача про події, що трапилися до закінчення строку чинності кваліфікованого сертифіката, зокрема: компрометацію особистого ключа, компрометацію паролю захисту особистого ключа, виявлені неточності або зміну даних, зазначених у кваліфікованому сертифікаті;

– не використовувати особистий ключ у разі його компрометації;

– не використовувати особистий ключ, відповідний до кваліфікованих сертифікатів, заява на скасування чи блокування яких подана до Кваліфікованого надавача, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування кваліфікованих сертифікатів;

– не використовувати для накладання кваліфікованого підпису та печатки скасований або блокований особистий ключ, відповідний до кваліфікованого сертифіката.

Підписувач має право:

– своєчасно отримувати ЕДП;

– цілодобово користуватись вільним доступом до кваліфікованих сертифікатів інших підписувачів, до даних про статус кваліфікованих сертифікатів, до реєстру кваліфікованих

сертифікатів Кваліфікованого надавача та до нормативних документів у сфері надання ЕДП з використанням телекомунікаційних мереж загального користування;

– одержувати кваліфіковані сертифікати Кваліфікованого надавача;

– одержувати списки відкликаних сертифікатів, сформовані Кваліфікованим надавачем;

– застосовувати кваліфікований сертифікат Кваліфікованого надавача для перевірки кваліфікованих сертифікатів, сформованих Кваліфікованим надавачем;

– застосовувати списки відкликаних сертифікатів, сформовані Кваліфікованим надавачем, для перевірки статусу власних кваліфікованих сертифікатів та кваліфікованих сертифікатів інших користувачів;

– ознайомлюватись з інформацією щодо діяльності Кваліфікованого надавача у сфері надання ЕДП;

– подавати заяви та скарги;

– здійснювати скасування, блокування або поновлення кваліфікованих сертифікатів відповідно до вимог Регламенту;

– вимагати від Кваліфікованого надавача усунення наслідків порушення умов та вимог Регламенту та договору про надання ЕДП;

– вимагати від Кваліфікованого надавача виконання вимог захисту персональних даних користувачів;

– оскаржити дії чи бездіяльність Кваліфікованого надавача у судовому порядку.

8.10. Порядок генерації та резервного копіювання ключів Кваліфікованого надавача

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

Генерація особистих ключів Кваліфікованого надавача та особистих ключів серверів Кваліфікованого надавача виконується на сервері Кваліфікованого надавача у спеціальному приміщенні серверів Кваліфікованого надавача двома посадовими особами Кваліфікованого надавача – керівником Кваліфікованого надавача та адміністратором безпеки та аудиту з використанням засобів КЕП.

В процесі генерації ключів Кваліфікованого надавача, здійснюється запис особистого ключа Кваліфікованого надавача у постійний запам’ятовуючий пристрій криптомодуля. Запит на формування сертифіката ключа Кваліфікованого надавача, що містить відкритий ключ, записується на локальний диск центрального сервера Кваліфікованого надавача.

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

Після генерації особистого ключа Кваліфікованого надавача та особистих ключів серверів створюється не менше 2 (двох) резервних копій особистого ключа та особистих ключів серверів. Кожна резервна копія особистого ключа Кваліфікованого надавача та особистих ключів серверів Кваліфікованого надавача записується на захищені носії інформації типу «Кристал-1». Захищені носії інформації з копіями особистого ключа Кваліфікованого надавача та особистих ключів серверів Кваліфікованого надавача зберігаються в тубусах. Доступ до особистого ключа Кваліфікованого надавача має керівник Кваліфікованого надавача, який запечатує тубус своєю печаткою. Доступ до особистих ключів серверів Кваліфікованого надавача має адміністратор безпеки та аудиту, який запечатує тубус своєю печаткою. Резервні копії особистого ключа Кваліфікованого надавача та особистих ключів серверів Кваліфікованого надавача зберігаються в спеціальному приміщенні Кваліфікованого надавача. Резервні копії особистого ключа Кваліфікованого

надавача та особистих ключів серверів Кваліфікованого надавача зберігаються у сейфі, який запечатується керівником Кваліфікованого надавача.

Сформований запит на сертифікат ключа Кваліфікованого надавача та сервера позначок часу (TSP) записується на з'ємний носій та передається адміністратором сертифікації у ЦЗО.

Формування сертифіката ключа Кваліфікованого надавача виконується у ЦЗО згідно з відповідними інструкціями.

Сформований у ЦЗО сертифікат ключа Кваліфікованого надавача та сервера позначок часу (TSP) записується на з'ємний носій та передається адміністратору сертифікації Кваліфікованого надавача.

Формування сертифікатів ключів серверів Кваліфікованого надавача виконується на основному сервері Кваліфікованого надавача в службовому приміщенні Кваліфікованого надавача адміністратором сертифікації у присутності адміністратора безпеки.

Сформовані сертифікати ключів записуються в базу даних відповідного сервера Кваліфікованого надавача.

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

8.11. Умови та порядок реєстрації заявника

8.11.1. Загальні положення

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

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

Допускається ідентифікація заявника Кваліфікованим надавачем за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

Ідентифікація іноземців здійснюється відповідно до законодавства за умови наявності у заявника посвідки на проживання та національного паспорта іноземця або документа, що його замінює.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи Кваліфікований надавач зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань (далі – ЄДР), а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

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

8.11.2. Реєстрація заявника – представника юридичної особи/фізичної особи-підприємця

Для проведення процедури реєстрації юридичних осіб та фізичних осіб-підприємців Кваліфікованому надавачу заявником надаються наступні документи та відомості:

– заповнений та підписаний договір у двох примірниках або заповнену та підписану заявником заяву - приєднання до електронного договору (в одному примірнику);

– паспорт заявника (або інший документ, що посвідчує особу відповідно до законодавства) та його копія (1–6 сторінки за наявності в них інформації, та сторінка з адресою реєстрації власника);

– при наявності у заявника паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в ЄДДР, заявником надаються копії обох його сторін та копія документу про реєстрацію місця проживання, засвідчені в установленому порядку;

– при реєстрації фізичних осіб-нерезидентів заявником надаються засвідчені штампами апостиляції копія посвідки на тимчасове чи постійне місце проживання, копія національного паспорта іноземця чи копія документа, що замінює національний паспорт;

– копія довідки про присвоєння ідентифікаційного номера (картки фізичної особи - платника податку), засвідчена підписом власника. У випадку, коли через релігійні переконання фізична особа відмовилась від реєстраційного номеру облікової картки платника податків, подається копія сторінки паспорту з відміткою про відмову;

– задокументовані відомості, що містяться в оприлюднених на веб-сайті Міністерства юстиції України документах, що стосуються державної реєстрації заявника.

Для відокремлених підрозділів (філії, представництва, тощо) юридичних осіб надається:

– копія довідки з управління статистики про внесення відомостей про відокремлений підрозділ до ЄДРПОУ, засвідчена нотаріально або особистим підписом директора (керівника) організації та печаткою організації у разі відсутності печатки - тільки особистим підписом;

– документи, що підтверджують належність підписувача до юридичної особи – заявника та його повноваження, засвідчені печаткою (за наявності) та особистим підписом керівника юридичної особи або відділом кадрів юридичної особи, або фізичної особи підприємця, у разі відсутності печатки - тільки особистим підписом;

– реєстр даних, в якому розміщені відомості стосовно контактної та іншої інформації - адреса місцезнаходження, телефон, електронна адреса, умови публікації сертифіката на інформаційному ресурсі Кваліфікованого надавача тощо.

У випадку, коли заявником надається оригінал документа або нотаріально завірена його копія, копія цього документа може бути засвідчена підписом посадової особи та печаткою Кваліфікованого надавача.

Отримання юридичними особами та фізичними особами - підприємцями сертифіката ключа для забезпечення застосування електронної печатки здійснюється в тому ж порядку, що й для КЕП.

Інформація стосовно призначення КЕП у якості електронної печатки заноситься заявником до реєстру даних, який він надає Кваліфікованому надавачу у складі реєстраційних документів.

До сертифіката ключа, що використовується установою у якості електронної печатки, заноситься також сфера його застосування та текстова інформація стосовно назви підприємства, поштової адреси та коду ЄДРПОУ.

У разі використання для встановлення юридичної особи та її уповноваженого представника інформації з інформаційного ресурсу ЄДР, Кваліфікований надавач забезпечує зберігання отриманих даних у вигляді роздрукованого документа на паперовому носії, в якому відображається інформація в обсязі, що є достатнім для заповнення реквізитів посиленого сертифіката відкритого ключа КЕП.

На сформованому паперовому документі, що містить інформацію з інформаційного

ресурсу ЄДР, проставляється дата встановлення юридичної особи і її представника, а також особистий підпис адміністратора реєстрації Кваліфікованого надавача, який безпосередньо здійснював встановлення особи.

8.11.3. Реєстрація заявника – фізичної особи

Для проведення процедури реєстрації фізичних осіб заявником до Кваліфікованого надавача надаються наступні документи та відомості:

– заповнений та підписаний договір – у двох примірниках або заповнену та підписану заявником заяву- приєднання до електронного договору (в одному примірнику);

– паспорт заявника (або інший документ, що посвідчує особу відповідно до законодавства України) та його копія (1– 6 сторінки за наявності в них інформації, та сторінка з адресою реєстрації власника);

– при наявності у заявника паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в ЄДДР, заявником надаються копії обох його сторін та копія витягу з ЄДДР, засвідчені в установленому порядку;

– при реєстрації фізичних осіб-нерезидентів заявником надаються засвідчені штампами апостиляції копія посвідки на тимчасове чи постійне місце проживання, копія національного паспорта іноземця чи копія документа, що замінює національний паспорт;

– копія довідки про присвоєння ідентифікаційного номера (картки фізичної особи – платника податку), засвідчена підписом власника. У випадку, коли через релігійні переконання фізична особа відмовилась від реєстраційного номеру облікової картки платника податків, подається копія сторінки паспорту з відміткою про відмову;

– реєстр даних, в якому розміщені відомості стосовно контактної та іншої інформації - адреса місцезнаходження, телефон, електронна адреса, умови публікації сертифіката на інформаційному ресурсі Кваліфікованого надавача тощо, зразок заповнення реєстру даних розміщено на сайті Кваліфікованого надавача.

8.11.4. Порядок надання та опрацювання документів

Встановлення (ідентифікація) юридичних та фізичних осіб, які проходять процедуру реєстрації, здійснюється шляхом вивчення наданих документів з метою визначення повноти, достовірності та актуальності інформації, що в них міститься.

Бланки документів встановленої форми, які використовуються під час реєстрації заявників, розміщені на електронному інформаційному ресурсі Кваліфікованого надавача.

Адміністратор реєстрації може прийняти рішення про відмову в реєстрації заявника у наступних випадках:

– при наданні на реєстрацію неповного комплекту документів;

– при поданні неякісних копій документів;

– при поданні копій документів, засвідчених неналежним чином;

– при встановленні невідповідності даних, що визначені у наданих документах, фактичним даним.

У разі відмови у реєстрації заявнику повертаються надані документи з поясненнями про причини відмови у реєстрації.

Особа, вважається встановленою, при одночасному виконанні наступних умов:

- відомості, зазначені у заяві на формування сертифіката відкритого ключа користувачів, збігаються із відповідними відомостями, наведеними в наданих документах;

- надані документи відповідають вигляду, встановленого чинним законодавством та не містять ознак навмисного внесення змін до їх змісту (підчистки, затирання окремих місць, незавірені виправлення тощо).

У разі прийняття позитивного рішення про реєстрацію адміністратор реєстрації приймає документи, виконує встановлену процедуру обліку отриманих документів, та виконує дії по занесенню реєстраційної інформації до списку підписувачів Кваліфікованого надавача.

Усі документи, що були надані заявником під час реєстрації, скануються, формуються у справу підписувача, яка в подальшому передається на зберігання до електронного архіву.

Реєстрація заявника є підставою для генерації ключів заявника, створення запиту на сертифікацію та формування сертифіката ключа підписувача.

У разі, якщо нормативно-правовими актами тимчасово встановлюються інші вимоги до певних видів документів, то на цей період будуть діяти відповідні норми прийнятих нормативно-правових актів без внесення додаткових змін до даного Регламенту.

8.12. Фізичне середовище

Приміщення Кваліфікованого надавача розділені на два типи - приймальні та службові приміщення. Двері між приймальними та службовими приміщеннями обладнані засобами розмежування доступу.

Приміщення Кваліфікованого надавача обладнані системою охоронної та пожежної сигналізації, а також системою відеоспостереження.

У приміщенні ВПР, що має доступ до ПТК ІТС, допускається відсутність службових приміщень, приймальне приміщення поділене столами персоналу ВПР та спеціальним бар'єром на зони для відвідувачів і для персоналу ВПР. Комплекс технічних засобів розміщений у зоні для персоналу ВПР так, щоб унеможливити доступ до технічних засобів ВПР з боку відвідувачів.

Право проходу й перебування у службових приміщеннях Кваліфікованого надавача надається на підставі:

- затвердженого керівником Кваліфікованого надавача списку посадових осіб;
- тимчасових списків осіб, відряджених до Кваліфікованого надавача;
- заявок на разове відвідування сторонньою особою службових приміщень Кваліфікованого надавача;
- заявок на разове відвідування сторонньою особою спеціального приміщення.

Пропускний режим передбачає порядок допуску персоналу та представників інших організацій на територію Кваліфікованого надавача, порядок внесення і винесення матеріальних цінностей, а також виконання особами, що перебувають на території Кваліфікованого надавача, встановлених вимог режиму і розпорядку робочого дня.

Загальне керівництво, контроль за організацією охорони, станом пропускного та внутрішнього режиму має здійснювати керівник Кваліфікованого надавача.

Особи, що порушують пропускний і внутрішній режим, притягуються до дисциплінарної відповідальності.

Допуск співробітників правоохоронних органів, пожежної інспекції, санепідемстанції, контрольно - ревізійних служб, на територію Кваліфікованого надавача, здійснюється в робочий час по пред'явленню службового посвідчення й припису на перевірку з попереднім повідомленням керівника Кваліфікованого надавача.

Допуск аварійних бригад, для оперативної ліквідації надзвичайної ситуації (пожежі, затоплення і т. ін.) на територію Кваліфікованого надавача, здійснюється негайно службою охорони з одночасним повідомленням керівництва Кваліфікованого надавача. До прибуття керівництва адміністратор безпеки та аудиту повинен контролювати дії аварійної бригади.

При прийомі на роботу до Кваліфікованого надавача співробітник має включатися до переліку персоналу Кваліфікованого надавача з дати, що зазначена в наказі про прийом його на роботу, з обов'язковим ознайомленням його під особистий підпис із вимогами пропускного й внутрішнього режиму. У випадку звільнення з роботи співробітник повинен бути виключений зі списку від дня, зазначеного в наказі про звільнення. Для остаточного

розрахунку колишнього співробітника, допуск на територію Кваліфікованого надавача здійснюється по разових дозволах із пред'явленням документів, що засвідчують особу.

До приміщень, у яких установлені технічні засоби та обладнання ПТК ІТС сторонні особи можуть допускатися лише за наявності дозволу керівника Кваліфікованого надавача у присутності адміністратора безпеки та аудиту.

8.13. Порядок ведення журналів аудиту подій

Кваліфікований надавач налаштований на реєстрацію таких подій:

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

Параметри реєстрації подій в ПТК ІТС (в електронній або паперовій формі):

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

Записи подій у журналах аудиту подій в паперовій формі підписуються адміністратором безпеки та аудиту.

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

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

Журнали аудиту подій, що ведуться в ПТК ІТС, зберігаються протягом 2 років, після чого забезпечується їх передача на архівне зберігання.

Резервні копії журналів аудиту подій, сертифікатів відкритих ключів, списків відкликаних сертифікатів на з'ємних носіях зберігаються в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

Резервне копіювання журналів аудиту здійснюється раз на добу (на резервний сервер Кваліфікованого надавача), резервне копіювання журналів аудиту на з'ємні носії здійснюється раз на тиждень.

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

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

Перегляд журналів аудиту, що ведуться в ПТК ІТС, дозволяється здійснювати лише керівнику Кваліфікованого надавача та адміністратору безпеки та аудиту.

8.14. Порядок ведення архівів

Архівному зберіганню підлягають наступні документи Кваліфікованого надавача:

– службові документи Кваліфікованого надавача, у тому числі журнали аудиту ПТК тощо на паперових носіях;

– дані про надані послуги фіксування часу, в тому числі позначки часу, передані користувачам послуги фіксування часу, на електронних носіях;

– сертифікати ключів Кваліфікованого надавача, на електронних носіях;

– сертифікати ключів серверів Кваліфікованого надавача, на електронних носіях;

– сертифікати ключів посадових осіб Кваліфікованого надавача, на електронних носіях;

– сертифікати ключів підписувачів, на електронних носіях;

– укладені договори про надання послуг електронного цифрового підпису, на електронних носіях;

– документи та копії документів, що використовуються під час реєстрації, на електронних носіях;

– заяви на скасування, блокування та поновлення сертифікатів ключів підписувачів на електронних/паперових носіях.

Документи, отримані від підписувачів/заявників у електронному вигляді, повинні зберігатись на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність.

Термін зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

При зберіганні електронних документів обов'язкове додержання таких вимог:

- інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

- має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений або одержаний;

- повинна зберігатися інформація, яка дає змогу встановити дату і час його створення або отримання.

Сертифікати ключів Кваліфікованого надавача, сертифікати ключів серверів Кваліфікованого надавача, сертифікати ключів посадових осіб Кваліфікованого надавача та сертифікати ключів підписувачів, а також списки відкликаних сертифікатів зберігаються в електронному вигляді постійно.

Для перевірки електронних документів, підписаних особистими ключами підписувачів, відповідні сертифікати ключів яких не є чинними, Кваліфікований надавач надає можливість доступу до списку відкликаних сертифікатів через електронний інформаційний ресурс Кваліфікованого надавача. Кваліфікований надавач додатково забезпечує можливість перевірки статусу сертифіката ключа на момент накладання КЕП.

Засоби СКБД, що входять до складу серверу Кваліфікованого надавача, виконують автоматичне резервне копіювання БД. Автоматичне створення резервної копії засобами СКБД виконується раз на добу, під час найменшого завантаження серверу.

Додатково виконується резервне копіювання БД та журналів аудиту ПТК в ручному режимі на оптичні носії, або інші з'ємні носії інформації. Резервне копіювання виконується засобами операційної системи. Після створення нової резервної копії, попередня резервна копія стає архівною.

З'ємні носії зберігаються в упаковці, на якій вказується обліковий номер копії та наноситься власноручний підпис адміністратора безпеки та аудиту. Факти створення та використання копій фіксуються в окремому журналі із зазначенням облікового номеру, дати та часу створення копії а також нанесенням прізвища, імені, по-батькові, посади та особистого підпису особи, що створила копію.

Архівні копії журналів аудиту ПТК ІТС зберігаються в приміщенні Кваліфікованого надавача не менше 2 (двох) років. Відповідальність за контроль автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора Кваліфікованого надавача. Адміністратор безпеки та аудиту періодично контролює процес створення та зберігання резервних копій.

9. ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

Формування сертифіката відкритого ключа здійснюється адміністратором сертифікації після завершення процедури реєстрації заявника.

9.1. Порядок формування сертифікатів відкритих ключів

Процедура формування сертифіката відкритого ключа виконується на підставі відомостей, що містяться в наданих підписувачем документах при проведенні процедури реєстрації.

Під час формування сертифіката відкритого ключа Кваліфікований надавач виконує наступні процедури:

– присвоює унікальний реєстраційний номер сертифіката;

– перевіряє унікальність відкритого ключа підписувача в реєстрі чинних, блокованих та скасованих сертифікатів.

Кваліфікований надавач повинен забезпечити в межах своєї відповідальності унікальність розпізнавального імені підписувача та реєстраційного номера сертифіката відкритого ключа.

Для фізичної особи обов'язковими реквізитами розпізнавального імені є прізвище, ім'я та по батькові.

Для юридичної особи обов'язковими реквізитами розпізнавального імені є повна назва юридичної особи відповідно до статуту (положення) та ідентифікаційний код за ЄДРПОУ.

Сформований сертифікат відкритого ключа вноситься до реєстру сертифікатів відкритих ключів Кваліфікованого надавача на інформаційному ресурсі Кваліфікованого надавача.

Після формування сертифікат відкритого ключа, за згодою підписувача, може бути опублікований на електронному інформаційному ресурсі Кваліфікованого надавача.

Після завершення процедури формування сертифіката відкритого ключа заявнику, за його бажанням, надаються:

– сертифікат відкритого ключа в електронному вигляді, записаний на електронний носій інформації;

– інсталяційний пакет клієнтського програмного забезпечення, записаний на електронний носій інформації;

– сертифікат відкритого ключа в друкованому вигляді на паперовому носії, засвідчений печаткою Кваліфікованого надавача та власноручним підписом адміністратора реєстрації (на вимогу підписувача).

Після отримання сертифіката відкритого ключа підписувач повинен перевірити достовірність відомостей, що в ньому містяться. При виявленні недостовірних даних, підписувач повинен у встановленому порядку звернутись до Кваліфікованого надавача з вимогою скасування та формування нового сертифіката.

У разі позитивних результатів перевірки сформованого сертифіката відкритого ключа заявник визнає свій сертифікат відкритого ключа шляхом підписання акта виконаних робіт.

Формат сертифіката відкритого ключа повинен відповідати вимогам до форматів, структури та протоколів, що реалізуються в засобах кваліфікованого електронного підпису, затвердженим наказом Міністерства юстиції України та Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453, зареєстрованим в Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710.

9.2. Повторне формування сертифіката ключа

Повторне формування сертифіката ключа здійснюється за зверненням підписувача у разі:

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

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

- компрометації або підозри в компрометації особистого ключа, з генерацією нових відкритого та особистого ключів;

- прийняття підписувачем такого рішення, необхідність генерації нових відкритого та особистого ключів встановлює підписувач.

При повторному формуванні сертифіката відкритого ключа старий сертифікат скасовується.

Обслуговування підписувачів при повторному формуванні сертифікатів може здійснюватись за процедурами, ідентичними процедурам при первинному формуванні сертифіката, або в автоматизованому режимі (з використанням «Онлайн-сервісу»).

9.3. Порядок обслуговування заявників з використанням «Онлайн-сервісу»

9.3.1. Обслуговування підписувачів при повторному формуванні сертифікатів

Підписувачі, які установленим порядком пройшли реєстрацію та володіють чинними, незаблокованими та не анульованими сертифікатами, можуть в автоматизованому режимі вносити зміни до даних, зазначених у сертифікатах, та/або здійснювати повторне формування сертифікатів, пов'язане з закінченням терміну дії чинних сертифікатів, шляхом надсилання на електронну адресу Кваліфікованого надавача електронних документів та електронних копій документів, виготовлених скануванням оригіналів документів на паперових носіях.

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

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

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

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

Форми та зміст зазначених документів розміщено на офіційному сайті Кваліфікованого надавача.

У випадку повторного формування сертифіката відкритого ключа при зміні відомостей, зазначених у сертифікаті ключа, окрім названих документів Кваліфікованому надавачу надсилаються також електронні копії документів, що підтверджують достовірність змін, які вносяться.

На всі електронні документи, що надсилаються підписувачем Кваліфікованому надавачу, має бути накладено КЕП користувача з використанням особистого ключа, що відповідає чинному сертифікату, термін дії якого закінчується, та/або до якого вносяться зміни.

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

Шляхом накладання КЕП на електронні документи та електронні копії документів, що надаються Кваліфікованому надавачу, підписувач засвідчує достовірність та актуальність на момент відправки зазначених документів усіх реєстраційних даних, що в них містяться, та реєстраційних даних, що надавались Кваліфікованому надавачу підписувачем під час первинного формування сертифіката. Автентифікація підписувача виконується шляхом перевірки КЕП підписувача на документах.

У разі, коли підписувачем виступає посадова особа юридичної особи, а оригінали документів на паперових носіях, електронні копії яких надсилаються Кваліфікованому

надавачу, підписуються керівником цієї юридичної особи, на електронні копії таких документів наклається КЕП зазначеного керівника.

Запит на формування нового сертифіката містить згенерований та засвідчений КЕП підписувача новий відкритий ключ. Підтвердження володіння підписувачем відповідним новим особистим ключем виконується установленим порядком.

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

9.3.2. Обслуговування заявників у разі відсутності доступу ВПР до ПТК ІТС

Для отримання права на реєстрацію заявників в ВПР, що не має доступу до ПТК ІТС, фізичні особи, фізичні особи - підприємці або юридичні особи повинні укласти з Кваліфікованим надавачем договір цивільно-правового характеру, корпоративний, дилерський або інший договір, у якому визначаються функції, обов'язки та перелік осіб, уповноважених на виконання процедур реєстрації заявників згідно з положеннями статті 7.4 цього Регламенту.

Після укладення договору уповноважені особи згідно з вимогами та в порядку, викладеним у п. 8.7 розділу 8 Регламенту, звертаються до Кваліфікованого надавача з запитом стосовно формування для них сертифікатів відкритих ключів.

Кваліфікований надавач у разі прийняття позитивного рішення щодо надання уповноваженим особам сертифікатів відкритих ключів виконує процедури їх авторизації та установлення прав і повноважень стосовно використання програмного забезпечення «Онлайн-сервіс», а також надає засоби КЕП для генерації та завантаження на носій відкритого та приватного ключів КЕП заявника.

Порядок використання та опис програмного забезпечення «Онлайн-сервіс» розміщені на офіційному сайті Кваліфікованого надавача.

Для отримання електронної довірчої послуги заявник обирає необхідний пакет послуг, формує пакет відповідних документів та копій документів згідно з вимогами та у порядку, викладеним у п. 8.7 розділу 8 та, враховуючи рекомендації уповноваженої особи, обирає один з варіантів генерації та завантаження на носій відкритого та закритого ключів:

- на власному робочому місці, за умови надання йому уповноваженою особою необхідних для цього засобів КЕП;

- на робочому місці уповноваженої особи.

При цьому уповноважена особа повинна забезпечити заявнику можливість використання захищених електронних носіїв ключової інформації: токенів, SIM-карт та інших.

Після завантаження відкритого та приватного ключів КЕП в носій заявник долучає до пакету документів запит на формування сертифіката та надає зазначені документи на опрацювання уповноваженій особі.

Уповноважена особа на підставі вивчення та опрацювання наданих документів здійснює встановлення особи заявника та виконує інші, наведені в договорі та пов'язані з реєстрацією заявника процедури.

Після завершення реєстрації заявника уповноважена особа переводить надані ним документи та копії документів на паперових носіях в електронну форму шляхом фото фіксації та сканування.

До виготовлених електронних копій документів долучаються відомості про заявника в електронному вигляді, сформований таким чином пакет електронних копій документів

підписується КЕП уповноваженої особи та вноситься в «Онлайн-сервіс» для завершення адміністраторами Кваліфікованого надавача процедур обслуговування заявника та занесення електронних копій наданих ним документів до електронного архіву.

Уповноважена особа повертає заявнику документи та копії документів на паперових носіях, або знищує надані ним скановані копії документів.

9.4. Управління статусом сертифікатів

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

Скасування, блокування та поновлення чинності сертифіката відкритого ключа виконує уповноважена особа Кваліфікованого надавача.

Блокування сертифіката відкритого ключа також може виконувати його власник за умови придбання у Кваліфікованого надавача засобу КЕП або отримання установленим порядком прав на використання програмного забезпечення «Онлайн-сервіс».

9.4.1. Скасування сертифікатів

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

Особистий ключ, сертифікат якого скасований, не може бути використаний підписувачем для накладання КЕП.

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

9.4.2. Підстави для скасування сертифіката

Підставами для скасування сертифіката є:

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

9.4.3. Порядок скасування сертифікатів

Скасування сертифіката можуть ініціювати:

- підписувач;

- заявник;
- посадова особа Кваліфікованого надавача, яка має відповідні повноваження.

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

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

Заява щодо скасування повинна містити наступні відомості:
- ідентифікаційні дані підписувача;
- серійний номер сертифіката, що скасовується;
- причина скасування сертифіката;
- дата та підпис підписувача, відбиток печатки підписувача (за наявності), КЕП підписувача – для заяви в електронній формі.

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

Електронна заява, що подається до Кваліфікованого надавача, повинна засвідчуватись КЕП підписувача. Заяви приймаються на електронну адресу, вказану на сайті Кваліфікованого надавача.

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

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

Розгляд та опрацювання заяви на скасування сертифіката та інформування заявника/підписувача про скасування здійснюється протягом двох годин з моменту надходження заяви до Кваліфікованого надавача.

Часом скасування сертифіката встановлюється час зміни статусу сертифіката у реєстрі сертифікатів Кваліфікованого надавача.

9.4.4. Блокування сертифікатів

Блокування сертифіката - це тимчасове припинення його чинності.

Особистий ключ, сертифікат якого заблокований, не може бути використаний підписувачем для накладання КЕП.

Кваліфікований надавач має право блокувати сертифікат з подальшим його скасуванням у випадку несплати послуг Кваліфікованому надавачу відповідно до договору надання послуг.

9.4.5. Підстави для блокування сертифікатів

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

9.4.6. Порядок блокування сертифікатів

Блокування сертифіката можуть ініціювати:
- підписувач;
- заявник;
- посадова особа Кваліфікованого надавача , яка має відповідні повноваження.

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

Прийняття і опрацювання заяв на блокування сертифікатів ключів здійснюється цілодобово.

Розгляд та опрацювання заяви на блокування сертифіката, інформування заявника/підписувача про блокування здійснюється протягом двох годин з моменту надходження заяви до Кваліфікованого надавача.

Часом блокування сертифіката встановлюється час зміни статусу сертифіката у реєстрі сертифікатів Кваліфікованого надавача.

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

При поданні заяви на блокування сертифіката підписувач повинен повідомити Кваліфікованого надавача наступну інформацію:

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

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

Електронна заява на блокування сертифіката повинна підписуватись власником сертифіката з використанням надійних засобів КЕП і подаватись до Кваліфікованого надавача засобами телекомунікаційного зв'язку на електронну адресу, вказану на сайті Кваліфікованого надавача.

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

Зразок оформлення заяви на блокування сертифіката розміщується на сайті Кваліфікованого надавача.

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

9.4.7. Поновлення сертифікатів

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

9.4.8. Підстави для поновлення сертифікатів

Кваліфікований надавач поновлює заблокований сертифікат в наступних випадках;

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

9.4.9. Порядок поновлення сертифікатів

Поновлення заблокованого сертифіката можуть ініціювати:

- підписувач;
- заявник;
- посадова особа Кваліфікованого надавача , яка має відповідні повноваження.

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

При поданні заяви на поновлнння сертифіката підписувач повинен повідомити Кваліфікованого надавача наступну інформацію:

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

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

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

Зразок заповнення заяви розміщується на сайті Кваліфікованого надавача.

Прийняття та опрацювання заяв на поновлення сертифіката ключа здійснюються посадовими особами Кваліфікованого надавача цілодобово.

Опрацювання письмової заяви на поновлення чинності сертифіката та інформування заявника/підписувача про поновлення здійснюється протягом двох годин з моменту надходження заяви до Кваліфікованого надавача.

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

9.4.10. Ідентифікація підписувача при блокуванні, скасуванні або поновленні чинності сертифіката.

При блокуванні, скасуванні та поновленні сертифіката ключа використовуються наступні ідентифікатори підписувача:

–у разі письмового звернення підписувача – власноручний підпис підписувача та відбиток печатки (за наявності);

–у разі надання запиту в вигляді електронного документа – КЕП підписувача;

–у разі звернення в телефонному режимі – умовна фраза що встановлюється підписувачем під час реєстрації.

9.5. Розповсюдження інформації про статус сертифікатів ключів

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

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

Кваліфікований надавач надає усім користувачам послугу інтерактивного визначення статусу сертифіката. Послуга надається шляхом відправлення запиту за протоколом HTTP на OCSP-сервер Кваліфікованого надавача відповідно до вимог спільного Наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 за №1236/5/453, зареєстрованим в Міністерстві юстиції України 20.08.2012 за №1398/21710.

Послуга інтерактивного визначення статусу сертифіката надається цілодобово.

9.6. Закінчення строку чинності сертифіката ключа

Термін чинності сертифіката ключа встановлюється рівним терміну чинності відповідних йому особистому та відкритому ключам.

Кваліфікований надавач зберігає сертифікат ключа та пов'язану з ним інформацію про його статус безстроково. За запитом користувачів Кваліфікований надавач надає доступ до необхідного сертифіката ключа та інформацію про його статус.

9.7. Надання інформації про статус сертифіката на визначений момент часу

Для отримання засвідчення чинності сертифіката ключа, особистим ключем якого був підписаний електронний документ, користувач подає до Кваліфікованого надавача заяву встановленої форми на засвідчення чинності сертифіката ключа на момент підписання електронного документу.

У разі, якщо користувач не може особисто прибути до офісу Кваліфікованого надавача, він може надати довіреній особі довіреність встановленої форми для здійснення процедури засвідчення чинності сертифіката ключа.

Прийняття та розгляд заяви на засвідчення чинності сертифіката ключа, виконується в офісі Кваліфікованого надавача тільки у робочий час.

Опрацювання заяви на засвідчення чинності сертифіката ключа та видача висновку щодо чинності сертифіката ключа на час підписання електронного документа здійснюється комісією, до складу якої входить не менше 3 (трьох) посадових осіб Кваліфікованого надавача, протягом 5 (п’яти) робочих днів з моменту отримання заяви Кваліфікованим надавачем.

В результаті проведення процедури встановлення чинності сертифіката ключа на час підписання електронного документа, комісія складає звіт-висновок, який засвідчується підписами всіх членів комісії та скріплюється печаткою Кваліфікованого надавача.

9.8. Захист персональних даних підписувачів

При опрацюванні документів, наданих на реєстрацію, та впродовж всього часу обслуговування сертифікатів ключів посадові особи Кваліфікованого надавача повинні впроваджувати заходи та дотримуватись вимог щодо захисту інформації, що містить відомості, які відносяться до персональних даних підписувачів, зокрема:

– впроваджувати заходи стосовно забезпечення працездатності КСЗІ автоматизованої системи Кваліфікованого надавача;

– вживати заходи щодо обліку та зберігання особових справ користувачів;

– використовувати засоби захисту інформації, що мають отримані установленим порядком документи, які підтверджують їх відповідність вимогам НД ТЗІ та КЗІ;

– вести журнали реєстрації подій;

– застосовувати антивірусні засоби;

– забезпечувати захист персональних даних підписувачів від несанкціонованого ознайомлення з ними сторонніх осіб при обміні електронними документами з використанням зовнішніх комп’ютерних мереж.

9.9. Управління ключами

9.9.1. Термін дії сертифікатів Кваліфікованого надавача

Термін дії сертифікатів Кваліфікованого надавача та сертифікатів серверів позначки часу не може перевищувати п’ять років.

Термін дії усіх інших сертифікатів, сформованих Кваліфікованим надавачем, не може перевищувати двох років.

Початком строку дії особистого ключа Кваліфікованого надавача або посадової особи Кваліфікованого надавача вважається дата та час початку строку дії відповідного сертифіката ключа Кваліфікованого надавача або посадової особи Кваліфікованого надавача.

Після закінчення строку чинності сертифіката ключа Кваліфікованого надавача або посадової особи Кваліфікованого надавача відповідний особистий ключ та всі його резервні копії знищуються методом, що не допускає можливості їх відновлення.

9.9.2. Порядок планової заміни ключів Кваліфікованого надавача та посадових осіб Кваліфікованого надавача

Планова зміна ключів Кваліфікованого надавача та сервера позначки часу (TSP) виконується не пізніше, ніж за два роки до закінчення терміну дії особистого ключа Кваліфікованого надавача. Планова зміна ключів серверів Кваліфікованого надавача (CMP, OCSP) та посадових осіб Кваліфікованого надавача виконується при закінченні термінів їх дії.

Формування нових ключів Кваліфікованого надавача та ключів серверів Кваліфікованого надавача (TSP, OCSP та CMP) здійснюється на території Кваліфікованого надавача.

Формування нових сертифікатів Кваліфікованого надавача та сервера позначки часу (TSP) здійснюється в ЦЗО.

Формування нових сертифікатів серверів Кваліфікованого надавача (CMP та OCSP) здійснюється на території Кваліфікованого надавача та підписується особистим ключем Кваліфікованого надавача.

Після здійснення генерації нової пари ключів (особистий та відкритий) та формування нового сертифіката відкритого ключа Кваліфікованого надавача старий особистий ключ Кваліфікованого надавача до завершення терміну дії останнього з підписаних ним сертифікатів продовжує використовуватись для підпису списків відкликаних сертифікатів, після чого особистий ключ Кваліфікованого надавача знищується надійним способом, що не дозволяє його відтворення.

Старий сертифікат Кваліфікованого надавача використовується для перевірки КЕП на раніше сформованих сертифікатах та списках відкликаних сертифікатів.

Старі сертифікати серверів Кваліфікованого надавача використовується для перевірки КЕП на раніше сформованих повідомленнях (позначках часу, інформації про статус сертифікатів тощо).

Особисті ключі Кваліфікованого надавача та серверів Кваліфікованого надавача зберігаються та використовуються в спеціальному захищеному сховищі, що входить до складу ПТК ІТС.

Відомості щодо створення та відновлення резервної копії попереднього особистого ключа Кваліфікованого надавача та його перенесення з одного до іншого засобу КЗІ реєструються адміністратором безпеки у відповідному журналі обліку.

Після введення в дію нових особистих ключів, усі особисті ключі, термін дії сертифікатів яких завершився, знищуються методом, що не допускає можливості їх відновлення, за участі не менше двох осіб, одним із яких обов’язково повинен бути адміністратор безпеки та аудиту.

Процедура планової заміни ключів Кваліфікованого надавача здійснюється в наступному порядку:

– адміністратор безпеки та аудиту разом з керівником Кваліфікованого надавача генерують новий особистий ключ і відповідний йому відкритий ключ;

– адміністратор сертифікації забезпечує процес засвідчення чинності відкритого ключа Кваліфікованого надавача у ЦЗО;

– новий сертифікат ключа Кваліфікованого надавача розміщується у загальнодоступних каталогах та на електронному інформаційному ресурсі Кваліфікованого надавача.

Процедура планової заміни ключів уповноважених посадових осіб Кваліфікованого надавача здійснюється в наступному порядку:

– уповноважена посадова особа Кваліфікованого надавача генерує новий особистий ключ та відповідний йому відкритій ключ;

– адміністратор безпеки та аудиту Кваліфікованого надавача формує новий сертифікат ключа посадової особи Кваліфікованого надавача;

– старий особистий ключ посадової особи Кваліфікованого надавача знищується, а старий сертифікат ключа скасовується.

Перевірка КЕП на документах, підписаних за допомогою старого особистого ключа посадової особи, здійснюється шляхом застосування відповідного йому скасованого

сертифіката ключа, який зберігається в реєстрі сертифікатів ключів Кваліфікованого надавача.

9.9.3. Порядок позапланової заміни ключів Кваліфікованого надавача та посадових осіб Кваліфікованого надавача

У випадку компрометації або загрози компрометації особистого ключа Кваліфікованого надавача або посадових осіб Кваліфікованого надавача виконується позапланова заміна ключів.

Кваліфікований надавач негайно інформує ЦЗО про факт компрометації особистого ключа Кваліфікованого надавача з метою його скасування шляхом внесення до списку відкликаних сертифікатів.

Процедура позапланової зміни ключів Кваліфікованого надавача виконується в порядку, визначеному процедурою планової зміни ключів.

Сертифікати ключів всіх підписувачів Кваліфікованого надавача скасовуються шляхом занесення в список відкликаних сертифікатів. Усі сертифікати ключів, що діяли на момент компрометації ключа Кваліфікованого надавача, а також сертифікати ключів, які були заблоковані, повинні бути позапланово сформовані повторно.

Список відкликаних сертифікатів підписується новим особистим ключем Кваліфікованого надавача.

Кваліфікований надавач офіційно оповіщає підписувачів про факт позапланової заміни ключів Кваліфікованого надавача. Після одержання офіційного повідомлення про факт позапланової заміни ключів Кваліфікованого надавача підписувачам необхідно виконати процедуру одержання нових сертифікатів ключів.

У випадку компрометації особистого ключа уповноваженої посадової особи Кваліфікованого надавача сертифікат ключа уповноваженої посадової особи Кваліфікованого надавача скасовується.

Після скасування сертифіката ключа посадової особи Кваліфікованого надавача виконується процедура позапланової заміни її відкритого та приватного ключів. Процедура позапланової заміни ключів уповноваженої посадової особи Кваліфікованого надавача виконується в порядку, визначеному у процедурі планової заміни ключів уповноваженої посадової особи Кваліфікованого надавача.

9.9.4. Порядок позапланової заміни особистого ключа підписувача

Позапланова заміна особистого ключа підписувача здійснюється в випадку компрометації або підозри компрометації його діючого особистого ключа.

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