Додаток 2

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

ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

Кваліфікованого надавача електронних довірчих послуг «MASTERKEY» щодо кваліфікованих сертифікатів електронного підпису та печатки

ЗМІСТ

1. ВСТУП

1.1. Огляд

Ці Положення сертифікаційних практик визначають перелік практичних дій та процедур щодо кваліфікованих сертифікатів електронного підпису та печатки (далі - кваліфіковані сертифікати) користувачів електронних довірчих послуг, зокрема, підписувачів та створювачів електронних печаток (далі - користувачі), які застосовуються Надавачем для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту).

Дотримання практичних дій та процедур, визначених у цих Положеннях сертифікаційних практик, є обов'язковим для керівника Надавача та найманих працівників Надавача, посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванню їхніх кваліфікованих сертифікатів (далі - персонал), а також фізичних та юридичних осіб, які на підставі договорів укладених з ТОВ «АРТ-МАСТЕР» пов'язані з реєстрацією користувачів, зокрема, відокремлених пунктів реєстрації Надавача.

Визнання користувачами вимог, визначених у цих Положеннях сертифікаційних практик, є обов'язковою умовою та підставою для укладення з ними договору про надання електронних довірчих послуг.

Перелік усіх правил, що застосовуються Надавачем у процесі реєстрації користувачів, формування та обслуговування кваліфікованих сертифікатів відкритих ключів КНЕДП «MASTERKEY» та користувачів, зокрема управління їх статусом (блокування, поновлення та скасування) визначається Політиками сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до Регламенту Надавача).

Ці Положення сертифікаційних практик відповідають вимогам, визначеним у стандарті:

- ДСТУ ETSI EN 319 411-1 (ETSI EN 319 411-1) «електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги» (далі - ДСТУ ETSI EN 319 411-1).

1.2. Назва документа та його ідентифікація

Назва документа та його ідентифікація визначається відповідно до положень пункту 5.3 ДСТУ ETSI EN 319 411-1

Повна назва документа: Положення сертифікаційних практик Кваліфікованого Надавача електронних довірчих послуг «MASTERKEY» щодо кваліфікованих сертифікатів електронного підпису та печатки.

Скорочена назва документа: Положення сертифікаційних практик КНЕДП «MASTERKEY»

1.3. Учасники інфраструктури відкритих ключів

Учасники інфраструктури відкритих ключів зазначені в пункті 5.4 ДСТУ ETSI EN 319 411-1

1.3.1. Надавач

КНЕДП «MASTERKEY» є кваліфікованим надавачем електронних довірчих послуг, що надає кваліфіковані електронні довірчі послуги з дотриманням вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги», зокрема, здійснює реєстрацію користувачів самостійно або через відокремлені пункти реєстрації Надавача, формує та обслуговує їхні кваліфіковані сертифікати в тому числі здійснює управління їхнім статусом (блокування, поновлення та скасування).

1.3.2. Органи реєстрації

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

1.3.3. Користувачі

Користувачами Надавача є підписувачі та створювачі електронних печаток, з якими Надавач укладає договори на надання електронних довірчих послуг та здійснює їх реєстрацію самостійно або через відокремлені пункти реєстрації, з подальшим формуванням та обслуговуванням їхніх кваліфікованих сертифікатів.

Типи підписувачів:

- фізичні особи - резиденти;
- фізичні особи - нерезиденти;
- самозайняті особи (нотаріуси, адвокати, арбітражні керуючі, приватні виконавці, тощо);
- посадові особи юридичної особи, фізичної особи - підприємця, самозайнятої особи, представництва юридичної особи - нерезидента.

Типи створювачів електронних печаток:

- юридичні особи – резиденти;
- представництва юридичних осіб - нерезидентів;
- фізичні особи - підприємці.

1.3.4. Суб'єкти, які довіряють Надавачу

Фізичні та юридичні особи, а також їхні інформаційно-комунікаційні системи є суб'єктами, які довіряють Надавачу, та використовують

кваліфіковані сертифікати користувачів з метою їх автентифікації, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

1.3.5. Інші учасники

Фізичні та юридичні особи, які прямо чи опосередковано пов'язані з формуванням та/або обслуговування кваліфікованих сертифікатів Надавача та користувачів, є іншими учасниками.

Політика сертифіката кваліфікованого надавача електронних довірчих послуг КНЕДП «MASTERKEY» (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.4. Використання сертифіката

Використання сертифіката відповідає положенням пункту 5.5 ДСТУ ETSI EN 319 411-1 з застосуванням наступних вимог:

1.4.1. Дозволене використання сертифіката

Кваліфіковані сертифікати відкритих ключів, сформованих Надавачем дозволено використовувати для:

- автентифікації;
- створення, перевірки та підтвердження кваліфікованого електронного підпису;
- створення, перевірки та підтвердження кваліфікованої електронної печатки;
- узгодження ключів шифрування.

Усі кваліфіковані сертифікати, сформовані Надавачем, у розширенні «qualified certificate statement» містять значення:

- 1.2.804.2.1.1.1.2.1 (для забезпечення електронного документообігу та автентифікації осіб в межах країни);
- 1.2.804.2.1.1.1.2.2 (для програмних ключів);
- 1.2.804.2.1.1.1.2.4 (для особистих ключів, що зберігаються в засобі кваліфікованого електронного підпису чи печатки).

Крім того, для визначення сфери використання кваліфікованого сертифіката користувача, під час його формування встановлює додаткове розширення «Уточнене призначення відкритого ключа» із об’єктним ідентифікатором:

- 1.2.804.2.1.1.1.11.30404750.46 (керівник підприємства, ФОП або самозайнята особа);
- 1.2.804.2.1.1.1.11.30404750.47 (головний бухгалтер);
- 1.2.804.2.1.1.1.3.9 (електронна печатка).

Вищезазначений перелік не є вичерпним.

У випадках коли особистий ключ було згенеровано із застосуванням засобу кваліфікованого електронного підпису, під час формування кваліфікованого сертифікату встановлюється відповідне значення об’єктного ідентифікатора.

1.4.1.1. Види кваліфікованих сертифікатів

Надавач формує кваліфіковані сертифікати наступних видів:

- кваліфікований сертифікат електронного підпису, що пов'язує відкритий ключ кваліфікованого електронного підпису з фізичною особою та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованого електронного підпису;
- кваліфікований сертифікат електронної печатки, що пов'язує відкритий ключ кваліфікованої електронної печатки з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованої електронної печатки;
- кваліфікований сертифікат шифрування, що пов'язує відкритий ключ кваліфікованого електронного підпису чи печатки з фізичною особою, юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією.

1.4.1.2. Строк дії кваліфікованих сертифікатів

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

1.4.2. Заборонене використання сертифіката

Кваліфікований сертифікат може використовуватися лише відповідно до зазначеного у ньому призначенні відкритого ключа.

1.5. Управління Положеннями сертифікаційних практик

1.5.1. Відповідальність за Положення сертифікаційних практик

Ці Положення сертифікаційних практик підтримується Товариством з обмеженою відповідальністю «Арт-мастер» (далі – ТОВ «Арт-мастер»).

ТОВ «Арт-мастер» є зареєстрованою відповідно до законодавства юридичною особою.

Головний офіс КНЕДП «MASTERKEY» представлений функціональним підрозділом ТОВ «Арт-мастер», що здійснює організацію надання кваліфікованих електронних довірчих послуг КНЕДП «MASTERKEY» і

відокремленими пунктами реєстрації «MASTERKEY» та забезпечує виконання вимог законодавства до кваліфікованих надавачів електронних довірчих послуг. Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «Арт-мастер».

Реквізити ТОВ «Арт-мастер»:
- Код ЄДРПОУ: 30404750
- Юридична адреса: 03035, місто Київ, вул. Монастирського Дениса, 3
- Телефон: +38 (044) 206-13-78
- Електронна пошта: help@am-soft.ua

Реквізити КНЕДП «MASTERKEY»:
- Веб-сайт: https://ca.masterkey.ua
- Електронна пошта: info@masterkey.ua

Ці Положення сертифікаційних практик, а також зміни до них затверджується директором ТОВ «Арт-мастер».

Ці Положення сертифікаційних практик, а також зміни до них погоджуються Міністерством цифрової трансформації України, яке направляє їхні копії до Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

1.5.2. Внесення змін до Політики сертифіката

Внесення змін до цих Положень сертифікаційних практик здійснюється у разі:
- змін вимог, процесів та процедур описаних в цих Положеннях сертифікаційних практик;
- змін у вимогах до надавачів щодо надання послуг;
- змін в законодавстві.

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

У цих Положеннях сертифікаційних практик використано терміни, встановлені в Законі України «Про електронну ідентифікацію та електронні довірчі послуги» та документах, зазначених у п. 3 Регламенту Надавача.

1.6.2. Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ІКС	Інформаційно-комунікаційна система
РНОКПП	Реєстраційний номер облікової картки платника податків
УНЗР	Унікальний номер запису в ЄДДР

CMP	Certificate Management Protocol (Протокол управління сертифікатами)
OCSP	Online Certificate Status Protocol (протокол визначення статусу сертифіката ключа)
OLS	Online Service (Онлайн сервіс)
TSP	Time Stamp Protocol (протокол позначки часу)

2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.1 ДСТУ ETSI EN 319 411-1

2.1. Репозиторій/Веб-сайт

Надавач забезпечує вільний доступ до наступної інформації через свій офіційний веб-сайт:

- відомості про Надавача, в тому числі про ВПР Надавача, в обсязі, достатньому для їх однозначного встановлення користувачем (реквізити, адреси, контактні телефони, режими роботи тощо);
- інформація про внесення Надавача до Довірчого списку;
- перелік кваліфікованих електронних довірчих послуг, які надає Надавач;
- кваліфіковані сертифікати відкритих ключів Надавача;
- кваліфіковані сертифікати відкритих ключів користувачів (за згодою користувачів);
- списки відкликаних сертифікатів відкритих ключів;
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів користувачами;
- перелік, форми документів, на підставі яких надаються електронні довірчі послуги, та роз’яснення щодо їх оформлення;
- дані про засоби кваліфікованого електронного підпису та печатки, що використовуються під час надання електронних довірчих послуг;
- дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;
- Регламент Надавача з Політикою сертифіката та Положенням сертифікаційних практик;
- перелік нормативно-правових актів у сфері електронних довірчих послуг.

Ці Положення сертифікаційних практик доступні 24 години на добу 7 днів на тиждень на офіційному веб-сайті Надавача.

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

Адміністратор сертифікації Надавача забезпечує публікацію кваліфікованих сертифікатів користувачів, згода на публікацію яких надана такими користувачами, та списків відкликаних сертифікатів на офіційному веб-сайті Надавача.

Згода на публікацію кваліфікованого сертифіката надається користувачем під час подання заяви на формування кваліфікованого сертифіката.

2.2.2. Публікація сертифікатів Надавача

Надавач забезпечує публікацію кваліфікованих сертифікатів Надавача на власному веб-сайті.

2.2.3. Доступ до сертифікатів користувачів

Надавач забезпечує цілодобовий доступ користувачів до їхніх власних кваліфікованих сертифікатів.

Доступ інших осіб до кваліфікованих сертифікатів користувачів надається за умови надання такими користувачами згоди на публікацію їх кваліфікованих сертифікатів.

2.2.4. Строк закінчення дії сертифіката

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

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

2.3. Час та періодичність публікації

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

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

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

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

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів користувачів.

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

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

2.4. Контроль доступу до репозиторію/веб-сайту

Кваліфіковані сертифікати Надавача та користувачів, списки відкликаних сертифікатів, відповідні Положення сертифікаційних практик та Політика сертифіката доступні у репозиторію/веб-сайті Надавача цілодобово.

Доступ лише для читання необмежений. Всі зміни у репозиторії/веб-сайті здійснюються виключно Надавачем.

Користувач може знайти інформацію про свій кваліфікований сертифікат шляхом здійснення його пошуку на офіційному веб-сайті Надавача у розділах «Сертифікати підписувачів» або «Пошук сертифікатів» заповнивши у відповідних вкладках інформацію про РНОКПП (у разі відсутності серія (за наявності) та номер паспорта).

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2 ДСТУ ETSI EN 319 411-1

3.1. Позначення

Кваліфіковані сертифікати сформовані Надавачем обов'язково повинні містити відомості, визначені частиною другою статті 23 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», а саме:

1) позначку (у формі, придатній для автоматизованої обробки) про те, що сертифікат виданий як кваліфікований сертифікат;

2) позначку, що сертифікат виданий в Україні;

3) ідентифікаційні дані, які однозначно визначають Надавача, у тому числі обов'язково найменування та код згідно з ЄДРПОУ;

4) ідентифікаційні дані, які однозначно визначають користувача , у тому числі обов'язково:

- прізвище, власне ім'я, по батькові (за наявності) підписувача та УНЗР або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття РНОКПП та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі

за серією та/або номером паспорта), або номер паспортного документа іноземця чи особи без громадянства;

- найменування або прізвище, власне ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з ЄДРПОУ (код/номер з торговельного, банківського чи судового реєстру, що ведеться країною резидентства іноземної юридичної особи, код/номер з реєстраційного посвідчення місцевого органу влади іноземної держави про реєстрацію юридичної особи), крім міжнародних організацій, відомості про яких не внесені до ЄДР або торговельного, банківського чи судового реєстру, що ведеться іноземною державою, за місцезнаходженням штаб-квартири міжнародної організації, або унікальний номер запису в ЄДДР, або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття РНОКПП та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта);

5) значення відкритого ключа, який відповідає особистому ключу;

6) відомості про початок та закінчення строку дії кваліфікованого сертифіката;

7) серійний номер кваліфікованого сертифіката, унікальний для Надавача;

8) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені Надавачем;

9) відомості про місце розміщення в безоплатному доступі кваліфікованого сертифіката, з використанням якого перевіряється удосконалений електронний підпис чи печатка, передбачені підпунктом 8 цього пункту;

10) відомості про місце надання послуги перевірки статусу відповідного кваліфікованого сертифіката;

11) зазначення про те, що особистий ключ, пов'язаний з відкритим ключем, зберігається в засобі кваліфікованого електронного підпису чи печатки, - у формі, придатній для автоматизованої обробки.

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

Кваліфіковані сертифікати можуть містити інші необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів. Такі атрибути не повинні впливати на інтероперабельність і визнання кваліфікованих електронних підписів чи печаток.

Відомостям, що містяться в кваліфікованих сертифікатах, відповідають позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 Політики сертифіката КНЕДП «MASTERKEY» (додаток 1 до цього Регламенту).

3.1.1. Типи позначень сертифіката

Типи позначень (реквізитів, атрибутів) кваліфікованого сертифіката, що відповідають відомостям, які містяться в кваліфікованих сертифікатах, визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 Політики сертифіката КНЕДП «MASTERKEY» (додаток 1 до цього Регламенту).

3.1.2. Позначення (реквізити та атрибути) сертифікатів

Кваліфікований сертифікат повинен мати всі необхідні позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 Політики сертифіката КНЕДП «MASTERKEY» (додаток 1 до цього Регламенту).

3.1.3. Використання псевдонімів

Використання псевдонімів здійснюється відповідно до пункту 3.1.3 Політики сертифіката КНЕДП «MASTERKEY» (додаток 1 до цього Регламенту).

3.1.4. Правила інтерпретації різних форм позначень сертифіката

Міжнародні літери повинні кодуватися згідно з UTF-8.

3.1.5. Унікальність позначень сертифіката

Надавач повинен гарантувати, що сертифікати з однаковими даними, зазначеними в полях «Повне ім’я/найменування користувача» («Common Name») та «Серійний номер» («SerialNumber»), не видаються різним користувачам.

3.1.6. Визнання, автентифікація та роль торгових марок

Не застосовується.

3.2. Первинна перевірка ідентифікації

3.2.1. Метод підтвердження володіння особистим ключем

Пункт 3.2.1 Політики сертифіката КНЕДП «MASTERKEY» містить інформацію щодо методів підтвердження володіння користувачем особистим ключем.

3.2.2. Автентифікація особи

Для ідентифікації користувача, що звернувся до Надавача для отримання кваліфікованих електронних довірчих послуг, Надавач вимагає разом із заявою надати, а користувач надає ідентифікаційні дані, які вносяться до кваліфікованого сертифіката.

Перелік ідентифікаційних даних, які вносяться до кваліфікованого сертифіката, та механізми їх підтвердження визначається у Таблицях 1 та 2.

Таблиця 1

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

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

Таблиця 2

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

Ідентифікаційні дані	Обов'язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
Найменування юридичної особи	Обов'язково	Документальне або технічне (отримання інформації в електронній формі з ЄДР)
Код ЄДРПОУ	Обов'язково	Документальне або технічне (отримання інформації в електронній формі з ЄДР)
Юридична адреса	Обов'язково	Документальне або технічне (отримання інформації в електронній формі з ЄДР)

Повноваження або займана посада	Обов’язково	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: рішення засновників, протокол, наказ про призначення, договір, посвідчення тощо)

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

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

Для підтвердження належного проведення процедури встановлення користувача, Надавач забезпечує зберігання заяв на формування або зміну статусу кваліфікованих сертифікатів та копій документів, які надавались користувачами під час їх ідентифікації. Копії таких документів зберігаються в електронному вигляді в захищеному середовищі онлайн сервісу «OLS» Надавача.

Заяви та копії документів, які використовувались в процедурі встановлення користувача засвідчуються за правилами, наведеними у Таблиці 3.

Таблиця 3

Правила засвідчення документів,
які використовуються в процедурі встановлення користувача

Форма документу	**Засвідчення з боку користувача** засвідчується у першу чергу	**Засвідчення з боку Надавача (адміністратора реєстрації, уповноваженої особи ВПР)** засвідчується у другу чергу
	Тип підпису	**Тип підпису**
Паперова первинна, електронна архівна	Власноручний підпис на паперовому документі	КЕП адміністратора реєстрації (уповноваженої особи ВПР) на електронній копії паперового документу
Електронна	КЕП користувача	Відсутній

Надавач може здійснювати перевірку чинності документів наданих фізичною особою за даними щодо недійсних документів на інформаційному ресурсі Державної міграційної служби України.

Для здійснення перевірки цивільної правоздатності та дієздатності юридичної особи здійснюється перевірка інформації про юридичну особу, що міститься в ЄДР. Надавач також може здійснювати перевірку в реєстрі платників податків на інформаційному ресурсі Державної податкової служби України.

Під час встановлення особи Надавач може використовувати засоби фото або відео фіксації для підтвердження факту пред’явлення користувачем документів, що посвідчують особу. Збереження фото або відео фіксації в ІКС

надавача здійснюється з урахуванням положень законодавства України в сфері захисту інформації та захисту персональних даних.

3.2.3. Неперевірена інформація про користувача

Неперевірена інформація про користувача не допускається.

Ідентифікація особи здійснюється Надавачем (відокремленим пунктом реєстрації Надавача) шляхом перевірки та підтвердження належності фізичній чи юридичній особі, яка звернулася за отриманням послуги формування кваліфікованого сертифіката, ідентифікаційних даних особи, отриманих Надавачем (відокремленим пунктом реєстрації Надавача).

3.2.4. Підтвердження повноважень

Під час ідентифікації уповноваженого представника юридичної особи або фізичної особи - підприємця Надавач здійснює автентифікацію такого користувача відповідно до пункту 3.2.2 цих Положень сертифікаційних практик, перевіряє обсяг повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця, чи з використанням інформації, що міститься в ЄДР.

3.3. Ідентифікація та автентифікація за заявою на зміну реквізитів в кваліфікованих сертифікатах відкритого ключа

У разі зміни відомостей, що містяться у кваліфікованому сертифікаті, користувач своєчасно повідомляє про це Надавача та надає документи, що підтверджують відповідні зміни разом із заявою на зміну реквізитів в кваліфікованому сертифікаті відкритого ключа

На підставі наданих користувачем документів, що підтверджують зміни відомостей, які містяться у кваліфікованому сертифікаті, Надавач здійснює повторне формування такого сертифіката (згідно тарифу Надавача) та його публікацію у разі згоди користувача.

Перевірка ідентифікаційних даних користувача, який звертається з заявою в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації користувача та його повноважень за результатами перевірки кваліфікованого електронного підпису на заяві та встановленням чинності на момент подання заяви кваліфікованого сертифіката, що містить ідентифікаційні дані особи.

Повторне формування кваліфікованого сертифіката користувача при зміні його реквізитів не продовжує строку його дії.

3.4. Ідентифікація та автентифікація користувача за заявами про скасування, блокування або поновлення сертифіката

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

Таблиця 4

Перелік
механізмів ідентифікації та автентифікації користувачів

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

Перевірка ідентифікаційних даних користувача, який звертається із заявою про блокування або скасування кваліфікованого сертифіката в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації та ідентифікації користувача на електронному сервісі «OLS» Надавача за допомогою чинного кваліфікованого сертифіката користувача, що містить ідентифікаційні дані особи на момент подання заяви.

3.5. Автентифікація при втраті засобу автентифікації

Автентифікація користувача при втраті засобу автентифікації здійснюється по телефону опублікованому на офіційному веб-сайті Надавача за участю відповідального співробітника Надавача шляхом надання відповіді на секретне запитання зазначене при реєстрації користувача.

4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3 ДСТУ ETSI EN 319 411-1

4.1. Запит на формування сертифіката

До переліку суб’єктів, уповноважених подавати запит на формування кваліфікованого сертифіката належать користувачі, що пройшли процедури ідентифікації та автентифікації.

Запит на формування кваліфікованого сертифіката приймається в обробку після приймання та реєстрації заяви на формування кваліфікованого сертифіката, ідентифікації та автентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

Перелік, форми документів, на підставі яких надаються електронні довірчі послуги, та роз’яснення щодо їх оформлення опубліковані на офіційному веб-сайті Надавача.

4.2. Обробка запиту на формування сертифіката

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

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

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

Строк обробки запиту на формування кваліфікованого сертифіката, поданого разом із заявою на реєстрацію, залежить від обраного користувачем пакета послуг і становить не більше 48 годин після внесення оплати за послугу.

4.3. Формування сертифіката

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

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

- запису файлу із сформованим кваліфікованим сертифікатом відкритого ключа на носій інформації, наданий користувачем;
- публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному веб-сайті Надавача.

4.4. Прийняття сертифіката

Публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному веб-сайті Надавача відбувається одразу після обробки запиту на сертифікат.

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

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

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката та виявлених користувачем після отримання сформованого кваліфікованого сертифіката, власник такого сертифіката особисто звертається до Надавача для скасування цього сертифіката та формування нового кваліфікованого сертифіката у встановленому порядку.

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

4.5. Пара ключів та призначення сертифіката

4.5.1. Використання особистого ключа та сертифіката користувачем

Під час використання особистого ключа та кваліфікованого сертифіката користувач повинен дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- Політики сертифіката КНЕДП «MASTERKEY»;
- цих Положення сертифікаційних практик;
- Загальних положень Регламенту Надавача;
- Договору про надання кваліфікованих електронних довірчих послуг, укладеного з ТОВ «Арт-мастер».

4.5.2. Використання відкритого ключа та сертифіката суб'єктами, які довіряють Надавачу

Під час використання відкритого ключа та кваліфікованого сертифіката користувача суб'єкти, які довіряють Надавачу, повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- цих Положення сертифікаційних практик;
- Політики сертифіката КНЕДП «MASTERKEY».

4.6. Поновлення сертифіката

Надавач поновлює заблокований сертифікат в наступних випадках:

- подання користувачем електронних довірчих послуг заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи користувача (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);
- 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.

Прийняття заяви на поновлення сертифіката ключа здійснюються згідно графіка роботи Надавача та його відокремлених пунктів реєстрації.

Опрацювання заяви на поновлення чинності сертифіката та інформування користувача про поновлення здійснюється протягом двох годин з моменту отримання заяви Надавачем.

Кваліфікований сертифікат, який був заблокованим, відновлює свою чинність з моменту його поновлення.

Кваліфікований сертифікат вважається поновленим з моменту зміни Надавачем статусу кваліфікованого сертифіката на «поновлений».

4.7. Повторне формування сертифіката

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

При наданні послуги щодо повторного формування сертифіката у разі, коли термін дії чинного сертифіката ще не закінчився, 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.

На всі електронні документи та копії документів, що надсилаються користувачем Надавачу, має бути накладено КЕП користувача з використанням особистого ключа, що відповідає чинному сертифікату. Шляхом накладання КЕП на електронні документи та електронні копії документів, що надаються Надавачу, користувач засвідчує достовірність та актуальність на момент відправки зазначених документів усіх реєстраційних даних, що в них містяться, та реєстраційних даних, що надавались Надавачу користувачем під час первинного формування сертифіката. Автентифікація користувача виконується шляхом перевірки КЕП користувача на документах.

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

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

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

Обслуговування користувачів при повторному формуванні сертифікатів може здійснюватися за процедурами, ідентичними процедурам при первинному формуванні сертифіката, або за наявності чинного кваліфікованого сертифікату, що містить ідентифікаційні дані користувача, в автоматизованому режимі (з використанням електронного сервісу «OLS» Надавача).

4.8. Зміна сертифіката

Зміна ідентифікаційних даних, що внесені до кваліфікованого сертифіката користувача, є підставою для скасування кваліфікованого сертифіката.

4.9. Скасування та блокування сертифіката

Надавач скасовує сформований ним кваліфікований сертифікат протягом двох годин у разі:

- подання користувачем заяви про скасування виданого йому кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача;

- подання заяви про скасування кваліфікованого сертифіката працівника юридичної особи чи фізичної особи - підприємця за підписом уповноваженої особи відповідної юридичної особи чи фізичної особи – підприємця.

Також, підставою для скасування кваліфікованого сертифіката є надходження до Надавача інформації, що підтверджує:

- смерть фізичної особи - користувача;
- державну реєстрацію припинення юридичної особи або припинення підприємницької діяльності фізичної особи - підприємця, що є користувачем;
- зміну ідентифікаційних даних користувача, які містяться у кваліфікованому сертифікаті;
- надання користувачем недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката;
- факт компрометації особистого ключа користувача, виявлений користувачем самостійно або контролюючим органом під час здійснення заходів державного контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг;
- набрання законної сили рішенням суду про скасування кваліфікованого сертифіката, оголошення фізичної особи або фізичної особи - підприємця, що є користувачем, померлою, визнання її безвісно відсутньою, недієздатною, обмеження її цивільної дієздатності, визнання користувача банкрутом.

Надавач блокує сформований ним кваліфікований сертифікат протягом двох годин у разі:

- подання користувачем заяви про блокування виданого йому кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача;
- подання заяви про блокування кваліфікованого сертифіката працівника юридичної особи чи фізичної особи - підприємця за підписом уповноваженої особи відповідної юридичної особи чи фізичної особи – підприємця.
- набрання законної сили рішенням суду про блокування кваліфікованого сертифіката;
- порушення користувачем істотних умов договору про надання кваліфікованих електронних довірчих послуг.

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

4.10. Послуга перевірки статусу сертифіката

Надавач забезпечує доступність інформації про статус сертифіката в реальному часі за допомогою OCSP-серверу та списків відкликаних сертифікатів (CRL), що публікуються на офіційному веб-сайті Надавача.

4.11. Закінчення строку дії сертифіката

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

Після настання дати та часу закінчення строку дії сертифіката користувача, зазначеного в ньому, такий сертифікат вважається скасованим.

Користувач може звернутися до Надавача із заявою про скасування виданого йому кваліфікованого сертифіката у разі необхідності дострокового припинення його обслуговування.

4.12. Депонування та повернення ключів

Не застосовується.

5. ОБ'ЄКТ, УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4 ДСТУ ETSI EN 319 411-1

5.1. Контроль фізичної безпеки

Пункт 5.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо вимог до приміщень Надавача та забезпечення фізичного доступу до них.

5.2. Процедурний контроль

Пункт 5.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо довірених ролей персоналу Надавача (керівник, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор, аудитор системи) та їх функціональних обов'язків, щодо кількості осіб, необхідних для виконання завдань, а також довірених ролей персоналу Надавача, що вимагають розподілу обов'язків.

5.3. Контроль персоналу

Пункт 5.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо вимог до кваліфікації, досвіду та допуску персоналу

Надавача, вимог та процедур навчання, санкцій за несанкціоновані дії, контролю відокремлених пунктів реєстрації Надавача, документації, яка надається персоналу Надавача.

5.4. Ведення журналу аудиту подій

Пункт 5.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо типів записаних подій, частоти обробки журналу аудиту подій, строків зберігання журналу аудиту подій, захисту журналу аудиту подій, процедур резервного копіювання журналу аудиту подій та питань синхронізації часу.

5.5. Архів документів

Пункт 5.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву та захисту архіву.

5.6. Зміна ключа

Пункт 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо підстав та періодичності зміни пари ключів Надавача, порядку використання та доступу до актуального відкритого ключа Надавача.

5.7. Компрометація і аварійне відновлення

Пункт 5.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо процедур обробки інцидентів і компрометації, процедур відновлення, якщо обчислювальні ресурси, програмне забезпечення та/або дані пошкоджені, процедур відновлення після компрометації особистого ключа, можливостей безперервності бізнесу після катастрофи.

5.8. Припинення діяльності надавача

Пункт 5.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо підстав припинення діяльності Надавача, порядку надання повідомлення про припинення діяльності, визначення дати припинення діяльності, питань правонаступництва та передачі документованої інформації, а також Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг.

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.5 ДСТУ ETSI EN 319 411-1

6.1. Генерація та встановлення пари ключів

Пункт 6.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо генерації пари ключів Надавача та користувачів, доставки особистого та відкритого ключів користувачам, доставки відкритого ключа Надавача суб’єктам, які довіряють Надавачу, щодо розмірів ключів та основних цілей використання особистих ключів.

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

Пункт 6.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо керування криптографічним модулем, резервного копіювання особистого ключа, архівації особистого ключа, відновлення особистого ключа, зберігання особистого ключа в криптографічному модулі, активації особистих ключів, деактивації особистих ключів, знищення особистих ключів, можливостей мережного криптографічного модуля.

6.3. Інші аспекти керування парами ключів

Пункт 6.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо архівації відкритого ключа Надавача, строків дії сертифіката та строків використання пари ключів Надавача.

6.4. Дані активації

Пункт 6.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо захисту даних активації особистого ключа.

6.5. Контроль комп'ютерної безпеки

Пункт 6.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо спеціальних технічних вимог до комп’ютерної безпеки, рейтингу комп’ютерної безпеки.

6.6. Контроль безпеки життєвого циклу

Пункт 6.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо контролю розробки ІКС Надавача, засобів керування безпекою в ІКС Надавача, контролю безпеки протягом життєвого циклу.

6.7. Контроль безпеки мережі

Пункт 6.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо елементів керування безпекою мережі.

6.8. Електронні позначки часу

Пункт 6.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо формування та перевірки кваліфікованої електронної позначки часу, наслідків недійсності кваліфікованої електронної позначки часу та процедури отримання Надавачем кваліфікованої електронної позначки часу.

7. ПРОФІЛІ СЕРТИФІКАТІВ, СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ (CRL) ТА ПРОТОКОЛА ВИЗНАЧЕННЯ СТАТУСУ СЕРТИФІКАТА (OCSP)

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.6 ДСТУ ETSI EN 319 411-1

7.1. Профілі сертифікатів

Пункт 7.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо відомостей, які повинні міститися в кваліфікованих сертифікатах.

7.2. Профілі списку відкликаних сертифікатів

Пункт 7.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо відомостей, які повинні міститися в списках відкликаних сертифікатів.

7.3. Профілі протоколу визначення статусу сертифіката

Пункт 7.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо можливості перевірки статусу кваліфікованого сертифіката

користувача в режимі реального часу через електронні комунікаційні мережі загального користування із використанням протоколу OCSP.

8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.7 ДСТУ ETSI EN 319 411-1

8.1. Частота або обставини оцінювання

Пункт 8.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо частоти та обставин оцінювання Надавача.

8.2. Особа/кваліфікація оцінювача

Пункт 8.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо вимог до кваліфікації посадових осіб контролюючого органу (КО) та органу з оцінки відповідності (ООВ).

8.3. Відносини експерта з об’єктом оцінки

Пункт 8.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо відносин посадових осіб контролюючого органу (КО) та експертів (аудиторів) органу з оцінки відповідності з об'єктом оцінки (Надавач).

8.4. Теми, охоплені оцінюванням

Пункт 8.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо питань, які підлягають перевірці під час державного контролю та під час оцінки відповідності.

8.5. Дії, вжиті внаслідок порушення

Пункт 8.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо дій, які вживаються внаслідок порушення, виявленого за результатами державного контролю або за результатами оцінки відповідності.

8.6. Повідомлення результатів

Пункт 8.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить

інформацію щодо оформлення результатів державного контролю або оцінки відповідності, надання припису про усунення порушень, виявлених під час державного контролю.

8.7. Самоперевірки

Пункт 8.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо проведення Надавачем регулярних внутрішніх аудитів дотримання встановлених вимог.

9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.8 ДСТУ ETSI EN 319 411-1

9.1. Ціни і тарифи

9.1.1. Плата за видачу або поновлення сертифіката

За формування кваліфікованого сертифіката сплачується плата, вартість якої визначається згідно з тарифними планами на надання кваліфікованих електронних довірчих послуг КНЕДП «MASTERKEY», опублікованими на офіційному веб-сайті Надавача.

Поновлення заблокованих кваліфікованих сертифікатів здійснюється на безоплатній основі.

9.1.2. Плата за доступ до сертифіката

Плата за доступ до кваліфікованого сертифіката відсутня.

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

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

9.1.4. Плата за інші послуги

Надавач може надавати користувачам додаткові послуги за плату, серед яких:

- надання засобів кваліфікованого електронного підпису чи печатки користувачам;
- виїзна генерація пари ключів користувача.

9.1.5. Політика відшкодування

Надавач не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Пункт 9.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо фінансової відповідальності Надавача.

9.3. Конфіденційність ділових даних

Пункт 9.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо змісту та обсягу конфіденційної інформації, що знаходиться в розпорядженні Надавача, а також відповідальності за захист конфіденційної інформації.

9.4. Захист персональних даних

Пункт 9.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо концепції захисту персональних даних, визначення персональних даних, а також персональних даних, що не вважаються конфіденційними, щодо відповідальності за захист персональних даних, щодо згоди на використання персональних даних та обставин розкриття персональних даних.

9.5. Права інтелектуальної власності

Питання прав інтелектуальної власності Надавача врегульовані відповідно до вимог чинного законодавства України.

9.6. Зобов’язання та гарантії

Пункт 9.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо зобов’язань та гарантій Надавача, відокремлених пунктів реєстрації Надавача, користувачів, довіряючих сторін, а також інших учасників.

9.7. Відмова від відповідальності

Пункт 9.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо відмови від гарантій.

9.8. Обмеження відповідальності

Пункт 9.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг «MASTERKEY» (додаток 1 до цього Регламенту) містить інформацію щодо обставин для обмеження відповідальності Надавача.

9.9. Відшкодування збитків

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

9.10. Термін дії та припинення дії

Ці Положення сертифікаційних практик застосовуються з моменту їх публікації та діють до закінчення строку дії останнього сертифіката, виданого відповідно до цих положень сертифікаційних практик або до моменту припинення діяльності Надавача.

9.11. Індивідуальні комунікації та угоди з суб'єктами інфраструктури відкритих ключів

Надавач здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на офіційномувеб-сайті Надавача;
- інформування ЦЗО, КО та органу з питань захисту персональних даних шляхом надсилання повідомлень в паперовій та електронній формах;
- надсилання електронних листів на адресу електронної пошти користувача;
- здійснення телефонних дзвінків та смс-інформування на номер телефону користувача.

9.12. Зміни

Внесення змін та доповнень до цих Положень сертифікаційних практик здійснюється Надавачем у разі:

- змін вимог, процесів та процедур, описаних у цих Положеннях сертифікаційних практик;
- змін в законодавстві;
- змін у вимогах до надавачів щодо надання послуг.

Нові версії цих Положень сертифікаційних після внесення змін до неї публікуються на офіційному веб-сайті Надавача.

9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей, Надавач вирішує їх шляхом переговорів та консультацій з учасниками інфраструктури відкритих ключів.

У разі недосягнення учасниками інфраструктури відкритих ключів згоди, спори (розбіжності) вирішуються у судовому порядку відповідно до чинного законодавства України.

9.14. Застосовне право

На відносини, що регулюються цими Положеннями сертифікаційних практик, поширюється чинне законодавство України.

9.15. Дотримання чинного законодавства

Пункт 9.15 Політики сертифіката Надавача містить інформацію щодо нормативно-правових актів, які встановлюють вимоги до надання Надавачем кваліфікованих електронних довірчих послуг.