ДОДАТОК 1
до Регламенту роботи кваліфікованого надавача
електронних довірчих послуг EDIN ID ТОВ "АТС"

ПОЛІТИКА СЕРТИФІКАТА КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ EDIN ID ТОВ "АТС"

Зміст

1. ВСТУП

1.1. Огляд

Ця Політика сертифіката визначає перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг EDIN ID ТОВ “АТС” (далі - КНЕДП ТОВ “АТС”) у процесі реєстрації користувачів електронних довірчих послуг, зокрема, підписувачів та створювачів електронних печаток (далі - користувачі) формування та обслуговування кваліфікованих сертифікатів відкритих ключів (далі - кваліфіковані сертифікати) КНЕДП ТОВ “АТС” та користувачів, зокрема, управління їх статусом (блокування, поновлення та скасування).

Дотримання вимог, визначених у цій Політиці сертифіката, є обов'язковим для керівника КНЕДП ТОВ “АТС” та найманих працівників КНЕДП ТОВ “АТС”, 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 КНЕДП ТОВ “АТС” (ТОВ “АТС”) безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням їхніх кваліфікованих сертифікатів, зокрема, відокремлених пунктів реєстрації КНЕДП ТОВ “АТС”.

Визнання користувачами вимог, визначених у цій Політиці сертифіката, є обов'язковою умовою та підставою для укладення з ними договору про надання електронних довірчих послуг.

Перелік усіх практичних дій та процедур, які застосовуються для реалізації КНЕДП ТОВ “АТС” цієї Політики сертифіката, визначають:

- Положення сертифікаційних практик КНЕДП ТОВ “АТС” щодо кваліфікованих сертифікатів електронного підпису та печатки.

Ця Політика сертифіката відповідає вимогам, визначеним у:

- 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);

- ДСТУ ETSI EN 319 411-2 (ETSI EN 319 411-2) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС” (далі - ДСТУ ETSI EN 319 411-2);

- ДСТУ ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) “Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам” (далі - ДСТУ ETSI EN 319 412-2);

- ДСТУ ETSI EN 319 401 (ETSI EN 319 401, IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг” (далі - ДСТУ ETSI EN 319 401).

ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018 IDT) – “Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів”

ДСТУ EN ISO/IEC 27002:2024 (IDT; ISO/IEC 27002:2022, IDT)– “Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки”

ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) – “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”

ДСТУ ISO/IEC 27003:2018 (ISO/IEC 27003:2017, IDT) – “Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова”

ДСТУ ISO/IEC 27004:2018 (ISO/IEC 27004:2016, IDT) – “Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання”

ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) – “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”

ДСТУ EN ISO/IEC 27007:2022 (ISO/IEC 27007:2020, IDT) – “Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою”

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 та ДСТУ ETSI EN 319 411-2.

Повна назва документа: Політика сертифіката кваліфікованого надавача електронних довірчих послуг EDIN ID ТОВ “АТС”.

Скорочена назва документа: Політика сертифіката КНЕДП ТОВ “АТС”.

Версія: 1.0.

Об'єктний ідентифікатор (OID) цієї Політики сертифіката: 1.2.804.2.1.1.1.2.

Об'єктний ідентифікатор (OID) цієї Політики сертифіката присвоєно відповідно до стандарту ASN.1 згідно з вмістом наведеної нижче таблиці.

Таблиця 1. Структура об'єктного ідентифікатора (OID) Політики сертифіката

Опис	Скорочена назва	Значення (індекс)
Ознака першої гілки (дуги) кореневого вузла світового дерева об'єктних ідентифікаторів (OID), що знаходиться в підпорядкуванні вузла Міжнародної організації стандартизації (ISO)	iso	1
Ознака національного органу стандартизації, що є членом Міжнародної організації стандартизації (ISO)	member-body	2
Унікальний числовий код України відповідно до ДСТУ ISO 3166-1:2009 “Коди назв країн світу” (ISO 3166-1:2006, IDT), затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 р. № 471 (далі - ISO 3166-1)	ua	804
Ознака інфраструктури відкритих ключів	root; security; cryptography; uapki	2.1.1.1
Ознака політики сертифікації	cp	2

Кваліфіковані сертифікати, сформовані КНЕДП ТОВ "АТС", містять об'єктний ідентифікатор (OID) цієї Політики сертифіката, який використовується суб’єктами, які довіряють КНЕДП ТОВ "АТС", для визначення придатності та надійності таких сертифікатів під час автентифікації користувачів, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

1.3. Учасники інфраструктури відкритих ключів

До учасників інфраструктури відкритих ключів зазначених в цьому розділі застосовуються вимоги визначені в пункті 5.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

1.3.1. Надавач

КНЕДП ТОВ "АТС" 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, формування та обслуговування їхніх кваліфікованих сертифікатів, в тому числі, управління їхнім статусом (блокування, поновлення та скасування).

КНЕДП ТОВ "АТС" здійснює реєстрацію користувачів самостійно та/або через представництва і відокремлені пункти реєстрації КНЕДП ТОВ "АТС".

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.3.1.1. Права Надавача

КНЕДП ТОВ "АТС" має право:

надавати електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг;

отримувати документи та/або електронні дані, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті;

проводити під час формування та видачі кваліфікованих сертифікатів перевірку інформації про осіб, яким видаються такі сертифікати, з використанням відомостей інформаційних ресурсів ЄІС МВС (відомостей, що містяться в ЄДДР, та відомостей щодо викрадених (втрачених) документів за зверненнями громадян), ДРФО, ДРАЦС, ЄДР, а також інформації з інших публічних електронних реєстрів відповідно до Закону України "Про публічні електронні реєстри", отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації (https://id.gov.ua/);

отримувати консультації від ЦЗО, КО з питань, пов'язаних з наданням електронних довірчих послуг;

звертатися до ООВ для отримання документів про відповідність;

звертатися до ЦЗО із заявами про формування кваліфікованих сертифікатів , їх скасування, блокування або поновлення;

самостійно обирати в рамках кожної послуги, які саме стандарти вони будуть застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, визначеного Кабінетом Міністрів України.

1.3.1.2. Обов'язки Надавача

КНЕДП ТОВ "АТС" зобов'язаний забезпечувати:

захист персональних даних користувачів відповідно до вимог Закону України "Про захист персональних даних";

функціонування ІКС та програмно-технічного комплексу, що використовуються для надання електронних довірчих послуг, та захист інформації, яка обробляється в них, відповідно до вимог законодавства у сфері електронних довірчих послуг;

створення та функціонування свого веб-сайту;

впровадження, підтримання в актуальному стані та публікацію на своєму веб-сайті відомостей з реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус кваліфікованих сертифікатів через комунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв в електронній формі користувачів про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів;

прийом і перевірка паперових заяв користувачів щодо скасування, блокування та поновлення їхніх кваліфікованих сертифікатів здійснюються протягом одного робочого дня з моменту отримання заяви, відповідно до встановленого режиму роботи КНЕДП ТОВ "АТС";

скасування, блокування та поновлення кваліфікованих сертифікатів відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги";

встановлення під час формування кваліфікованого сертифіката належності відкритого ключа та відповідного йому особистого ключа користувачу;

внесення даних користувача до відповідного кваліфікованого сертифіката;

вжиття організаційних і технічних заходів з управління ризиками, пов'язаними з безпекою електронних довірчих послуг;

інформування КО та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли їм стало відомо про таке порушення;

інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли стало відомо про таке порушення;

унеможливлення використання особистого ключа користувача, якщо стало відомо про компрометацію такого особистого ключа та якщо особистий ключ користувача зберігається у КНЕДП ТОВ "АТС" у межах надання послуги створення, перевірки та підтвердження електронного підпису чи електронної печатки;

постійне зберігання всіх виданих кваліфікованих сертифікатів;

постійне зберігання документів в електронному вигляді та електронних даних, отриманих у зв'язку з наданням електронних довірчих послуг;

внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування шкоди, яка може бути завдана користувачам чи третім особам внаслідок неналежного виконання КНЕДП ТОВ "АТС" своїх зобов'язань, або страхування цивільно-правової відповідальності для забезпечення відшкодування такої шкоди у розмірі, визначеному Законом України "Про електронну ідентифікацію та електронні довірчі послуги";

відновлення розміру внеску на поточному рахунку із спеціальним режимом використання у банку (на рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або розміру страхової суми, визначеного Законом України "Про електронну ідентифікацію та електронні довірчі послуги", протягом трьох місяців у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих користувачам чи третім особам внаслідок неналежного виконання своїх зобов'язань;

використання під час надання кваліфікованих електронних довірчих послуг виключно кваліфікованих сертифікатів, сформованих ЦЗО;

наймання працівників та, за потреби, виконання робіт субпідрядними організаціями, які володіють необхідними для надання електронних довірчих послуг знаннями, досвідом і кваліфікацією, та застосування адміністративних і управлінських процедур, які відповідають національним або міжнародним стандартам;

чітке та вичерпне повідомлення будь-якій особі, яка звернулася за отриманням електронної довірчої послуги, про умови використання такої послуги, у тому числі про будь-які обмеження її використання, перед укладенням договору про надання електронних довірчих послуг;

інформування КО та ЦЗО про намір припинити свою діяльність та про зміни у наданні кваліфікованих електронних довірчих послуг протягом 48 годин з моменту настання таких змін;

передачу ЦЗО або іншому надавачу документованої інформації в разі припинення діяльності з надання кваліфікованих електронних довірчих послуг;

приєднання до програмного інтерфейсу ІКС ЦЗО з метою забезпечення інтероперабельності, дослідження поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень.

1.3.2. Органи реєстрації

Відокремлені пункти реєстрації КНЕДП ТОВ "АТС" є органами реєстрації, що представлені окремими підрозділами, позаштатними одиницями КНЕДП ТОВ "АТС" або юридичними чи фізичними особами, які на підставі договору з КНЕДП ТОВ "АТС", здійснюють реєстрацію користувачів.

До працівників відокремлених пунктів реєстрації КНЕДП ТОВ "АТС , відповідальних за реєстрацію користувачів, висуваються такі ж вимоги, як і до адміністраторів реєстрації, що визначені у пункті 5.3.1.1.2 цієї Політики сертифіката.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.3.3. Користувачі

Користувачами є підписувачі та створювачі електронних печаток, щодо яких КНЕДП ТОВ "АТС" здійснює їх реєстрацію (самостійно або через відокремлені пункти реєстрації КНЕДП ТОВ "АТС"), формування та обслуговування їхніх кваліфікованих сертифікатів.

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

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

1.3.3.1. Права користувачів

Користувачі мають право на:

- вільний вибір надавача довірчих послуг;
- отримання електронних довірчих послуг;
- оскарження дій або бездіяльності надавача та органів державного регулювання у сфері електронних довірчих послуг у судовому порядку;
- відшкодування завданої шкоди та захист своїх прав і законних інтересів;
- подання заяви про скасування, блокування та поновлення свого кваліфікованого сертифіката.

1.3.3.2. Обов'язки користувачів

Користувачі зобов'язані:

- забезпечувати конфіденційність особистого ключа та унеможливлювати доступ до нього сторонніх осіб ;
- невідкладно повідомляти Надавача про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором про надання кваліфікованих електронних довірчих послуг, укладеним з Надавачем;
- своєчасно надавати Надавачу інформацію про зміну ідентифікаційних даних, які містить кваліфікований сертифікат;

- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування кваліфікованого сертифіката.

1.3.4. Суб'єкти, які довіряють Надавачу

Фізичні та юридичні особи, а також їхні інформаційно-комунікаційні системи є суб'єктами, які довіряють КНЕДП ТОВ "АТС", 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 КНЕДП ТОВ "АТС" та користувачів, є іншими учасниками.

До інших учасників належать також ЦЗО та КО, які є наглядовими органами щодо КНЕДП ТОВ "АТС".

Адміністратор ІКС ЦЗО та інтегрованої системи електронної ідентифікації здійснює технічне та технологічне забезпечення у відповідності до вимог статті 7^1 Закону України "Про електронну ідентифікації та електронні довірчі послуги" (зі змінами та доповненнями).

КО (Адміністрація Державної служби спеціального зв'язку та захисту інформації України), зокрема:

- здійснює державний контроль за дотриманням вимог законодавства у сфері електронних довірчих послуг;
- взаємодіє з ЦЗО та ООВ з питань державного контролю за дотриманням вимог законодавства;
- співпрацює з органами з питань захисту персональних даних шляхом невідкладного інформування про порушення вимог законодавства про захист персональних даних, виявлені під час проведення КО перевірок КНЕДП ТОВ "АТС";
- інформує громадськість у разі отримання від КНЕДП ТОВ "АТС" або за результатами його перевірки, відомостей про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів;
- видає приписи щодо усунення порушень вимог законодавства у сфері електронних довірчих послуг;
- накладає адміністративні штрафи за порушення вимог законодавства у сфері електронних довірчих послуг;
- аналізує документи про відповідність за результатами проведення процедур оцінки відповідності КНЕДП ТОВ "АТС" у рамках не виїзних заходів державного нагляду (контролю).

ООВ являє собою організацію, яка проводить відповідну оцінку відповідності вимогам для надавачів електронних довірчих послуг та надає відповідний документ відповідності.

Державні органи оцінки відповідності, акредитовані на проведення сертифікації засобів кваліфікованого електронного підпису чи печатки, формують, підтримують в актуальному стані та публікують на своїх офіційних веб-сайтах переліки сертифікованих ними засобів кваліфікованого електронного підпису чи печатки (Перелік засобів криптографічного захисту інформації, які мають експертний висновок за результатами державної експертизи у галузі КЗІ (cip.gov.ua)).

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

1.4. Використання сертифіката

Використання сертифіката здійснюється відповідно до положень пункту 5.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Крім того, застосовуються такі особливі вимоги:

1.4.1. Дозволене використання сертифіката

1.4.1.1. Види кваліфікованих сертифікатів

КНЕДП ТОВ "АТС" формує кваліфіковані сертифікати таких видів:

- кваліфікований сертифікат електронного підпису, що пов'язує відкритий ключ кваліфікованого або удосконаленого електронного підпису з фізичною особою та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованого або удосконаленого електронного підпису;

- кваліфікований сертифікат електронного підпису, що пов'язує відкритий ключ кваліфікованої або удосконаленого електронного підпису пов’язаного з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованого або удосконаленого електронного підпису;

- кваліфікований сертифікат електронної печатки, що пов'язує відкритий ключ кваліфікованої або удосконаленої електронної печатки з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованої або удосконаленої електронної печатки;

- кваліфікований сертифікат шифрування, що пов'язує відкритий ключ кваліфікованого або удосконаленого електронного підпису чи печатки з фізичною особою, юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ “АТС” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.4.1.2. Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати КНЕДП ТОВ "АТС" формуються ЦЗО зі строком дії не більше 5 років.

Строк дії кваліфікованих сертифікатів КНЕДП ТОВ "АТС" становить:

1. СМР 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», (далі - ДСТУ 4145-2002), розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

2. особистого ключа КНЕДП ТОВ "АТС" 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

3. TSP 5 років;

4. OCSP 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

5. OCSP 5 рік з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

Кваліфіковані сертифікати користувачів формуються КНЕДП ТОВ "АТС" зі строком дії до 2 років.

Кваліфіковані сертифікати обов'язково містять відомості про початок та закінчення строку їх дії.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

1.4.2. Заборонене використання сертифіката

Кваліфікований сертифікат може використовуватися лише відповідно до зазначеного у ньому призначення відкритого ключа (“keyUsage”).

1.4.3. Використання тестових сертифікатів

Формування тестових сертифікатів здійснюється КНЕДП ТОВ "АТС" через інтеграцію з тестовим програмно-технічним комплексом, створеним на офіційному веб-сайті ЦЗО в рамках інструменту моніторингу сфери електронних довірчих послуг (https://czo.gov.ua/tool) відповідно до наказу Міністерства цифрової трансформації України від 18.01.2024 № 11 “Про деякі питання діяльності та розвитку у сферах електронної ідентифікації та електронних довірчих послуг”, зареєстрованого в Міністерстві юстиції України 05 лютого 2024 р. за № 180/41525.

1.5. Управління Політикою сертифіката

1.5.1. Відповідальність за Політику сертифіката

Ця Політика сертифіката підтримується ТОВАРИСТВОМ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ “АТС” (далі - ТОВ “АТС”).

ТОВ «АТС», код платника податків згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб-підприємців та громадських формувань – 37636185, є зареєстрованою відповідно до законодавства юридичною особою, яка здійснює діяльність у сфері надання кваліфікованих електронних довірчих послуг. Компанія внесена державним підприємством «ДІЯ» - Адміністратором ІКС ЦЗО, - до Довірчого списку кваліфікованих надавачів електронних довірчих послуг.

Центральний офіс КНЕДП ТОВ "АТС" представлений окремим підрозділом або позаштатною структурою ТОВ "АТС", яка здійснює організацію та надання кваліфікованих електронних довірчих послуг як безпосередньо, так і через представництва КНЕДП ТОВ "АТС", забезпечуючи при цьому відповідність діяльності вимогам чинного законодавства щодо кваліфікованих надавачів електронних довірчих послуг. Представництва КНЕДП ТОВ "АТС" включають відокремлені пункти реєстрації, які можуть бути як окремими підрозділами або позаштатними одиницями КНЕДП ТОВ "АТС", так і юридичними чи фізичними особами, що діють на підставі договору з КНЕДП ТОВ "АТС". Вони здійснюють реєстрацію користувачів

засобів електронної ідентифікації чи підписувачів, забезпечуючи дотримання вимог чинного законодавства у сферах електронної ідентифікації, електронних довірчих послуг та захисту інформації.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ "АТС" або від імені представництва.

Реквізити ТОВ “АТС”:

- Код згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб-підприємців та громадських формувань (ЄДРПОУ): 37636185.
- Адреса: вул. Михайла Донця, буд. 6, м. Київ, 03061, Україна.
- Контактний телефон: +380(44)359-01-12.
- Адреса електронної пошти: ca@edin.ua

Реквізити КНЕДП ТОВ “АТС”:

- Код згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб-підприємців та громадських формувань (ЄДРПОУ): 37636185.
- Адреса: вул. Михайла Донця, буд. 6, м. Київ, 03061, Україна.
- Адреси веб-сайтів: https://id.edin.ua; https://ca.edin.ua
- Контактні особи: підрозділ відповідальний за діяльність КНЕДП.
- Контактний телефон: +380(44)359-01-12.
- Адреса електронної пошти: ca@edin.ua.

Ця Політика сертифіката структурована відповідно до RFC 3647 “Інфраструктура відкритих ключів Інтернету X.509 Політика сертифікатів і практика сертифікації” і містить всю необхідну інформацію.

Ця Політика сертифіката, а також зміни до неї підписуються керівником профільного підрозділу, на якого покладено виконання функцій Керівника КНЕДП ТОВ “АТС”, який відповідає за дотримання, визначених у ній правил, та затверджується директором ТОВ “АТС”.

Ця Політика сертифіката, а також зміни до неї 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

Відповідно до пункту 9.12 цієї Політики сертифіката.

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

У цій Політиці сертифіката терміни застосовуються у значеннях, наведених у Цивільному кодексі України, Законах України “Про захист інформації в інформаційно-комунікаційних системах”, “Про захист персональних даних”, “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, “Про електронні комунікації”, “Про електронну ідентифікацію та електронні довірчі послуги”, постанові Кабінету Міністрів України від 28.06.2024 р. № 764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг”, інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Перелік скорочень

ДРФО Державний реєстр фізичних осіб - платників податків
ЄДДР Єдиний державний демографічний реєстр
ЄДР Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄІС МВС Єдина інформаційна система Міністерства внутрішніх справ України
ІКС Інформаційно-комунікаційна система
КЗІ Криптографічний захист інформації
КО Контролюючий орган (Адміністрація державної служби спеціального зв'язку та захисту інформації України)
ООВ Орган з оцінки відповідності
ЦЗО Центральний засвідчувальний орган (Міністерство цифрової трансформації України)
CMP Certificate Management Protocol
OCSP Online Certificate Status Protocol
TSP Time Stamp Protocol
СУІБ Система управління інформаційною безпекою відповідно до положень стандарту ISO/IEC 27001:2022

2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги визначені в положеннях пункту 6.1 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Крім того, застосовуються такі особливі вимоги:

2.1. Репозиторій/веб-сайт

КНЕДП ТОВ "АТС" повинен забезпечувати:

створення та функціонування веб-сайту КНЕДП ТОВ "АТС", який є офіційним інформаційним ресурсом КНЕДП ТОВ “АТС”;

впровадження, підтримання в актуальному стані та публікацію на веб-сайті КНЕДП ТОВ "АТС" відомостей з реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через комунікаційні мережі загального користування.

КНЕДП ТОВ "АТС" також повинен забезпечувати інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на веб-сайті КНЕДП ТОВ "АТС".

КНЕДП ТОВ "АТС" через веб-сайт КНЕДП ТОВ "АТС" (https://ca.edin.ua) забезпечує вільний доступ до:

- відомостей про КНЕДП ТОВ "АТС";
- даних про внесення відомостей про КНЕДП ТОВ "АТС" до Довірчого списку;
- Політики сертифіката КНЕДП ТОВ "АТС";
- відповідних Положень сертифікаційних практик КНЕДП ТОВ "АТС";
- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП ТОВ "АТС";
- кваліфікованих сертифікатів КНЕДП ТОВ "АТС";
- переліку кваліфікованих електронних довірчих послуг, які надає КНЕДП ТОВ "АТС";

- даних про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС";

- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги - відомостей про відокремлені пункти реєстрації КНЕДП ТОВ "АТС";

- реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

- відомостей про обмеження під час використання кваліфікованих сертифікатів користувачами;

- даних про порядок перевірки чинності кваліфікованого сертифіката, у тому числі умови перевірки статусу сертифіката;

- перелік актів законодавства у сфері електронних довірчих послуг.

Відомості про умови надання кваліфікованих електронних довірчих послуг, у тому числі умови та порядок їх оплати, можуть оприлюднюватися на рекламно-інформаційному веб-сайті ТОВ «АТС»

Ця Політика сертифіката доступна 24 години на добу 7 днів на тиждень у форматі лише для читання на веб-сайті КНЕДП ТОВ "АТС".

КНЕДП ТОВ "АТС" забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик, списків відкликаних сертифікатів, договорів, актів законодавства та інших нормативних документів на веб-сайті КНЕДП ТОВ "АТС".

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

Кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію, публікуються одразу після формування таких кваліфікованих сертифікатів та виконання користувачами умов договору про надання кваліфікованих електронних довірчих послуг.

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

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

2.2.2. Публікація сертифікатів Надавача

Кваліфіковані сертифікати КНЕДП ТОВ "АТС" повинні публікуватися на веб-сайті КНЕДП ТОВ "АТС" одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати серверів КНЕДП ТОВ "АТС" публікуються одразу після їх формування КНЕДП ТОВ "АТС".

КНЕДП ТОВ "АТС" забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик КНЕДП ТОВ "АТС", CRL, договорів, законодавчих актів та інших нормативних документів на веб-сайті КНЕДП ТОВ "АТС": https://ca.edin.ua.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.2.3. Доступ до сертифікатів користувачів

Кваліфікований сертифікат користувача після його формування КНЕДП ТОВ "АТС" повинен бути доступний користувачу, для якого такий сертифікат був сформований.

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

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

2.2.4. Строк закінчення дії сертифіката

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років.

Строк дії кваліфікованих сертифікатів КНЕДП ТОВ "АТС" становить:

1. CMP 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

2. особистого ключа КНЕДП ТОВ "АТС" 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

3. TSP 5 років;

4. OCSP 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

5. OCSP 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

• алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.3. Час та періодичність публікації

Кваліфіковані сертифікати серверів КНЕДП ТОВ "АТС" публікуються одразу після їх формування КНЕДП ТОВ "АТС".

Кваліфіковані сертифікати серверів КНЕДП ТОВ "АТС" публікуються одразу після їх формування КНЕДП ТОВ "АТС".

Кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію, публікуються КНЕДП ТОВ "АТС" одразу після формування таких сертифікатів.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

2.4. Контроль доступу до репозиторію/веб-сайту

Репозиторій/веб-сайт захищений від несанкціонованого доступу та змін. КНЕДП ТОВ "АТС" забезпечує цілодобове функціонування власного репозиторію/веб-сайту.

За захист інформації на репозиторії/веб-сайті та базі даних КНЕДП ТОВ "АТС" відповідають працівники КНЕДП згідно їх функціональних обов'язків. Доступ до управління репозиторієм/веб-сайтом та базою даних КНЕДП ТОВ "АТС" надано відповідним адміністраторам КНЕДП ТОВ "АТС". Захист інформації на веб-сайті, в репозиторії та базі даних КНЕДП ТОВ "АТС" здійснюється відповідно до реалізованої СУІБ КНЕДП ТОВ "АТС".

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 та ДСТУ ETSI EN 319 411-2.

3.1. Позначення

Кваліфіковані сертифікати обов'язково повинні містити відомості, визначені частиною другою статті 23 Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

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 цієї Політики сертифіката.

Позначення, що використовуються в кваліфікованих сертифікатах користувачів, наведені в Таблиці 2.

Таблиця 2. Позначення, що використовуються в кваліфікованих сертифікатах користувачів

Найменування	Значення
Country (C)	Назва країни відповідно до ДСТУ ISO 3166-1:2009 "Коди назв країн світу" (ISO 3166-1:2006, IDT), затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 р. № 471
Organization (O)	Найменування юридичної особи для кваліфікованого сертифіката юридичної особи або кваліфікованого сертифіката представника юридичної особи. Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне
Organizational Unit (OU)	Назва підрозділу або відділу в організації. Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне

State or Province (S)	Назва області місцезнаходження або місця реєстрації користувача
Locality (L)	Назва міста місцезнаходження або місця реєстрації користувача
Common Name (CN)	Повне ім’я (найменування) користувача, якому належить кваліфікований сертифікат
E-Mail Address (E)	Електронна пошта користувача, якому належить кваліфікований сертифікат
Title (T)	Посада (для кваліфікованих сертифікатів представників юридичної особи за необхідності)
UniqueIdentifier(UID)	Ідентифікатор користувача, якому належить кваліфікований сертифікат: - для користувачів, що є фізичними особами, для UID використовується РНОКПП або номер паспорта; - для користувачів, що є фізичними особами - підприємцями, для UID використовується РНОКПП; - для користувачів, що є юридичними особами, для UID використовується код згідно з ЄДРПОУ
Серійний номер (SERIALNUMBER)	Ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг, що є фізичною особою чи фізичною особою-підприємцем: УНЗР або РНОКПП або серія (за наявності) та номер паспорта

Відповідні Положення сертифікаційних практик КНЕДП ТОВ “АТС” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

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 цієї Політики сертифіката.

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, розділу 7 цієї Політики сертифіката.

3.1.3. Анонімність або використання псевдонімів

Процедура використання псевдонімів здійснюється відповідно до Порядку використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 28.06.2024 №764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг” та ДСТУ ETSI EN 319 412-2.

3.1.4. Правила інтерпретації різних форм позначень сертифіката

Міжнародні літери повинні кодуватися згідно з UTF-8.

3.1.5. Унікальність позначень сертифіката

КНЕДП ТОВ "АТС" повинен гарантувати, що сертифікати з однаковими даними, зазначеними в полях “Common Name” та “SerialNumber”, не видаються різним користувачам.

3.1.6. Визнання, автентифікація та роль торгових марок

Не застосовується.

3.2. Первинна перевірка ідентифікації

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2.2 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Крім того, застосовуються такі особливі вимоги:

3.2.1. Метод підтвердження володіння особистим ключем

Підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката, забезпечується в один із таких способів:

- візуальним та технічним контролем запису та передачі до КНЕДП ТОВ "АТС" запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після ідентифікації користувача, за умови його особистої присутності;

- технічним контролем запису та передачі до КНЕДП ТОВ "АТС" запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після ідентифікації заявника та отримання ідентифікаційних даних за допомогою механізмів ідентифікації, зазначених у підпункті 3.2.2 цієї Політики сертифіката, а також відповідних Положень сертифікаційних практик КНЕДП ТОВ "АТС".

У всіх випадках за допомогою засобів кваліфікованого електронного підпису чи печатки КНЕДП ТОВ "АТС" здійснюється перевірка удосконаленого електронного підпису, створеного за допомогою особистого ключа користувача на запиті на формування кваліфікованого сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті.

Підтвердження володіння користувачем особистим ключем здійснюється у спосіб, що виключає розкриття змісту або доступ до самого особистого ключа.

3.2.2. Ідентифікація/Автентифікація особи

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

Ідентифікація особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката, здійснюється в один із таких способів:

1) за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством порядку з ЄДДР, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи (паспорт громадянина України, паспорт громадянина України для виїзду за кордон, посвідка на постійне/тимчасове місце проживання);

2) віддалено (без особистої присутності особи), з одночасним використанням засобу електронної ідентифікації, що має високий або середній рівень довіри, раніше виданого фізичній особі, фізичній особі - підприємцю чи уповноваженому представнику юридичної особи за особистої присутності, та багатофакторної автентифікації;

3) за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті, раніше сформованому та виданому згідно з підпунктом 1 або 2 цього пункту, за умови чинності такого сертифіката;

4) з використанням інших способів ідентифікації, визначених законом, надійність яких є еквівалентною особистій присутності та підтверджена ООВ.

У разі відсутності в іноземців та осіб без громадянства документів, виданих відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, їх ідентифікація у спосіб, визначений підпунктом 1 пункту 3.2.2 цієї Політики сертифіката, здійснюється за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки або автентифікації веб-сайту) чи фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) КНЕДП ТОВ "АТС" зобов'язаний використовувати інформацію про юридичну особу чи фізичну особу - підприємця, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, а також пересвідчитися, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа або автентифікації веб-сайту.

Перевірка цивільної правоздатності та дієздатності 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 здійснюється з використанням інформації з міжнародного договору або іншого офіційного документа, на підставі якого створена та/або діє міжнародна організація.

Під час проведення процедур ідентифікації та автентифікації Заявника можуть використовуватися, а також рекомендується використовувати сервіси перевірки чинності документів та ідентифікаційної інформації про особу:

- «Перевірка за базою недійсних документів» (dmsu.gov.ua);
- «Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань» (usr.minjust.gov.ua);

Також додатково можуть використовуватися сервіси:

- Єдиний державний веб-портал електронних послуг (Портал Дія);
- Сервіси та дані, отримані з інших продуктів і рішень компанії;
- «Youcontrol», «Opendatabot» та інші ресурси;
- У випадках передачі обслуговування кваліфікованих сертифікатів користувачів та документованої інформації, на підставі якої були сформовані зазначені сертифікати, від надавача, який припиняє свою діяльність, до КНЕДП ТОВ "АТС" процедура ідентифікації цих користувачів проводиться одним із способів зазначених в цьому пункті та відповідно до Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

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

Після створення електронних копій паперові документи повертаються заявнику.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

3.2.3. Неперевірена інформація про користувача

Використання неперевіреної інформації про користувача не допускається.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

3.2.4. Підтвердження повноважень

Уповноважений представник юридичної особи або фізичної особи - підприємця підписує документи, необхідні для формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця. КНЕДП ТОВ "АТС" під час формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємцю здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи - підприємця відповідно до вимог, встановлених підпунктом 3.2.2 цієї Політики сертифіката та перевіряє обсяг його повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця, чи з використанням інформації, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

Уповноваженим представником юридичної особи є керівник юридичної особи, який зазначений в ЄДР, або співробітник (керівник відокремленого підрозділу (філії) юридичної особи) наділений повноваженнями укладання правочинів з третіми особами, які зазначаються в наказі, довіреності тощо.

Перед формуванням кваліфікованого сертифіката представника юридичної особи та самозайнятої особи (адвокат, нотаріус, приватний виконавець, арбітражний керуючий тощо) також здійснюється перевірка повноважень користувача шляхом перевірки документів, що засвідчують його повноваження або приналежність до юридичної особи, право на здійснення діяльності у визначеній сфері (посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або шляхом перевірки інформації у відповідних державних інформаційних системах (реєстри, бази даних тощо).

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

3.3. Ідентифікація та автентифікація за заявою на повторне формування кваліфікованих сертифікатів відкритого ключа

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2.3 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

3.3.1. Ідентифікація та автентифікація користувача за заявою про формування сертифіката за умови чинності попереднього сертифіката

Для формування нового кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований КНЕДП ТОВ "АТС" або іншим кваліфікованим надавачем електронних довірчих послуг за умови дотримання вимог статті 22 Закону, такий користувач проходить процедуру автентифікації за поданою в електронній формі до КНЕДП ТОВ "АТС" заявою про формування кваліфікованого сертифіката за умови незмінності ідентифікаційних даних, внесених до попереднього кваліфікованого сертифіката, з моменту формування кваліфікованого сертифіката до моменту створення кваліфікованого електронного підпису на заяві про формування кваліфікованого сертифіката.

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

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

3.3.2. Ідентифікація та автентифікація користувача на отримання повторного формування кваліфікованого сертифіката відкритого ключа у разі скасування сертифіката

У разі, якщо кваліфікований сертифікат користувача скасовано, для формування нового кваліфікованого сертифіката в КНЕДП ТОВ "АТС" користувач повинен пройти ідентифікацію та автентифікацію згідно з умовами для первинної ідентифікації та автентифікації користувача.

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

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Користувач може подати заяву на скасування, блокування або поновлення кваліфікованого сертифіката у паперовому або електронному вигляді.

Паперова заява подається особисто Користувачем до Надавача, містить власноручний підпис і приймається протягом робочого дня відповідно до графіка, оприлюдненого на сайті Надавача. Після створення електронних копій паперові документи повертаються заявнику.

Електронна заява надсилається Надавачу і має бути підписана КЕП, УЕП, що базується на кваліфікованому сертифікаті Користувача, або Дія.Підпис та може бути подана цілодобово.

Для блокування або скасування кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований КНЕДП ТОВ "АТС", такий користувач проходить процедуру автентифікації за поданою в електронній формі до КНЕДП ТОВ "АТС" заявою про блокування або скасування кваліфікованого сертифіката.

Блокування може відбуватись у разі невиконання умов договірних відносин з Користувачем.

Подання користувачем електронних довірчих послуг заяви про скасування або блокування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи користувача. Подання заяви про скасування або блокування кваліфікованого сертифіката відкритого ключа електронного підпису працівника юридичної особи чи фізичної особи - підприємця за підписом уповноваженої особи відповідної юридичної особи чи фізичної особи - підприємця.

У телефонному режимі блокування здійснюється за умови підтвердження через ОТР або за кодовим словом. Факт звернення може бути зафіксований у заяві адміністратором Надавача. Контактна інформація для звернень оприлюднена на веб-сайті Надавача.

Користувач має можливість заблокувати або скасувати власний кваліфікований сертифікат безпосередньо через кабінет користувача. У кабінеті користувача, під час блокуванні або скасуванні сертифікатів, відбувається підтвердження звернення за допомогою ОТР/кодового слова або введенням пароля до особистого ключа.

Поновлення сертифіката можливе на підставі письмової заяви, поданої особисто Користувачем у паперовому вигляді протягом робочого дня. Перед поновленням здійснюється верифікація Користувача. Після створення електронних копій паперові документи повертаються заявнику. Також поновлення може бути ініційоване через Кабінет Користувача з автентифікацією за ОТР. Поновлення сертифіката може відбуватись на підставі договірних відносин з Користувачем.

Пункт 4.9 цієї Політики сертифіката та відповідних Положень сертифікаційних практик КНЕДП ТОВ "АТС" містить додаткову інформацію щодо блокування та скасування кваліфікованого сертифіката користувача.

3.5. Процес перевірки та збереження даних підпису

Набір процедур служб перевірки та збереження КНЕДП ТОВ «АТС» для перевірки технічної дійсності електронного підпису або електронної печатки базується на процесах, визначених у стандарті ETSI TS 119 102-1 [ETSI 119 102], та детально описаний у Політиці щодо кваліфікованих послуг з перевірки та кваліфікованих послуг зі збереження кваліфікованих електронних підписів і печаток КНЕДП ТОВ «АТС».

Для виконання процедур перевірки використовується окремий сервіс або програмний застосунок Надавача, безпосередньо інтегрований з його інформаційними системами.

Цей сервіс (або застосунок) публікується Надавачем у відкритому доступі та доступний користувачам для самостійного використання під час перевірки дійсності кваліфікованих сертифікатів, статусу електронного підпису чи інших довірчих даних.

У зазначеній Політиці також визначено механізми довгострокового збереження електронних підписів і печаток, які забезпечують підтримання їх доказової дійсності протягом усього строку зберігання, відповідно до вимог ETSI EN 319 422 та ETSI TS 119 511.

Ці механізми передбачають використання методів збереження та продовження криптографічної достовірності шляхом додавання часових позначок, повторного підпису та застосування актуальних алгоритмів криптографічного захисту.

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 та ДСТУ ETSI EN 319 411-2.

4.1. Запит на сертифікат

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 лише після:

- приймання та реєстрації заяви на його формування,
- ідентифікації та автентифікації особи користувача,
- підтвердження володіння користувачем особистим ключем, відповідний відкритий ключ якого використовується для формування кваліфікованого сертифіката.

Пункт 4.1 відповідних Положень сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію щодо процесу реєстрації користувача.

4.2. Обробка запиту на сертифікат

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.2 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС КНЕДП ТОВ "АТС" за участю адміністратора реєстрації, працівника відокремленого пункту реєстрації КНЕДП ТОВ "АТС", на якого покладено обов’язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв’язку, які забезпечують конфіденційність та цілісність даних. Автоматична обробка запитів не виключає процесів ідентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

Під час обробки запиту на формування кваліфікованого сертифіката засобами ІКС КНЕДП ТОВ "АТС" здійснюється перевірка унікальності відкритого ключа в реєстрі чинних,

блокованих та скасованих сертифікатів відкритих ключів та забезпечується унікальність серійного номера кваліфікованого сертифіката користувача.

Обробка запиту на формування кваліфікованого сертифіката, поданого разом із заявою на реєстрацію, здійснюється Надавачем відповідно до внутрішніх процедур та організаційних можливостей, з урахуванням забезпечення безперервності надання послуг, у строк, достатній для виконання всіх необхідних процедур ідентифікації, перевірки та формування сертифіката.

4.3. Формування сертифіката

Надання сформованого кваліфікованого сертифіката користувачу здійснюється в один із таких способів:

- шляхом публікації сформованого кваліфікованого сертифіката на веб-сайті КНЕДП ТОВ "АТС";
- шляхом запису файлу із сформованим кваліфікованим сертифікатом на носій інформації, наданий користувачем;
- шляхом надсилання файлу із сформованим кваліфікованим сертифікатом на адресу електронної пошти, вказану користувачем у заяві на формування кваліфікованого сертифіката;
- шляхом відображення сформованого сертифіката в особистому кабінеті користувача з можливістю його перегляду та завантаження;
- через інші сервіси Надавача, що забезпечують можливість перегляду, перевірки чинності або зчитування сформованого кваліфікованого сертифіката.

Заявник повинен перевірити свої ідентифікаційні дані, внесені Надавачем до кваліфікованого сертифіката відкритого ключа. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки. Заявник повинен використовувати особистий ключ для створення кваліфікованого електронного підпису чи печатки тільки після проведення перевірки. Використання підписувачем особистого ключа є фактом визнання ним кваліфікованого сертифіката відповідного відкритого ключа.

У разі виявлення Заявником невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката відкритого ключа, його власник звертається до Надавача для скасування кваліфікованого сертифіката відкритого ключа та формування нового сертифіката у порядку, встановленому цим Регламентом.

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

4.4. Прийняття сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Кваліфікований сертифікат користувача публікується на веб-сайті КНЕДП ТОВ "АТС" за посиланням https://ca.edin.ua/certificates-search відразу після обробки запиту на сертифікат. Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені КНЕДП ТОВ "АТС" до кваліфікованого сертифіката. КНЕДП ТОВ "АТС" повинен надавати відповідні консультації щодо проведення такої перевірки.

Користувач повинен використовувати особистий ключ для створення кваліфікованого електронного підпису тільки після проведення перевірки. Використання користувачем особистого ключа є фактом визнання ним кваліфікованого сертифіката, що відповідає його

відкритому ключу. Перевірка працездатності свого особистого ключа та ідентифікаційних даних внесених до кваліфікованого сертифіката здійснюється користувачем за допомогою сервісів спеціалізованого програмного забезпечення, що доступні на веб-сайті КНЕДП ТОВ "АТС" https://ca.edin.ua.

У разі виявлення користувачем протягом однієї доби невідповідності ідентифікаційних даних, внесених КНЕДП ТОВ "АТС" до кваліфікованого сертифіката, користувач повинен звернутися до КНЕДП ТОВ "АТС" для скасування кваліфікованого сертифіката та безплатного формування нового сертифіката. У разі звернення користувача після 24 годин формування сертифіката здійснюється на платній основі.

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

4.5. Використання пари ключів і сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

4.5.1. Використання особистого ключа та сертифіката користувачем

Користувач зобов'язаний дотримуватися таких правил під час використання особистого ключа:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- не передавати особистий ключ або засоби його зберігання іншим особам, навіть тимчасово;
- невідкладно повідомляти КНЕДП ТОВ "АТС" про підозру або факт компрометації особистого ключа;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування відповідного кваліфікованого сертифіката;
- особисто відповідати за захист паролю від особистого ключа;
- негайно подавати заяву про скасування або блокування сертифіката у разі виявлення будь-яких загроз для його безпеки;
- регулярно оновлювати програмне забезпечення, яке використовується для роботи з КЕП, з метою підтримки його безпеки та функціональності.

Користувач зобов’язаний використовувати кваліфікований сертифікат відповідно до зазначеного у ньому призначення відкритого ключа (“keyUsage”) та обмежень щодо його використання.

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

- цієї Політики сертифіката;
- відповідних Положень сертифікаційних практик КНЕДП ТОВ "АТС";
- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП ТОВ "АТС";
- Договору про надання кваліфікованих електронних довірчих послуг, укладеного з КНЕДП ТОВ "АТС" (ТОВ "АТС").

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

Кваліфіковані сертифікати користувачів, сформовані КНЕДП ТОВ "АТС", можуть використовуватися будь-якими суб’єктами, які довіряють КНЕДП ТОВ "АТС", з метою їх автентифікації, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

Перш ніж прийняти кваліфікований електронний підпис чи печатку користувача, суб’єкт, який довіряє КНЕДП ТОВ "АТС", повинен перевірити таку інформацію:

- статус кваліфікованого сертифіката користувача, сферу використання кваліфікованого сертифіката користувача, обмеження використання та інформацію про кваліфікований сертифікат користувача.

- відповідність особистого ключа кваліфікованого електронного підпису чи печатки відкритому ключу зазначеному в кваліфікованому сертифікаті користувача.

Суб’єкт, який довіряє КНЕДП ТОВ "АТС", повинен виконати такі перевірки:

- перевірити статус кваліфікованого сертифіката користувача на момент накладання кваліфікованого електронного підпису чи печатки за допомогою OCSP-серверу КНЕДП ТОВ "АТС" (сервер перевірки статусу кваліфікованого сертифіката), сферу використання (поле KeyUsage в сертифікаті), обмеження використання та інформацію про кваліфікований сертифікат, щоб переконатися, що кваліфікований сертифікат користувача чинний в даний момент;

- перевірити статус кваліфікованого сертифіката КНЕДП ТОВ "АТС" під час накладання кваліфікованого електронного підпису чи печатки користувачем.

Кваліфікований електронний підпис чи печатка вважаються дійсними, коли здійснені результати перевірки в наведених вище пунктах виконані успішно та є дійсними одночасно.

Суб’єкт, який довіряє КНЕДП ТОВ "АТС", несе відповідальність за наслідки невиконання або неналежного виконання встановленої процедури перевірки чинності кваліфікованого сертифіката, у тому числі за бездіяльність, що призвела до використання недійсного сертифіката, а також за дії, вчинені з використанням результатів перевірки, якщо йому було відомо або мало бути відомо про недійсність відповідного сертифіката на момент перевірки.те, що не дотримувалась вищевказаної процедури перевірки або виконувала перевірку, знаючи, що кваліфікований сертифікат не чинний на момент перевірки.

Під час використання відкритого ключа та кваліфікованого сертифіката користувача суб’єкти, які довіряють КНЕДП ТОВ "АТС", повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- цієї Політики сертифіката;

- відповідних Положень сертифікаційних практик КНЕДП ТОВ "АТС".

4.6. Поновлення сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.6 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП ТОВ "АТС" зобов'язаний забезпечувати, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів про поновлення їхніх кваліфікованих сертифікатів, які були заблоковані;

- прийом та перевірку заяв у паперовій формі користувачів про поновлення їхніх кваліфікованих сертифікатів, які були заблоковані, протягом одного робочого дня після надходження заяви та згідно з режимом роботи КНЕДП ТОВ "АТС";

- поновлення кваліфікованих сертифікатів, які були заблоковані, відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

4.7. Повторне формування сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.7 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП ТОВ "АТС" здійснює формування кваліфікованого сертифіката користувача, зокрема на підставі чинного кваліфікованого сертифіката, сформованого КНЕДП ТОВ "АТС", що містить ідентифікаційні дані користувача, отримані за результатами його ідентифікації в один із таких способів:

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

- віддалено (без особистої присутності особи), з одночасним використанням засобу електронної ідентифікації, що має високий або середній рівень довіри, раніше виданого фізичній особі, фізичній особі - підприємцю чи уповноваженому представнику юридичної особи за особистої присутності, та багатофакторної автентифікації.

Сформувати новий кваліфікований сертифікат користувач також може після закінчення строку дії та у разі нагальної потреби (компрометації особистого ключа чи паролю до нього, втрати особистого ключа, зміни відомостей, що містяться в кваліфікованому сертифікаті користувача), звернувшись до КНЕДП ТОВ "АТС" або відокремлений пункт реєстрації КНЕДП ТОВ "АТС".

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

4.8. Зміна (модифікація) сертифіката

Внесення змін до кваліфікованого сертифіката не допускається.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

4.9. Скасування та блокування сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.9 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП ТОВ "АТС" зобов'язаний забезпечувати, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих КНЕДП ТОВ "АТС";

- прийом та перевірку заяв у паперовій формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих КНЕДП ТОВ "АТС", протягом одного робочого дня після надходження заяви та згідно з режимом роботи КНЕДП ТОВ "АТС";

- скасування та блокування кваліфікованих сертифікатів, сформованих КНЕДП ТОВ "АТС", відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Користувач має право за власним бажанням здійснити скасування кваліфікованого сертифіката шляхом проходження електронної ідентифікації за допомогою засобів

електронної ідентифікації, які мають високий та середній рівень довіри, відповідно до пункту 3.4 цієї Політики.

Користувач має право за власним бажанням здійснити блокування кваліфікованого сертифіката. Блокування кваліфікованого сертифіката може здійснюватися КНЕДП ТОВ "АТС" за паперовою заявою про зміну статусу кваліфікованого сертифіката або віддалено, після ідентифікації користувача за OTP-кодом або ключовою фразою внесеною до заяви про реєстрацію. Після створення електронних копій паперові документи повертаються заявнику. Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення чинності кваліфікованого сертифіката.

Кваліфікований сертифікат втрачає чинність з моменту зміни його статусу на "скасований".

Скасований кваліфікований сертифікат поновленню не підлягає.

Кваліфікований сертифікат вважається заблокованим з моменту зміни його статусу на "заблокований".

Кваліфікований сертифікат, статус якого змінено на "заблокований", у період блокування є нечинним та не використовується.

Кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію, публікуються одразу після формування таких сертифікатів.

КНЕДП ТОВ "АТС" формує списки відкликаних сертифікатів (CRL) 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 КНЕДП ТОВ "АТС".

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

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

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів користувачів. Повний список відкликаних сертифікатів формується та публікується 1 (один) раз на тиждень та містить інформацію про всі відкликані сертифікати, які були сформовані КНЕДП ТОВ "АТС".

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.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" містять додаткову інформацію.

4.10. Служби статусу сертифіката

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

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.

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 пунктах 5, 6.3 і 7.3 ДСТУ ETSI EN 319 401.

5.1. Контроль фізичної безпеки

Контроль фізичної безпеки здійснюється відповідно до положень пункту 6.4.2 ДСТУ ETSI EN 319 411-1:2022

Крім того, застосовуються такі особливі вимоги:

5.1.1. Вимоги до приміщень Надавача

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.1.2. Фізичний доступ

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.2. Процедурний контроль

Процедурний контроль здійснюється відповідно до вимог, визначених в пункті 6.4.3 ДСТУ ETSI EN 319 411.

5.3. Контроль персоналу

Контроль персоналу здійснюється відповідно до вимог, визначених в пункті 6.4.4 ДСТУ ETSI EN 319 411.".

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.3.1. Довірені ролі персоналу

Персоналом КНЕДП ТОВ "АТС" є:

- керівник;
- адміністратор реєстрації;
- адміністратор сертифікації;
- адміністратор безпеки;
- аудитор системи;
- системний адміністратор.

Надавач для надання електронних довірчих послуг призначає розпорядчим актом керівника КНЕДП ТОВ "АТС", адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки, аудитора системи (далі - працівники Надавача). Надавач має право призначити розпорядчим актом заступника керівника Надавача, який виконує функції керівника Надавача у разі його відсутності або за його письмовим дорученням.

5.3.1.1.1. Керівник

Керівник профільного підрозділу КНЕДП ТОВ "АТС" є посадовою особою Надавача, виконує функції керівника кваліфікованого надавача електронних довірчих послуг. Керівник КНЕДП ТОВ «АТС» на яку покладені обов'язки керівника профільного (технічного) підрозділу в

межах виконання своїх обов'язків відповідає за організацію та контроль процесів, направлених на забезпечення функціонування, розвитку КНЕДП ТОВ "АТС" та захист інформації в ІКС КНЕДП ТОВ "АТС", а саме:

- ініціює розробку та затверджує розпорядчі документи, згідно з якими у КНЕДП повинен здійснюватися облік та забезпечуватися захист ключових даних та носіїв;
- ініціює та приймає участь у службових розслідуваннях за фактами порушень правил поводження з ключовими документами (зокрема, у випадках компрометації чи підозрі на компрометацію особистих ключів).
- здійснює контроль за виконанням регламентних процедур з експлуатації та технічного обслуговування ІКС КНЕДП ТОВ "АТС";
- здійснює контроль за впровадженням та забезпеченням функціонування ІКС КНЕДП ТОВ "АТС";
- здійснює контроль за забезпеченням працездатності загальносистемного та спеціального програмного забезпечення ІКС КНЕДП ТОВ "АТС";
- приймає участь у забезпеченні актуалізації баз даних, створюваних та оброблюваних в ІКС КНЕДП ТОВ "АТС";
- здійснює розгляд та оцінка технічних рішень щодо модернізації ІКС КНЕДП ТОВ "АТС";
- приймає участь у розробці та узгодженні технічних завдань, проектної та експлуатаційної документації ІКС КНЕДП ТОВ "АТС";
- приймає участь у генерації головного ключа КНЕДП та зберігати резервні копії ключів КНЕДП та сервісів, у разі необхідності;
- організовує проведення попередніх випробувань, дослідної експлуатації та введення ІКС КНЕДП ТОВ "АТС" в експлуатацію.

Керівник КНЕДП ТОВ "АТС" представляє КНЕДП ТОВ "АТС" у випадках, передбачених Політикою сертифіката та Положеннями сертифікаційних практик ЦЗО, а також у межах повноважень, визначених довіреністю, виданою Надавачем.

5.3.1.1.2. Адміністратор реєстрації

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

Основними обов’язками адміністратора реєстрації є:

- ідентифікація та автентифікація користувачів;
- перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів;
- встановлення належності відкритого ключа та відповідного йому особистого ключа користувачу;
- ведення обліку користувачів.

Додатковими обов’язками адміністратора реєстрації є:

- надання допомоги під час генерації пари ключів користувача;
- надання консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг;
- участь в обробці запитів на формування та зміну статусу сертифікатів ключів користувачів..

До працівників відокремлених пунктів реєстрації КНЕДП ТОВ "АТС", на яких покладено обов’язки з реєстрації користувачів, повинні застосовуватись такі ж вимоги, як і до адміністраторів реєстрації.

Більш детально функціональні обов’язки викладені у Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

5.3.1.1.3. Адміністратор сертифікації

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

Основними обов'язками адміністратора сертифікації є:

- участь у генерації пар ключів КНЕДП ТОВ "АТС" та створенні резервних копій особистих ключів КНЕДП ТОВ "АТС";
- зберігання особистих ключів КНЕДП ТОВ "АТС" та їх резервних копій;
- забезпечення використання особистих ключів КНЕДП ТОВ "АТС" під час формування та обслуговування кваліфікованих сертифікатів КНЕДП ТОВ "АТС" та користувачів;
- перевірка заяв про формування кваліфікованих сертифікатів КНЕДП ТОВ "АТС" на відповідність вимогам цієї Політики сертифікації та відповідних Положень сертифікаційних практик;
- участь у знищенні особистих ключів КНЕДП ТОВ "АТС";
- забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів користувачів;
- забезпечення публікації кваліфікованих сертифікатів користувачів та списків відкликаних сертифікатів на веб-сайті КНЕДП ТОВ "АТС";
- створення резервних копій кваліфікованих сертифікатів користувачів;
- зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІКС КНЕДП ТОВ "АТС".

Додатковими обов'язками адміністратора сертифікації є:

- надання допомоги під час генерації пари ключів користувача;
- обробка запитів на формування та зміну статусу сертифікатів ключів користувачів;
- надання консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг;
- ведення архіву КНЕДП ТОВ "АТС".

Додатковими обов'язками адміністратора сертифікації є ведення журналів обліку адміністратора сертифікації, передбачених внутрішньою документацією ІКС КНЕДП ТОВ "АТС".

Більш детально функціональні обов'язки викладені у Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

5.3.1.1.4. Адміністратор безпеки

Адміністратор безпеки відповідає за належне функціонування ІКС КНЕДП ТОВ "АТС".

Основними обов'язками адміністратора безпеки є:

- участь у генерації пар ключів КНЕДП ТОВ "АТС" та створенні резервних копій особистих ключів КНЕДП ТОВ "АТС";
- контроль за формуванням, обслуговуванням, створенням та перевіркою резервних копій кваліфікованих сертифікатів КНЕДП ТОВ "АТС", користувачів та списків відкликаних сертифікатів;
- контроль за зберіганням особистих ключів КНЕДП ТОВ "АТС" та їх резервних копій, особистих ключів адміністраторів;
- участь у знищенні особистих ключів КНЕДП ТОВ "АТС", контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів ІКС КНЕДП ТОВ "АТС";
- забезпечення спостереження за функціонуванням ІКС КНЕДП ТОВ "АТС" (реєстрація подій в ІКС КНЕДП ТОВ "АТС", моніторинг подій тощо);

- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування ІКС КНЕДП ТОВ "АТС" після збоїв, відмов;

- ведення журналів обліку адміністратора безпеки, визначених документацією щодо ІКС КНЕДП ТОВ "АТС" або звітності, що передбачена вимогами чинного законодавства;

- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації КНЕДП ТОВ "АТС" та СУІБ;

- контроль за дотриманням персоналом КНЕДП ТОВ "АТС" положень внутрішньої організаційно-розпорядчої документації КНЕДП ТОВ "АТС" та документації СУІБ;

- контроль за веденням баз даних КНЕДП ТОВ "АТС".

Адміністратор безпеки відповідає за проведення перевірок дотримання персоналом КНЕДП ТОВ "АТС" та відокремленими пунктами реєстрації КНЕДП ТОВ "АТС" положень внутрішньої організаційно-розпорядчої документації КНЕДП ТОВ "АТС" та документації СУІБ. Забороняється суміщення посадових обов’язків адміністратора безпеки з іншими посадовими обов’язками, безпосередньо пов’язаними з наданням кваліфікованих електронних довірчих послуг.

Більш детально функціональні обов’язки викладені у Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

5.3.1.1.5. Системний адміністратор

Системний адміністратор відповідає за функціонування технічних засобів ІКС КНЕДП ТОВ "АТС".

Основними обов’язками системного адміністратора є:

- організація експлуатації та технічного обслуговування ІКС КНЕДП ТОВ "АТС" і адміністрування її технічних засобів;

- забезпечення функціонування веб-сайту КНЕДП ТОВ "АТС";

- участь у впровадженні та забезпеченні функціонування ІКС КНЕДП ТОВ "АТС" та СУІБ;

- ведення журналів аудиту подій, що реєструють технічні засоби ІКС КНЕДП ТОВ "АТС";

- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІКС КНЕДП ТОВ "АТС";

- встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІКС КНЕДП ТОВ "АТС";

- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІКС КНЕДП ТОВ "АТС", у зв’язку із збоями.

Більш детально функціональні обов’язки викладені у Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

5.3.1.1.6. Аудитор системи

Аудитор системи відповідає за належне функціонування ІКС КНЕДП ТОВ "АТС". Аудитор системи КНЕДП ТОВ "АТС" виконує ключові функції контролю, оцінки та вдосконалення ІКС відповідно до вимог нормативно-правових актів та стандартів інформаційної безпеки.

Основними обов’язками аудитора системи є:

- проведення перевірок журналів аудиту подій, що реєструють засоби та обладнання програмно-технічного комплексу (далі - технічні засоби) ІКС КНЕДП ТОВ "АТС";

- контроль за веденням архіву КНЕДП ТОВ "АТС";

- контроль відповідності ІКС вимогам нормативно-правових актів у сфері електронних довірчих послуг та стандартів інформаційної безпеки;

- проведення планових та позапланових аудитів функціонування ІКС КНЕДП ТОВ "АТС", аналіз ризиків та виявлення потенційних загроз;

- перевірка ефективності заходів безпеки та захисту інформації, що застосовуються в ІКС, а також надання рекомендацій щодо їх удосконалення;
- аналіз журналів подій та логів безпеки для виявлення інцидентів інформаційної безпеки та забезпечення оперативного реагування на них;
- оцінка надійності резервного копіювання та аварійного відновлення системи, перевірка відповідності цих процесів політикам безпеки;
- перевірка управління доступом до інформаційних ресурсів, контроль надання, зміни та відкликання прав доступу для користувачів та адміністраторів;
- аналіз та оцінка заходів криптографічного захисту, що застосовуються для збереження конфіденційності та цілісності даних;
- документування результатів аудитів та підготовка звітів з висновками щодо відповідності ІКС встановленим вимогам;
- проведення внутрішніх аудитів ІКС, перевірка відповідності процедур та політик вимогам безпеки СУІБ;
- участь у розробці та оновленні політик безпеки, а також моніторинг впровадження нових технічних рішень для підвищення рівня захисту ІКС.

5.3.2. Вимоги щодо кваліфікації, досвіду та допуску персоналу

Персонал КНЕДП ТОВ "АТС" повинен володіти необхідними знаннями, досвідом і кваліфікацією для належного надання кваліфікованих електронних довірчих послуг. Всі працівники зобов’язані дотримуватися вимог і положень, визначених у СУІБ.

Посади адміністратора сертифікації, адміністратора безпеки, системного адміністратора та аудитора системи можуть обіймати лише особи, які відповідають таким критеріям:

- Мають вищу освіту за спеціальністю у сфері інформаційних технологій, захисту інформації або кібербезпеки.
- Мають стаж роботи за фахом у зазначених сферах не менше трьох років.

5.3.3. Вимоги та процедури навчання персоналу

Керівник профільного підрозділу КНЕДП ТОВ "АТС" зобов’язаний забезпечити створення умов для безперервної особистої освіти та постійне підвищення кваліфікації персоналу КНЕДП ТОВ "АТС" у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних.

Персонал КНЕДП ТОВ "АТС" регулярно бере участь в семінарах, конференціях та зустрічах щодо надання кваліфікованих електронних довірчих послуг, інформаційних технологій, захисту інформації, кібербезпеки та захисту персональних даних. Проходження навчання повинно підтверджуватись дипломом, сертифікатом тощо.

5.3.4. Санкції за несанкціоновані дії персоналу

Персонал КНЕДП ТОВ "АТС" несе відповідальність за недотримання своїх посадових обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг, вимог організаційно-розпорядчої документації КНЕДП ТОВ «АТС», цього Регламенту, а також вимог щодо забезпечення інформаційної безпеки, конфіденційності та нерозголошення інформації.

За вказані порушення передбачаються дисциплінарні стягнення, цивільна, адміністративна та кримінальна відповідальність, відповідно до:

- Трудового договору;
- Цивільно-правових договорів, укладених з персоналом КНЕДП ТОВ "АТС" в межах правового режиму Дія Сіті;

- Договору на здійснення представництва КНЕДП ТОВ "АТС" (для відокремлених пунктів реєстрації КНЕДП ТОВ "АТС");
- Кодексу законів про працю України;
- Цивільного кодексу України;
- Кодексу України про адміністративні правопорушення;
- Кримінального кодексу України.

5.3.5. Контроль відокремлених пунктів реєстрації

До працівників відокремлених пунктів реєстрації КНЕДП ТОВ "АТС", на яких покладено обов’язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації.

До складу працівників відокремлених пунктів реєстрації КНЕДП ТОВ "АТС", входять працівники юридичних осіб та фізичні особи - підприємці, які на підставі договору з КНЕДП ТОВ "АТС" (ТОВ “АТС”) здійснюють реєстрацію користувачів.

На працівників відокремлених пунктів реєстрації КНЕДП ТОВ "АТС" покладено такі функціональні обов’язки:

- віддаленого адміністратора реєстрації;
- відповідального за захист інформації на відокремленому пункті реєстрації КНЕДП ТОВ "АТС";
- адміністратор виїздної реєстрації.

Віддалений адміністратор реєстрації відповідають за виконання функцій та несуть обов’язки адміністратора реєстрації, визначені у цій Політиці сертифіката.

У разі необхідності, з числа віддалених адміністраторів реєстрації на відокремленому пункті реєстрації КНЕДП ТОВ "АТС" призначаються відповідальні за захист інформації.

В межах виконання своїх обов'язків відповідальний за захист інформації на відокремленому пункті реєстрації КНЕДП ТОВ "АТС" відповідає за належну експлуатацію комплексу засобів захисту відокремленого пункту реєстрації КНЕДП ТОВ "АТС".

Основними обов'язками відповідального за захист інформації на відокремленому пункті реєстрації КНЕДП ТОВ "АТС" є:

- організація експлуатації та технічного обслуговування апаратних та програмних засобів відокремленого пункту реєстрації КНЕДП ТОВ "АТС";
- участь у впровадженні та забезпеченні функціонування ІКС КНЕДП ТОВ "АТС" відокремленого пункту реєстрації КНЕДП ТОВ "АТС";
- контроль за роботою програмного комплексу відокремленого пункту реєстрації КНЕДП ТОВ "АТС";
- контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації КНЕДП ТОВ "АТС";
- участь у створенні та введенні в експлуатацію ІКС КНЕДП ТОВ "АТС" відокремленого пункту реєстрації КНЕДП ТОВ "АТС".

Допускається виконання функцій відповідального за захист інформації на відокремленому пункті реєстрації КНЕДП ТОВ "АТС" системним адміністратором та адміністратором безпеки у частині, що не суперечить їхнім аналогічними функціями по відношенню до інших складових ІКС КНЕДП ТОВ "АТС".

Відповідальна особа на яку покладено обов'язки адміністратора реєстрації в частині ідентифікації та автентифікації Користувачів, відповідає за перевірку документів, наданих Користувачами, в т.ч. Заяви про формування кваліфікованого сертифіката відкритого ключа/Заяви про блокування/скасування/поновлення кваліфікованого сертифіката відкритого ключа.

Основними обов'язками Відповідальної особи є:

- проведення належної ідентифікації та верифікації Користувачів на підставі

ідентифікаційних документів про фізичну особу відповідно до законодавства та Регламенту Надавача;

- перевірка Заяви про формування кваліфікованого сертифікату відкритого ключа, яка одночасно є Заявою про приєднання до Договору приєднання;
- ознайомлення Користувачів з умовами обслуговування кваліфікованих сертифікатів відкритих ключів перед укладенням Договору приєднання.

5.3.6. Документація, яка надається персоналу

Організаційно-правовий статус персоналу КНЕДП ТОВ "АТС", їх завдання та функції, права та обов'язки, відповідальність, а також професійні знання, досвід і кваліфікація визначаються у посадових інструкціях.

Посадові інструкції повинні містити вимоги інформаційної безпеки та методи її забезпечення.

Керівник і персонал КНЕДП ТОВ "АТС" повинні бути ознайомлені з положеннями їх посадових інструкцій, діяти відповідно до своїх посадових завдань та функцій.

Персонал КНЕДП ТОВ "АТС" повинен бути повідомлений про зміни в організації процесів КНЕДП ТОВ "АТС", що стосуються їх посадових обов'язків.

5.4. Ведення журналу аудиту подій

Ведення журналу аудиту подій здійснюється відповідно до вимог, визначених в пункті 6.4.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

5.4.1. Типи записаних подій

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.4.2. Частота обробки журналу аудиту подій

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.4.3. Строки зберігання журналу аудиту подій

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.4.4. Захист журналу аудиту подій

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.4.5. Процедури резервного копіювання журналу аудиту подій

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.4.6. Синхронізація часу

Синхронізацію часу у технічних засобах ІКС КНЕДП ТОВ "АТС" на основному та резервному майданчику забезпечує комплекс засобів синхронізації часу з урахуванням документа ІКС КНЕДП ТОВ "АТС". Порядок синхронізації із всесвітнім координованим часом (UTC).

Комплекс засобів синхронізації часу забезпечує отримання сигналів синхронізації часу з серверів взаємодії ІКС КНЕДП ТОВ "АТС" (далі - NTP-серверів), резервних NTP-серверів,

синхронізованих з державним еталоном одиниць часу і частоти, серверів синхронізації часу КНЕДП ТОВ "АТС" та синхронізацію системного часу на технічних засобах ІКС КНЕДП ТОВ "АТС".

Сервери синхронізації часу КНЕДП ТОВ "АТС" отримують сигнали часу від резервних джерел синхронізації часу: зовнішніх NTP-серверів ЦЗО (czo.gov.ua, time.czo.gov.ua), ntp.metrology.kharkov.ua та kyivtime.org, що синхронізовані з Державним еталоном одиниць часу і частоти та передають синхронізовані дані до серверів взаємодії КНЕДП ТОВ "АТС".

Основним джерелом часу для ІКС КНЕДП ТОВ "АТС" є NTP-сервери.

Всі сервери, обладнання КЗІ та робочі станції працівників КНЕДП ТОВ "АТС" підключаються до NTP-сервера та синхронізують системний годинник відповідно до значення часу, що отримується від нього.

5.5. Архів документів

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4.6 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

5.5.1. Види документів та даних, що підлягають архівному зберіганню

Архівне зберігання інформації здійснюється відповідно до внутрішніх організаційно-розпорядчих документів КНЕДП ТОВ "АТС" та регламентованих процедур.

Обов’язковому архівуванню підлягають:

- Кваліфіковані сертифікати КНЕДП ТОВ "АТС" та користувачів. Зберігаються в електронній формі. Резервне копіювання відбувається в автоматичному режимі засобами ІКС Надавача та ручне архівне копіювання відбувається на окремі носії інформації.
- Списки відкликаних сертифікатів (CRL), що містять інформацію про анульовані сертифікати. Зберігаються в електронній формі. Резервне копіювання відбувається в автоматичному режимі засобами ІКС Надавача та ручне архівне копіювання відбувається на окремі носії інформації.
- Журнали аудиту подій, що містять записи про дії в системі для забезпечення прозорості та безпеки. Зберігаються в електронній формі. Резервне копіювання відбувається в автоматичному режимі засобами ІКС Надавача та на окремі носії інформації відбувається в ручному режимі.
- Журнали самого Надавача. Можуть зберігатись як в електронній так і в паперовій формі. Електронна форма зберігається в ІКС Надавача. Паперова форма має знаходитись у приміщенні Надавача в окремому сховищі(сейфі). Резервне копіювання електронних журналів відбувається на окремі носії інформації в ручному режимі.
- Укладені договори про надання електронних довірчих послуг. Зберігаються в електронній формі. Резервне копіювання відбувається в автоматичному режимі засобами ІКС Надавача та на окремі носії інформації відбувається в ручному режимі.
- Документована інформація в електронному вигляді, включаючи заяви на формування, блокування, поновлення та скасування сертифікатів користувачів, на підставі якої їм надавалися електронні довірчі послуги. Зберігаються в електронній формі. Резервне копіювання відбувається в автоматичному режимі засобами ІКС Надавача та архівне копіювання на окремі носії інформації відбувається в ручному режимі.

Архівне зберігання забезпечує збереження цілісності та доступності даних, необхідних для аудиту, розслідування інцидентів та підтвердження законності наданих послуг.

5.5.2. Строки зберігання архіву

Документи у паперовій та електронній формах підлягають зберіганню відповідно до законодавства у сфері архівної справи та електронних довірчих послуг.

Сертифікати КНЕДП ТОВ "АТС", серверів, адміністраторів, користувачів, а також списки відкликаних сертифікатів (CRL) зберігаються безстроково, забезпечуючи їхню доступність для перевірки та аудиту.

5.5.3. Захист архіву

КНЕДП ТОВ "АТС" забезпечує надійний захист архіву відповідно до внутрішніх організаційно-розпорядчих документів та вимог законодавства у сфері архівної справи. Це гарантує збереження, цілісність та конфіденційність архівних даних, а також їх доступність для перевірки та аудиту.

Для зберігання носіїв із резервними та архівними копіями виділяється окреме сховище (сейф чи відсік сейфа) з двома екземплярами ключів і пристроями для опечатування. Один екземпляр ключа від сховища знаходиться в адміністратора безпеки, другий в опечатаному вигляді зберігається у сховищі (сейфі) керівника профільного підрозділу КНЕДП ТОВ "АТС".

5.5.4. Процедури резервного копіювання архіву

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.5.5. Вимога щодо накладання електронних позначок часу на записи

КНЕДП ТОВ "АТС" може накладати електронні позначки часу на записи, пов’язані з його діяльністю.

5.5.6. Система збирання архівів (внутрішня чи зовнішня)

Системи збору архівів знаходяться в приміщеннях КНЕДП ТОВ "АТС".

Вимоги до приміщення описані в пункті 5.1.2. цієї Політики сертифіката.

5.5.7. Процедури отримання та перевірки архівної інформації

Доступ до архівних даних суворо обмежений. Доступ до цієї системи мають лише уповноважені працівники згідно із службовими повноваженнями. КНЕДП ТОВ "АТС" оприлюднює інформацію з архіву лише за рішенням суду.

5.6. Зміна ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.7. Компрометація і аварійне відновлення

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4.8 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2 .

5.7.1. Процедури обробки інцидентів і компрометації

ТОВ "АТС" має План відновлення після аварійних ситуацій відповідно до вимог СУІБ організації.

Порядок дій та реагування персоналом КНЕДП ТОВ "АТС" на інциденти визначається Процедурою управління інцидентами ТОВ “АТС” та Планом безперервності бізнесу відповідно до вимог СУІБ.

Процедури з управління інцидентами повинні передбачати:

- виконання заходів, визначених Порядком координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10 червня 2008 р. № 94, зареєстрованим в Міністерстві юстиції України 7 липня 2008 р. за № 603/15294;

- інформування КО про порушення вимог з безпеки та захисту інформації, визначені в абзаці дванадцятому частини четвертої статті 13 Закону України "Про електронну ідентифікацію та електронні довірчі послуги", протягом 24 годин після виявлення порушення;

- інформування користувачів, яким надаються послуги, про порушення безпеки, які спричиняють на них негативний вплив, протягом двох годин після виявлення порушення.

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

Визначається наступними документами СУІБ - Планом відновлення після аварійних ситуацій.

5.7.3. Процедури відновлення після компрометації ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

5.7.4. Можливості безперервності бізнесу після катастрофи

КНЕДП ТОВ "АТС" має резервний майданчик аналогічний основному майданчику для забезпечення безперебійності роботи у випадку аварій або катастроф відповідно до Плану безперервності бізнесу ТОВ “АТС”.

У разі аварійної ситуації, катастрофи або виходу з ладу основного майданчика, КНЕДП ТОВ "АТС" негайно відновлює роботу з резервного майданчика, забезпечуючи безперервність надання кваліфікованих електронних довірчих послуг.

Резервні копії критично важливих даних, включаючи особисті ключі, конфігураційні дані та іншу інформацію, необхідну для відновлення роботи ІКС, постійно актуалізуються та надійно захищені відповідно до вимог інформаційної безпеки та політик ТОВ “АТС”.

5.8. Припинення діяльності Надавача

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4.9 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2. Припинення діяльності КНЕДП ТОВ "АТС" проводиться відповідно до затвердженого Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" (далі - План припинення діяльності) з урахуванням вимог Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (зі змінами та доповненнями).

5.8.1. Підстави припинення діяльності Надавача

КНЕДП ТОВ "АТС" припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг у разі:

1) прийняття ЦЗО рішення про скасування статусу кваліфікованого надавача;

2) прийняття КНЕДП ТОВ "АТС" рішення про припинення надання кваліфікованих електронних довірчих послуг, що зазначені у Довірчому списку;

3) припинення діяльності КНЕДП ТОВ "АТС" (припинення юридичної особи), крім випадків правонаступництва, визначених 5.8.4 цієї Політики сертифіката;

4) набрання законної сили рішенням суду про скасування статусу кваліфікованого надавача, визнання КНЕДП ТОВ "АТС" банкрутом.

Про рішення щодо припинення надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" зобов’язаний повідомити користувачів, ЦЗО та КО не пізніше п’яти робочих днів з дати прийняття такого рішення.

ЦЗО зобов’язаний оприлюднити інформацію про своє рішення щодо припинення діяльності КНЕДП ТОВ "АТС" з надання кваліфікованих електронних довірчих послуг, у тому числі у зв’язку з анулюванням статусу кваліфікованого надавача електронних довірчих послуг, не пізніше наступного робочого дня після прийняття такого рішення шляхом:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;

- надіслати до КНЕДП ТОВ "АТС" повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО зобов’язаний оприлюднити на своєму офіційному веб-сайті повідомлення про припинення надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" не пізніше наступного робочого дня з дати отримання повідомлення про виникнення підстав для примусового припинення діяльності.

Повідомлення ЦЗО про припинення надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" повинно містити дату публікації.

КНЕДП ТОВ "АТС" припиняє діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дати оприлюднення ЦЗО на своєму офіційному веб-сайті повідомлення про припинення надання КНЕДП ТОВ "АТС" кваліфікованих електронних довірчих послуг.

З дати оприлюднення ЦЗО на своєму офіційному веб-сайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" та до дати припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

КНЕДП ТОВ "АТС", припиняючи діяльність з надання кваліфікованих електронних довірчих послуг, передає іншому надавачу обслуговування користувачів, з якими ним було укладено договори про надання кваліфікованих електронних довірчих послуг.

У разі відмови користувача від продовження отримання послуг за договором про надання кваліфікованих електронних довірчих послуг, укладеним з КНЕДП ТОВ "АТС" (ТОВ "АТС"), з іншим надавачем до закінчення терміну дії відповідного договору, КНЕДП ТОВ "АТС" зобов’язаний повернути кошти такому користувачеві за послуги, які не можуть бути надані в майбутньому, якщо вони були попередньо оплачені користувачем.

Якщо користувач дав згоду на продовження надання послуг за договором про надання кваліфікованих електронних довірчих послуг, укладеним з КНЕДП ТОВ "АТС" (ТОВ "АТС") з іншим надавачем до закінчення терміну дії відповідного договору, КНЕДП ТОВ "АТС" зобов’язаний оплатити подальше надання кваліфікованих електронних довірчих послуг такому користувачеві за тарифами, встановленими відповідним надавачем.

ЦЗО у день, визначений як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС", вносить відповідні зміни до Довірчого списку.

У разі припинення надання кваліфікованих довірчих послуг КНЕДП ТОВ "АТС" зобов’язаний передати іншому надавачу або ЦЗО документовану інформацію (документи, на підставі яких користувачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати відкритих ключів, усі сформовані кваліфіковані сертифікати відкритих ключів, а також реєстри сформованих кваліфікованих сертифікатів відкритих ключів).

Передача документованої інформації буде здійснена КНЕДП ТОВ "АТС" не пізніше дати, визначеної ним як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або дати набрання законної сили відповідним рішенням суду.

ЦЗО скасовує виданий ним кваліфікований сертифікат КНЕДП ТОВ "АТС" в день, визначений КНЕДП ТОВ "АТС" як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або в день набрання законної сили рішенням відповідного суду.

5.8.2. Повідомлення про припинення діяльності Надавача

Про прийняте рішення про припинення надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" зобов'язаний повідомити користувачам, ЦЗО та КО не пізніше п'яти робочих днів з дня прийняття такого рішення.

ЦЗО зобов'язаний оприлюднити інформацію про рішення ЦЗО щодо припинення КНЕДП ТОВ "АТС" діяльності з надання кваліфікованих електронних довірчих послуг, в тому числі у зв'язку із скасуванням статусу кваліфікованого надавача електронних довірчих послуг, не пізніше наступного робочого дня після прийняття такого рішення шляхом:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;
- надіслання до КНЕДП ТОВ "АТС" повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО зобов'язаний опублікувати на своєму офіційному веб-сайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" не пізніше наступного робочого дня з дня одержання повідомлення про настання підстав, передбачених підпунктами 2 - 4 пункту 5.8.1 цієї Політики сертифіката.

Повідомлення ЦЗО про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" повинно містити дату опублікування.

5.8.3. Дата припинення діяльності Надавача

КНЕДП ТОВ "АТС" припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дня опублікування на своєму офіційному веб-сайті ЦЗО повідомлення про припинення надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" .

З дня опублікування на своєму офіційному веб-сайті ЦЗО повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

З дня опублікування на своєму офіційному веб-сайті ЦЗО повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

ЦЗО у день, визначений як дата припинення діяльності КНЕДП ТОВ "АТС" з надання кваліфікованих електронних довірчих послуг, вносить відповідні зміни до Довірчого списку.

5.8.4. Правонаступництво

З метою забезпечення безперервного надання кваліфікованих електронних довірчих послуг їх користувачам ЦЗО може прийняти рішення про внесення змін до Довірчого списку щодо заміни кваліфікованого надавача електронних довірчих послуг шляхом заміни відомостей про КНЕДП ТОВ "АТС" відомостями про іншого кваліфікованого надавача електронних довірчих послуг, якщо передача відповідних прав та обов'язків здійснюється за

спільною згодою таких надавачів, за договором або з інших підстав для правонаступництва, визначених законодавством.

У разі відмови користувача продовжити обслуговування за договором про надання кваліфікованих електронних довірчих послуг, укладеним з КНЕДП ТОВ "АТС" (ТОВ "АТС"), що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, в іншого кваліфікованого надавача електронних довірчих послуг до закінчення строку дії відповідного договору КНЕДП ТОВ "АТС" зобов'язаний повернути такому користувачу кошти за послуги, які не можуть надаватися в подальшому, якщо вони були попередньо оплачені користувачем.

Якщо користувач погодився продовжити обслуговування за договором про надання кваліфікованих електронних довірчих послуг, укладеним з КНЕДП ТОВ "АТС" (ТОВ "АТС"), що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, в іншого кваліфікованого надавача електронних довірчих послуг до закінчення строку дії відповідного договору, КНЕДП ТОВ "АТС" зобов'язаний оплатити подальше надання кваліфікованих електронних довірчих послуг такому користувачу за тарифами, встановленими відповідним кваліфікованим надавачем електронних довірчих послуг.

5.8.5. Передача документованої інформації

КНЕДП ТОВ "АТС" у разі припинення діяльності з надання кваліфікованих електронних довірчих послуг, зобов'язаний передати до іншого кваліфікованого надавача електронних довірчих послуг, який виявив намір продовжити обслуговування користувачів до закінчення строку дії відповідних договорів про надання кваліфікованих електронних довірчих послуг, або до ЦЗО документи, на підставі яких користувачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати, усі сформовані кваліфіковані сертифікати, а також реєстри сформованих кваліфікованих сертифікатів.

Передача документованої інформації здійснюється відповідно до:

- Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 23 липня 2024 р. № 842;

- Порядку зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 10 грудня 2024 р. № 1408;

- підпунктів 6.3.4-10A та 6.3.4-11A ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

5.8.6. План припинення діяльності

КНЕДП ТОВ "АТС" має затверджений План припинення діяльності.

План припинення діяльності визначає умови, яких повинен дотримуватися КНЕДП ТОВ "АТС" з метою недопущення негативних наслідків у разі припинення ним діяльності з надання кваліфікованих електронних довірчих послуг, а також забезпечення стабільності та довговічності кваліфікованих електронних довірчих послуг.

КНЕДП ТОВ "АТС" затверджує План припинення діяльності та за необхідності вносить до нього зміни з метою актуалізації інформації, що в ньому міститься.

ЦЗО погоджує План припинення діяльності та зміни до нього в установленому законодавством порядку.

У Плані припинення діяльності визначаються:

- порядок повідомлення користувачів, центрального засвідчувального органу, персоналу КНЕДП ТОВ "АТС", відокремлених пунктів реєстрації та представників, суб'єктів, які довіряють КНЕДП ТОВ "АТС" та контрагентів про припинення діяльності з надання кваліфікованих електронних довірчих послуг;

- домовленості та угоди з третіми сторонами для продовження виконання зобов'язань у разі припинення КНЕДП ТОВ "АТС" діяльності з надання кваліфікованих електронних довірчих послуг (передача обслуговування користувачів до іншого кваліфікованого надавача).

План припинення діяльності є конфіденційним і перевіреним ООВ.

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, ДСТУ ETSI EN 319 411-2 та відповідними документами СУІБ ТОВ "АТС".

Крім того, застосовуються такі особливі вимоги:

6.1. Генерація та встановлення пари ключів

6.1.1. Генерація пари ключів

6.1.1.1. Генерація пари ключів Надавача

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.1.1.2. Генерація пари ключів користувача

Під час надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток КНЕДП ТОВ "АТС" забезпечується:

- використання користувачем виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката;

- захист обміну інформацією між користувачем та КНЕДП ТОВ "АТС" засобами електронних комунікаційних мереж загального користування;

- створення умов для генерації пари ключів користувача;

- допомога під час генерації пари ключів користувача 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 користувача;

- зберігання особистого ключа користувача;

- захист від доступу сторонніх осіб до параметрів особистого ключа користувача під час використання засобу кваліфікованого електронного підпису чи печатки.

Особистий ключ у складі пари ключів користувача може бути згенерований:

- на стаціонарному робочому місці користувача або на власному портативному обчислювальному пристрої;

- на робочій станції генерації ключів в офісах КНЕДП ТОВ "АТС" та відокремлених пунктів реєстрації КНЕДП ТОВ "АТС";

- за допомогою кабінету користувача (веб-сервіс Надавача)

У разі коли пара ключів була згенерована користувачем поза приміщенням КНЕДП ТОВ "АТС" та/або за відсутності відповідного персоналу, ідентифікація такого користувача, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката здійснюється КНЕДП ТОВ "АТС" після перевірки факту володіння користувачем особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката.

Генерацію та/або управління парою ключів від імені користувача може здійснювати виключно КНЕДП ТОВ "АТС". Під час управління парою ключів користувача, може здійснювати резервне копіювання особистого ключа користувача з метою його зберігання за умови дотримання таких вимог:

- рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;

- кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

Для генерації особистих ключів використовуються засоби кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів (захищені носії особистих ключів, токени, SIM-картки, мережні криптомодулі), які можуть функціонувати під управлінням або з використанням окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків та які перебувають у власності користувачів, або надаються КНЕДП ТОВ "АТС".

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

Для надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" використовуються засоби кваліфікованого електронного підпису чи печатки, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

Надання КНЕДП ТОВ "АТС" засобів кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів та їх технічна підтримка і обслуговування здійснюється на договірних засадах.

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

6.1.2. Доставка особистого ключа користувачу

Отримання користувачем особистого ключа у володіння в результаті надання КНЕДП ТОВ "АТС" кваліфікованої електронної довірчої послуги здійснюється за таких умов:

- отримання та використання особистого ключа на правах повного володіння засобом кваліфікованого електронного підпису чи печатки, у тому числі, носієм особистого ключа;

- отримання та використання особистого ключа на правах повного володіння або доступу на договірних засадах до частини ресурсу засобу кваліфікованого електронного підпису чи печатки, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережний криптомодуль).

Фактичне отримання користувачем особистого ключа відбувається у момент генерації особистого ключа особисто або у момент зміни атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа) у випадку, коли ключові пари були попередньо створено КНЕДП ТОВ "АТС". Не допускається формування КНЕДП ТОВ "АТС" кваліфікованих сертифікатів до моменту фактичного отримання особистого ключа користувачем.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

6.1.3. Доставка відкритого ключа користувачу

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

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

6.1.4. Доставка відкритого ключа надавача суб'єктам, які довіряють Надавачу

Кваліфіковані сертифікати КНЕДП ТОВ "АТС" та центрального засвідчувального органу публікуються на веб-сайті КНЕДП ТОВ "АТС".

Контейнер ланцюжків сертифікатів, доступний для завантаження суб'єктами, які довіряють КНЕДП ТОВ "АТС", розміщений на веб-сайті КНЕДП ТОВ "АТС".

Актуальний кваліфікований сертифікат КНЕДП ТОВ "АТС" доступний для перегляду та завантаження на офіційному веб-сайті Центрального засвідчувального органу (ЦЗО) .

6.1.5. Розміри (параметри) ключів

В ІКС КНЕДП ТОВ "АТС" використовуються особисті та відповідні їм відкриті ключі з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);

- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

6.1.6. Генерація параметрів відкритого ключа

Під час генерації відкритого ключа використовується апаратна генерація ключів генератор випадкових чисел (ГВЧ), що включає в себе статистичну перевірку виходу генератора. Статистична перевірка випадкових бітових послідовностей з апаратного ГВЧ здійснюється відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами. Ключі генеруються та зберігаються в апаратному мережному криптомодулі "Гряда-301".

6.1.7. Основні цілі використання особистого ключа надавачем

Особисті ключі КНЕДП ТОВ "АТС" забезпечують функціонування ІКС КНЕДП ТОВ "АТС".

КНЕДП ТОВ "АТС" визначає практику використання ключів КНЕДП ТОВ "АТС" для підпису сертифікатів користувачів, сертифікатів серверів OCSP, СМР КНЕДП ТОВ "АТС", списку відкликаних сертифікатів (CRL).

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

6.2.1. Стандарти та елементи керування криптографічним модулем

Для зберігання особистих ключів користувачів КНЕДП ТОВ "АТС" використовує ЗКЕП, що мають документально підтверджену відповідність вимогам статей 18 і 19 Закону України "Про електронну ідентифікацію та електронні довірчі послуги", отриману за результатами сертифікації таких засобів.

Крім того, можливе зберігання особистих ключів на флеш-носіях у вигляді файлів у форматах *.dat та *.pfx, відповідно до вимог безпеки та політик КНЕДП.

Для зберігання особистих ключів КНЕДП ТОВ "АТС" та серверів ІКС КНЕДП ТОВ "АТС" використовуються мережні криптомодулі, що виконані у вигляді окремих апаратних пристроїв. Криптомодулі повинні мати документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

6.2.2. Особистий ключ (n з m) керування кількома особами

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.3. Управління особистим ключем підписувача

КНЕДП ТОВ "АТС" забезпечує зберігання та захист особистих ключів користувачів, згенерованих в мережних криптомодулях "Гряда-301", які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів, які розміщені у серверних шафах в приміщеннях ЦОД, доступ до яких мають тільки відповідальні особи КНЕДП ТОВ "АТС".

КНЕДП ТОВ "АТС" забезпечує зберігання та захист особистих ключів користувачів згенерованих в мережних криптомодулях, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів, на віддалених пунктах реєстрації та представництв за договором, укладеними з ними, які здійснюють реєстрацію користувачів, доступ до яких мають тільки відповідальні особи на відповідному пункті реєстрації.

6.2.4. Резервне копіювання особистого ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.5. Архівація особистого ключа

Особисті ключі КНЕДП ТОВ "АТС" та користувачів архівуються відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами до ІКС КНЕДП ТОВ "АТС".

Після скасування або завершення строку дії кваліфікованих сертифікатів користувачів особистий ключ користувача, що зберігається в мережному криптомодулі "Гряда-301" (високопродуктивний пристрій) КНЕДП ТОВ "АТС", автоматично знищується.

Також видалення особистих ключів, термін дії сертифікатів яких закінчився або які були скасовані, може здійснюватися на регулярній основі в межах проведення аудитів, перевірок та контрольних заходів, відповідно до вимог політик інформаційної безпеки та внутрішніх регламентів КНЕДП.

Цей абзац розділу не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.6. Відновлення особистого ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.7. Зберігання особистого ключа в криптографічному модулі

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.8. Активація особистих ключів

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.9. Деактивація особистих ключів

Процедура деактивації особистих ключів КНЕДП ТОВ "АТС" шляхом їх знищення визначена в пункті 6.2.10 цієї Політики сертифіката.

6.2.10. Знищення особистих ключів

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.2.11. Можливості мережного криптографічного модуля

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.3. Інші аспекти керування парами ключів

6.3.1. Архівація відкритого ключа

Відкриті ключі, на основі яких сформовано кваліфіковані сертифікати зберігаються в базі даних КНЕДП ТОВ "АТС" постійно.

6.3.2. Строки дії сертифіката та строки використання пари ключів

Строки дії особистих ключів КНЕДП ТОВ "АТС" відповідають строкам чинності кваліфікованих сертифікатів відповідних їм відкритих ключів і становлять:

- для особистих ключів КНЕДП ТОВ "АТС" та його серверів (OCSP, CMP, TSP) - не більше 5 років;

- для особистих ключів адміністраторів та користувачів - не більше 2 років.

6.4. Дані активації

6.4.1. Створення та встановлення даних активації

Відповідно до пункту 3.2 цієї Політики сертифіката.

6.4.2. Захист даних активації

Особисті ключі, що зберігаються на кваліфікованих засобах електронного підпису (ЗКЕП), повинні бути захищені одним або кількома з таких способів:

- паролем, що складається не менше ніж з 8 символів, які містять великі та малі латинські літери, цифри та символи.;
- PIN-кодом (вводитися безпосередньо на пристрої або у захищеному інтерфейсі, що виключає можливість перехоплення даних.);
- біометричною автентифікацією (Face ID, Touch ID, відбиток пальця, розпізнавання обличчя тощо);
- одноразовим паролем (OTP);
- апаратним токеном або ключем безпеки (U2F, FIDO2);
- мультифакторною автентифікацією (поєднання декількох методів);
- Інші методи автентифікації

Користувач має право самостійно обрати спосіб захисту особистого ключа із підтримуваних його засобом ЗКЕП, за умови дотримання вимог безпеки, установлених Надавачем.

6.4.3. Інші аспекти даних активації

Жодних додаткових умов не встановлюється.

6.5. Контроль комп'ютерної безпеки

6.5.1. Спеціальні технічні вимоги до комп’ютерної безпеки

КНЕДП ТОВ "АТС" забезпечує захист інформаційних ресурсів від зовнішніх загроз, кібератак та несанкціонованого витоку інформації шляхом впровадження та підтримки безпечних інформаційних технологій.

Одним із ключових заходів є застосування багатофакторної автентифікації, що підвищує рівень контролю доступу до критичних даних. Доступ до інформації різних категорій організований таким чином, що лише уповноважені користувачі або процеси можуть взаємодіяти з певною інформацією.

Реалізовано механізми обмеження доступу та гарантування цілісності даних під час їхньої обробки як в електронному вигляді, так і у формі друкованих документів або даних на змінних носіях інформації.

Безпекові заходи здійснюються відповідно до вимог Політики контролю доступу ТОВ “АТС”, що визначає правила та регламенти забезпечення захисту інформаційних активів організації.

КНЕДП ТОВ "АТС" забезпечує:

- конфіденційність та цілісність інформації, яка зберігається, обробляється та передається між компонентами інформаційно-комунікаційної системи (ІКС) КНЕДП ТОВ "АТС".
- захист особистих ключів користувачів та компонентів КНЕДП ТОВ "АТС" від несанкціонованого доступу та компрометації.
- конфіденційність технологічної інформації, що забезпечує функціонування ІКС КНЕДП, включаючи криптографічні алгоритми та внутрішні механізми безпеки.
- контрольований доступ до інформації та ресурсів ІКС відповідно до Політики контролю доступу ТОВ “АТС”, що визначає рівні доступу для користувачів.
- спостереженість за діями користувачів через механізми контролю, реєстрації активностей та проведення аудиту зареєстрованих подій, що дозволяє своєчасно виявляти та реагувати на потенційні загрози безпеці.

Ці заходи гарантують високий рівень інформаційної безпеки, відповідність законодавчим вимогам та збереження довіри користувачів до послуг КНЕДП ТОВ "АТС".

6.5.2. Рейтинг комп'ютерної безпеки

Надавач забезпечує рівень комп’ютерної безпеки, що відповідає вимогам чинних національних і міжнародних стандартів у сфері захисту інформації.

Система технічного та організаційного захисту КНЕДП ТОВ «АТС» підтримує рівень безпеки, достатній для запобігання несанкціонованому доступу, втраті, зміні або розголошенню даних, які обробляються під час надання електронних довірчих послуг.

Рівень комп’ютерної безпеки визначається, підтримується та періодично оцінюється за результатами внутрішніх аудитів, зовнішніх перевірок відповідності та оцінювання ризиків відповідно до політик інформаційної безпеки та стандартів ETSI EN 319 401, ETSI EN 319 411-1, ISO/IEC 27001.

Рейтинг комп’ютерної безпеки встановлюється за результатами оцінки відповідності та може коригуватися відповідно до змін рівнів загроз і ризиків.

6.6. Контроль безпеки життєвого циклу

6.6.1. Контроль розробки системи

При розробці та впровадженні ІКС КНЕДП ТОВ "АТС" повинні бути враховані сучасні тенденції у сфері захищених інформаційних технологій, актуальні розробки засобів захисту інформації, а також вимоги нормативної бази з технічного захисту інформації.

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІКС КНЕДП ТОВ "АТС" повинна передбачати застосування наступних заходів та засобів захисту інформації:

− організаційно-правові заходи, які реалізуються поза ІКС КНЕДП ТОВ "АТС";

− інженерно-технічні заходи, що реалізуються поза ІКС КНЕДП ТОВ "АТС";

– апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється і зберігається в КНЕДП ТОВ "АТС".

Розробка програмного забезпечення із захисту інформації та оновлення його компонентів отримується безпосередньо від розробника. Допускається завантаження з офіційних веб-сайтів розробника.

Апаратне забезпечення комплексу засобів захисту КНЕДП ТОВ "АТС" отримує безпосередньо від розробника, або від організацій, що мають відповідні ліцензії на впровадження комплексу засобів захисту комплексу технічних рішень.

6.6.2. Засоби керування безпекою

Контроль за дотриманням вимог з безпеки в ІКС КНЕДП ТОВ "АТС" здійснюється відповідальним за захист інформації КНЕДП ТОВ "АТС", на якого покладається забезпечення захисту інформації в ІКС.

Підтримка функціонування та обслуговування системи здійснюється адміністраторами згідно їх посадових обов’язків та положень Політики інформаційної безпеки ТОВ “АТС”.

Моніторинг інформації про стан функціонування ІКС КНЕДП ТОВ "АТС", такої як відомості про використання апаратних ресурсів, збої, відмови та проблеми у роботі програмного забезпечення, сервісів здійснюється в автоматичному режимі. Адміністратори КНЕДП ТОВ "АТС" отримують від системи моніторингу повідомлення у разі виникнення/усунення позаштатної ситуації.

6.6.3. Контроль безпеки протягом життєвого циклу

КНЕДП ТОВ "АТС" гарантує, що обладнання та робочі станції адміністраторів ІКС КНЕДП ТОВ "АТС" мають останні оновлення безпеки.

6.7. Контроль безпеки мережі

Цей розділ не входить до обсягу положень, визначених КНЕДП ТОВ "АТС" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП ТОВ "АТС".

6.8. Електронні позначки часу

6.8.1. Формування кваліфікованої електронної позначки часу

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

- формування кваліфікованої електронної позначки часу;
- передачу кваліфікованої електронної позначки часу користувачеві електронної довірчої послуги.

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.

Кваліфікована електронна позначка часу повинна відповідати таким вимогам:

- пов'язувати дату і час з електронними даними в такий спосіб, що обґрунтовано виключає можливість зміни електронних даних, яка не може бути виявлена;
- базуватися на джерелі точного часу, синхронізованому із Всесвітнім координованим часом (UTC) з точністю до секунди;
- до кваліфікованої електронної позначки часу додається створений для неї удосконалений електронний підпис чи удосконалена електронна печатка КНЕДП ТОВ "АТС" або може застосовувати інший метод, рівнозначний додаванню до кваліфікованої

електронної позначки часу удосконаленого електронного підпису чи удосконаленої електронної печатки, за умови що він забезпечує рівнозначний рівень безпеки кваліфікованої електронної позначки часу та відповідає вимогам Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

Формування кваліфікованої електронної позначки часу здійснюється КНЕДП ТОВ "АТС" за запитом користувача.

Під час формування кваліфікованої електронної позначки часу користувач та КНЕДП ТОВ "АТС" за допомогою ЗКЕП вчиняють такі дії:

1) користувач обчислює геш-значення електронних даних, на які необхідно сформувати кваліфіковану електронну позначку часу;

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

- обчислене геш-значення;
- об’єктний ідентифікатор (OID) політики формування позначки часу (необов’язково);
- ідентифікатор алгоритму гешування, що використовувався;
- унікальний ідентифікатор запиту (необов’язково);
- необов’язкові розширення;

3) користувач передає сформований запит до КНЕДП ТОВ "АТС";

4) КНЕДП ТОВ "АТС" перевіряє правильність формату запиту та здійснює його обробку, формує кваліфіковану електронну позначку часу та відповідь, що містить кваліфіковану електронну позначку часу, чи відповідь з інформацією про відмову у формуванні кваліфікованої електронної позначки часу;

5) КНЕДП ТОВ "АТС" надсилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, в якій зазначені такі дані:

- об’єктний ідентифікатор (OID) 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 чи печатку КНЕДП ТОВ "АТС", накладені на кваліфіковану електронну позначку часу;

6) користувач після отримання відповіді від КНЕДП ТОВ "АТС" вчиняє такі дії:

- перевіряє результат обробки запиту;
- перевіряє відповідність імені чи найменування суб’єкта, що наклав кваліфікований електронний підпис чи печатку на кваліфіковану електронну позначку часу, найменуванню КНЕДП ТОВ "АТС";
- перевіряє відповідність призначення сертифіката КНЕДП ТОВ "АТС" (для формування позначки часу);
- перевіряє чинність сертифіката КНЕДП ТОВ "АТС";
- перевіряє кваліфікований електронний підпис чи 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.

6.8.2. Перевірка кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу повинна забезпечувати:

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

Перевірка кваліфікованої електронної позначки часу може проводитися 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 такі дії:
- отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити КНЕДП ТОВ "АТС";
- перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) сертифіката КНЕДП ТОВ "АТС";
- 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).

6.8.3. Недійсність кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу вважається недійсною у разі:

- недотримання вимоги щодо точності часу в програмно-технічному комплексі КНЕДП ТОВ "АТС";

- використання скасованого або блокованого сертифіката КНЕДП ТОВ "АТС" на момент формування кваліфікованої електронної позначки часу.

Правильність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в засобі кваліфікованого електронного підпису чи печатки (QSCD) забезпечує протокол фіксування часу.

6.8.4. Отримання кваліфікованої електронної позначки часу надавачем

КНЕДП ТОВ "АТС" отримує кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження кваліфікованої електронної позначки часу від ЦЗО.

Механізм синхронізації часу із Всесвітнім координованим часом (UTC) в програмнотехнічному комплексі КНЕДП ТОВ "АТС" та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із Всесвітнім координованим часом (UTC).

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) розробляється КНЕДП ТОВ "АТС" та погоджується з ЦЗО.

7. ПРОФІЛІ СЕРТИФІКАТІВ, СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ (CRL) ТА ПРОТОКОЛУ 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 та ДСТУ ETSI EN 319 411-2.

7.1. Профілі сертифікатів

Кваліфіковані сертифікати, що формуються КНЕДП ТОВ "АТС" відповідають вимогам таких стандартів:

- ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів” (далі - ISO/IEC 9594-8:2020).

- ДСТУ ETSI EN 319 412-1 (ETSI EN 319 412-1 V1.4.4, IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних” (далі - ДСТУ ETSI EN 319 412-1).

- ДСТУ ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) “Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам” (далі - ETSI EN 319 412-2).

- ДСТУ ETSI EN 319 412-3 (ETSI EN 319 412-3, IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профілі сертифікатів, виданих юридичним особам”.

- ДСТУ ETSI EN 319 412-5 (ETSI EN 319 412-5, IDT) “Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 5. Кваліфіковані сертифікати”.

- ДСТУ ETSI TS 119 312 (ETSI TS 119 312, IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні набори”.

- ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», (далі - ДСТУ 4145-2002). З функцією гешування за ГОСТ 34.311-95 96 ‘ «Информационная технология. Криптографическая защита информации. Функция хэширования» або за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування».

Типи кваліфікованих сертифікатів, що формує Надавач, зазначені у п. 1.4.1.1 данної Політики:

№	Ідентифікатор	Політика	Власник	Використання		
				Кваліфікований	Удосконалений	Шифрування
1	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					
	0.4.0.194112.1.2	QCP-n-qscd	Фізична особа	так	ні	ні
2	кваліфікований сертифікат електронного підпису, що пов'язує відкритий ключ удосконаленого електронного підпису з фізичною особою та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження удосконаленого електронного підпису					
	0.4.0.194112.1.0	QCP-n	Фізична особа	ні	так	ні
3	кваліфікований сертифікат електронного підпису, що пов'язує відкритий ключ кваліфікованої електронного підпису пов’язаного з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованого електронного підпису					
	0.4.0.194112.1.2	QCP-n-qscd	Представник юр. особи	так	ні	ні

4	кваліфікований сертифікат електронного підпису, що пов'язує відкритий ключ удосконаленого електронного підпису пов’язаного з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження удосконаленого електронного підпису					
	0.4.0.194112.1.0	QCP-n	Представник юр. особи	ні	так	ні
5	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					
	0.4.0.194112.1.3	QCP-l-qscd	Юридична особа	так	ні	ні
6	кваліфікований сертифікат електронної печатки, що пов'язує відкритий ключ удосконаленої електронної печатки з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження удосконаленої електронної печатки					
	0.4.0.194112.1.1	QCP-l	Юридична особа	ні	так	ні
7	кваліфікований сертифікат шифрування, що пов'язує відкритий ключ кваліфікованого електронного підпису з фізичною особою та забезпечує направлене шифрування під час обміну інформацією (узгодження ключ шифрування)					
	0.4.0.194112.1.2	QCP-n-qscd	Фізична особа	ні	ні	так
8	кваліфікований сертифікат шифрування, що пов'язує відкритий ключ удосконаленого електронного підпису з фізичною особою та забезпечує направлене шифрування під час обміну інформацією (узгодження ключ шифрування)					
	0.4.0.194112.1.0	QCP-n	Фізична особа	ні	ні	так
9	кваліфікований сертифікат шифрування, що пов'язує відкритий ключ кваліфікованого електронного підпису з юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією (узгодження ключ шифрування)					
	0.4.0.194112.1.2	QCP-n-qscd	Представник юр. особи	ні	ні	так
10	кваліфікований сертифікат шифрування, що пов'язує відкритий ключ удосконаленого електронного підпису з юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією (узгодження ключ шифрування)					

	0.4.0.194112.1.0	QCP-n	Представник юр. особи	ні	ні	так
11	кваліфікований сертифікат шифрування, що пов'язує відкритий ключ кваліфікованого електронної печатки з юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією (узгодження ключ шифрування)					
	0.4.0.194112.1.3	QCP-l-qscd	Юридична особа	ні	ні	так
12	кваліфікований сертифікат шифрування, що пов'язує відкритий ключ удосконаленої електронної печатки з юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією (узгодження ключ шифрування)					
	0.4.0.194112.1.1	QCP-l	Юридична особа	ні	ні	так
13	кваліфікований сертифікат автентифікації веб-сайту, що пов'язує відкритий ключ кваліфікованої електронного підпису з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації					
	0.4.0.194112.1.4	QCP-w	Юридична особа	так	ні	ні

Поля та формат інформації, що міститься в кваліфікованому сертифікаті:

Найменування	**Значення**
Версія	Версія 3 (версія 3) стандарт X.509
Серійний Номер	Номер сертифіката Значення цього поля є унікальним
Алгоритм підпису	Криптографічний алгоритм Визначає алгоритм, який використовується для підпису кваліфікованого сертифіката
Емітент	Назва надавача, що формує кваліфікований сертифікат
Дійсний від	Дата початку дії кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Дійсний до	Дата закінчення строку дії кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Тема	Інформація про отримувача кваліфікованого сертифіката (відповідно до стандарту RFC 5280)

	Детальніше див. п. 3.1.1
Відкритий ключ	Відкритий ключ, що відповідає особистому ключу кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Підпис	Кваліфікований електронний підпис КНЕДП ТОВ "АТС", що надає послугу створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки згенерований та закодований відповідно до стандарту RFC 5280.

Надавач може включати розширення Extended Key Usage (EKU) до кваліфікованих сертифікатів користувачів, які визначають сферу використання кваліфікованих сертифікатів.
До таких розширень (certificate extensions) можуть належати:

- ServerAuth — автентифікація TLS вебсервера (OID: 1.3.6.1.5.5.7.3.1);
- ClientAuth — автентифікація TLS вебклієнта (OID: 1.3.6.1.5.5.7.3.2);
- CodeSigning — підписання програмного коду (OID: 1.3.6.1.5.5.7.3.3);
- EmailProtection — захист електронної пошти (OID: 1.3.6.1.5.5.7.3.4);
- TimeStamping — формування позначок часу (OID: 1.3.6.1.5.5.7.3.8);
- OCSPSigning — підписання відповідей служби перевірки статусу сертифікатів (OID: 1.3.6.1.5.5.7.3.9);
- DocumentSigning — підписання електронних документів (OID: 1.3.6.1.4.1.311.10.3.12);
- Інші, відповідно до технічних і функціональних потреб користувача або вимог до конкретного виду кваліфікованого сертифіката.

7.2. Профілі списку відкликаних сертифікатів (CRL)

Списки відкликаних сертифікатів (CRL), що формуються КНЕДП ТОВ "АТС" повинні відповідати вимогам таких стандартів:

- ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів” (далі - ISO/IEC 9594-8:2020).

- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. Формат інформації в CRL, що публікується КНЕДП ТОВ "АТС", відповідає стандарту ITU-T X.509 та регламенту RFC 5280. CRL повинен мати щонайменше такі поля:

Найменування	**Значення**
Версія	Версія CRL (version 2).
Емітент	Назва Надавача, що формує CRL
Дата набрання чинності	Поточна дата випуску (оновлення) CRL
Наступне оновлення	Дата наступного оновлення CRL
Скасовані сертифікати	У цьому полі міститься інформація про скасовані кваліфіковані сертифікати, зокрема: - серійний номер (серійний номер скасованого кваліфікованого сертифіката);

	- дата скасування (час, коли кваліфікований сертифікат було скасовано); - запис про скасування (розширена інформація скасованого кваліфікованого сертифіката (необов'язкове поле)
Алгоритм підпису	Алгоритм, що використовується для підписання CRL
Алгоритм ґешування підпису	Алгоритм ґешування
Підпис	Значення цифрового підпису від надавача
Розширення CRL	Інша розширена інформація (необов'язкове поле)

7.3. Профілі протоколу визначення статусу сертифіката (OCSP)

Розповсюдження інформації про статус кваліфікованих сертифікатів користувачів здійснюється шляхом створення можливості перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу через електронні комунікаційні мережі загального користування із використанням протоколу OCSP.

Посилання на сервіс перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу вносяться до кваліфікованих сертифікатів користувачів.

Процедура інтерактивного визначення статусу сертифіката та формати даних повинні відповідати вимогам таких стандартів:

- ISO/IEC 8825-1:2002 “Information technology - ASN.1 Encoding Rules - Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

- RFC 2560 “Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - 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 та ДСТУ ETSI EN 319 411-2.

8.1. Частота або обставини оцінювання

Не допускається надання кваліфікованих електронних довірчих послуг без чинних документів, визначених законодавством, що підтверджують відповідність ІКС КНЕДП ТОВ "АТС" та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність, за результатами проходження процедури оцінки відповідності, у сфері електронних довірчих послуг.

КНЕДП ТОВ "АТС" знаходиться під наглядом КО, функції якого виконує Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

КО у випадках, визначених законом, може:

1) здійснити позапланову перевірку щодо дотриманням надавачем вимог законодавства у сфері електронних довірчих послуг:

- за його заявою;

- у разі виявлення та підтвердження наявності недостовірних відомостей у поданих ним документах;

- після отримання інформації чи повідомлення про порушення вимог законодавства у сфері електронних довірчих послуг від ЦЗО, суду, користувачів або третіх осіб;

- за обґрунтованим рішенням КО.

КО не здійснює планові заходи контролю.

2) подати запит до ООВ про надання аудиторського звіту щодо проведення процедури оцінки відповідності надавача за рахунок такого надавача для підтвердження того, що він та електронні довірчі послуги, які він надає, відповідають вимогам у сфері електронних довірчих послуг.

Про результати оцінки відповідності надавач повідомляє КО шляхом надання копії документа про відповідність не пізніше трьох робочих днів з дня його отримання.

КНЕДП ТОВ "АТС" повинен кожні 24 місяці за власний рахунок проходити процедуру оцінки відповідності для доведення того, що він та електронні довірчі послуги, які він надає, відповідають вимогам законодавства та стандартів.

Оцінку відповідності проводить ООВ, як зазначено в розділі 8.2 цієї Політики сертифіката.

КНЕДП ТОВ "АТС" проходить оцінку відповідності згідно з вимогами:

- ДСТУ ETSI EN 319 401;
- ДСТУ ETSI EN 319 411-1;
- ДСТУ ETSI EN 319 411-2.

Атестат (сертифікат) підтвердження відповідності ІКС КНЕДП ТОВ «АТС», виданий за результатами проходження процедури оцінки відповідності (сертифікації) Надавача, діє протягом строку, зазначеного у відповідному атестаті (сертифікаті), та підтверджує відповідність ІКС вимогам нормативних документів у сфері електронних довірчих послуг та інформаційної безпеки.

8.2. Особа/кваліфікація оцінювача

8.2.1. Вимоги до кваліфікації контролюючого органу (КО)

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

Виїзний позаплановий захід державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг (далі - перевірка) здійснюється посадовими особами КО відповідно до їх функціональних обов’язків за місцезнаходженням КНЕДП ТОВ "АТС".

Перевірка здійснюється відповідно до рішення КО.

Рішення щодо проведення перевірки повинно містити:

1) найменування КО;

2) найменування Надавача,

3) місцезнаходження Надавача;

4) підставу для проведення перевірки;

5) предмет перевірки;

6) дати початку та закінчення перевірки;

7) посадовий та персональний склад комісії з перевірки.

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

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

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

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

8.2.3. Вимоги до кваліфікації установи, що проводить Експертизу

У випадку необхідності проходження перевірки щодо відповідності вимогам КСЗІ, установа, яка здійснює Експертизу КСЗІ, повинна мати чинну ліцензію, видану Адміністрацією Державної служби спеціального зв'язку та захисту інформації України на провадження діяльності у сфері технічного захисту інформації (ТЗІ).

Вибір такої установи здійснюється за ініціативою КНЕДП ТОВ «АТС» та погоджується з Адміністрацією Держспецзв'язку в установленому порядку. Установа повинна мати підтверджений досвід проведення Експертиз об'єктів інформаційної інфраструктури, що обробляють інформацію з обмеженим доступом, та відповідати усім критеріям професійної компетентності, передбаченим чинним законодавством.

8.3. Відносини експерта з об'єктом оцінки

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

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

Члени комісії з перевірки зобов'язані:

- об'єктивно та неупереджено проводити перевірку;
- дотримуватися вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг, захисту інформації та захисту персональних даних;
- сумлінно, вчасно та якісно виконувати свої службові обов'язки та доручення голови комісії з перевірки;
- дотримуватися ділової етики у взаємовідносинах з керівником та персоналом КНЕДП ТОВ "АТС";
- ознайомлювати керівника КНЕДП ТОВ "АТС" чи уповноваженого ним представника з результатами перевірки;
- надавати КНЕДП ТОВ "АТС" консультаційну допомогу з питань проведення перевірки;
- не розголошувати інформацію з обмеженим доступом, яка стала їм відома у зв'язку з виконанням службових обов'язків.

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

Експерти (аудитори), які проводять оцінку відповідності, повинні бути незалежними, неупередженими та не мати спільних ділових інтересів або будь-яких інших ділових чи фінансових зв'язків із КНЕДП ТОВ «АТС», що можуть вплинути на об'єктивність результатів оцінки.

8.3.3. Відносини експертів, що проводять Експертизу

У разі необхідності проведення експертизи комплексної системи захисту інформації (КСЗІ) експерти, які здійснюють відповідну перевірку, повинні бути незалежними та неупередженими, а також не мати спільних ділових інтересів або будь-яких інших ділових зв'язків із КНЕДП ТОВ «АТС», що можуть вплинути на об'єктивність і достовірність результатів експертизи.

8.4. Теми, охоплені оцінюванням

8.4.1. Питання, що підлягають перевірці під час державного контролю

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

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

8.4.2. Питання, що підлягають перевірці під час оцінки відповідності

Предметом оцінки відповідності, що проводиться ООВ, є стан дотримання вимог ДСТУ ETSI EN 319 411.

8.4.3. Питання, що підлягають перевірці під час Експертизи

У випадку проходження перевірки щодо відповідності вимогам КСЗІ, перелік питань, які розглядаються у межах експертної оцінки, визначається у Програмі проведення Експертизи. Така Програма узгоджується з КНЕДП ТОВ "АТС".

8.5. Дії, вжиті внаслідок порушення

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

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

- здійснювати виїзні та невиїзні заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг;
- у разі виявлення порушення вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг видавати обов'язкові для виконання приписи про усунення порушень і визначати строк усунення виявлених порушень;
- накладати на винних осіб адміністративні стягнення за порушення вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги" та інших нормативно-правових актів, прийнятих відповідно до цього Закону;
- звертатися до суду щодо застосування заходів реагування;
- виконувати інші повноваження, визначені законом.

За результатами проведення перевірок КО вживає таких заходів реагування:

1) вимагає від КНЕДП ТОВ "АТС" усунення порушень вимог законодавства у сфері електронних довірчих послуг у встановлений приписом строк;

2) приймає рішення про блокування кваліфікованого сертифіката КНЕДП ТОВ "АТС", якщо під час перевірки виникла підозра компрометації особистого ключа;

3) приймає рішення про скасування кваліфікованого сертифіката КНЕДП ТОВ "АТС", якщо під час перевірки виявлено факт компрометації особистого ключа.

Рішення про блокування або скасування кваліфікованого сертифіката КНЕДП ТОВ "АТС" КО надсилає в день його прийняття до ЦЗО;

4) надсилає до ЦЗО подання про відкликання статусу кваліфікованого надавача електронних довірчих послуг або послуги, яку надає КНЕДП ТОВ "АТС", у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, визначених законодавством, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг;

- надання кваліфікованих електронних довірчих послуг за відсутності у КНЕДП ТОВ "АТС" поточного рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) з необхідним обсягом коштів або чинного договору страхування цивільно-правової відповідальності з необхідним розміром страхової суми, що встановлені Законом України "Про електронну ідентифікацію та електронні довірчі послуги", для забезпечення відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг або третім особам внаслідок неналежного виконання надавачем своїх зобов'язань;

- порушення вимог до умов експлуатації КСЗІ ІКС КНЕДП ТОВ "АТС";

- надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ "АТС" без чинних документів, визначених законодавством, що підтверджують його право власності та/або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються для надання кваліфікованих електронних довірчих послуг;

- встановлення факту надання недостовірних відомостей, наведених у документах, поданих КНЕДП ТОВ "АТС" для внесення відомостей про нього до Довірчого списку;

- не усунення виявлених під час перевірки порушень у встановлений приписом строк;

- блокування або скасування кваліфікованого сертифіката КНЕДП ТОВ "АТС".

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

За результатами проведення процедури оцінки відповідності у сфері електронних довірчих послуг ООВ приймається одне з таких рішень:

- про відповідність об’єкта оцінки відповідності у повному обсязі вимогам у сфері електронних довірчих послуг;

- про невідповідність об’єкта оцінки відповідності вимогам у сфері електронних довірчих послуг.

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

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

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

КО надсилає до ЦЗО подання про відкликання статусу надавача або послуги, яку надає надавач, у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, визначених законодавством, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг.

8.5.3. Дії, що вживаються внаслідок порушення, виявленого за результатами Експертизи

У випадку проходження перевірки щодо відповідності вимогам КСЗІ, у разі виявлення порушення або невідповідностей за результатами Експертизи, КНЕДП ТОВ «АТС» впроваджує необхідні заходи для усунення порушення та запобігання його повторенню в майбутньому. Після впровадження коригувальних дій КНЕДП ТОВ «АТС» може ініціювати проведення повторної Експертизи з метою підтвердження усунення порушень і відповідності системи вимогам нормативних документів у сфері ТЗІ. Результати повторної Експертизи додаються до загальної технічної документації КСЗІ.

8.6. Повідомлення результатів

8.6.1. Оформлення результатів державного контролю

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

Акт перевірки має містити такі відомості:

- найменування КО;
- персональний та посадовий склад комісії з перевірки;
- прізвище та ініціали керівника надавача;
- реквізити посвідчення на проведення перевірки;
- дати початку і закінчення перевірки;
- адреса приміщень надавача, в яких проводилася перевірка;
- результати попередньої перевірки;
- інформація про результати останньої оцінки відповідності у сфері електронних довірчих послуг, що передує перевірці;
- назва та короткий зміст документів, наданих під час перевірки;
- якісні та кількісні показники, встановлені під час перевірки, що характеризують діяльність надавача, пов'язану з наданням електронних довірчих послуг;
- виявлені під час перевірки порушення і недоліки (за наявності) та пояснення надавача про причини невиконання встановлених законодавством вимог (за наявності);
- висновки за результатами перевірки;
- факти протидії проведенню перевірки (за наявності);
- рекомендації щодо усунення виявлених порушень (у разі наявності);
- дата складення акту перевірки;
- підписи голови та членів комісії з перевірки;
- підпис керівника надавача чи уповноваженого ним представника, що підтверджує факт ознайомлення з актом перевірки.

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

Член комісії з перевірки, який не погоджується з висновками комісії з перевірки, зазначеними в акті перевірки, зобов'язаний підписати його та письмово викласти свою окрему

думку, що додається до акту перевірки. При цьому перед підписом акту перевірки зазначається "З окремою думкою, що додається".

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

Зауваження до акту перевірки оформлюються окремим документом та підписуються керівником надавача чи уповноваженим ним представником. Зауваження до акту перевірки та окрема думка члена комісії з перевірки є невід'ємними частинами акту перевірки.

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

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

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

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

Форма припису про усунення порушень затверджується КО.

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

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

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

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

8.6.3. Оформлення результатів оцінки відповідності

Документ про відповідність повинен містити такі відомості:

- найменування ООВ;
- інформацію про акредитацію ООВ (дата та номер атестата про акредитацію);
- прізвище, ім'я, по батькові (у разі наявності) осіб, що проводили процедуру оцінки відповідності;
- період проведення процедури оцінки відповідності;
- реквізити надавача (найменування, ідентифікаційні дані та контактна інформація);
- сфера оцінки відповідності;
- перелік кваліфікованих електронних довірчих послуг, які має намір надавати КНЕДП ТОВ "АТС";

- найменування ІКС;

- найменування засобів кваліфікованого електронного підпису, які використовуються під час надання кваліфікованих електронних довірчих послуг;

- перелік вимог у сфері електронних довірчих послуг, національних стандартів та/або технічних специфікацій, щодо відповідності яким проводилася процедура оцінка відповідності;

- висновок щодо відповідності вимогам у сфері електронних довірчих послуг;

- строк дії документа про відповідність.

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

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

8.6.4. Оформлення результатів Експертизи

У випадку проходження перевірки щодо відповідності вимогам КСЗІ, експертний висновок повинен містити:

- загальні відомості щодо об’єкта Експертизи (тип, місце розташування, власник);
- загальну характеристику об’єкта Експертизи (призначення, функції, можливості щодо вирішення певних завдань захисту інформації);
- перелік нормативних документів з ТЗІ, на відповідність вимогам яких проводиться оцінка об’єкта Експертизи;
- назви програми та методики, згідно з якими проводилася оцінка об’єкта Експертизи, ким розроблені та затверджені, реєстраційний номер та дату затвердження;
- перелік документів і специфікацій програмних та технічних засобів ТЗІ, які Замовник надав Організатору;
- перелік засобів ТЗІ (із зазначенням їх типів, заводських номерів, року випуску), які Замовник надав Організатору (у разі проведення Експертизи засобів ТЗІ);
- результати робіт щодо кожного пункту програми проведення експертизи об’єкта;
- розгорнутий висновок щодо відповідності об’єкта Експертизи вимогам нормативних документів із ТЗІ;
- сферу використання (вимоги до умов експлуатації) об’єкта Експертизи;
- строк дії експертного висновку;
- особливі думки експертів, зафіксовані в протоколах виконання робіт.

8.7. Самоперевірки

Протягом періоду формування сертифікатів, КНЕДП ТОВ "АТС" контролює дотримання цієї Політики сертифіката та відповідних Положень сертифікаційних практик, суворо контролюючи якість своїх послуг, час від часу виконуючи самоперевірки, виданих сертифікатів.

КНЕДП ТОВ "АТС" проводить регулярні внутрішні аудити, щоб оцінювати дотримання вимог законодавства, внутрішньої політики та вимог цієї Політики сертифіката та відповідних Положень сертифікаційних практик щонайменше раз на рік.

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 та ДСТУ ETSI EN 319 411-2.

9.1. Збори

9.1.1. Плата за видачу або поновлення сертифіката

Плата за формування кваліфікованого сертифіката справляється у порядку та розмірах, визначених тарифними планами на надання кваліфікованих електронних довірчих послуг КНЕДП ТОВ «АТС», опублікованими на веб-сайті КНЕДП ТОВ «АТС», якщо інше не передбачено внутрішніми документами КНЕДП ТОВ «АТС» або договорами про надання кваліфікованих електронних довірчих послуг з користувачами. У разі якщо кваліфікована електронна довірча послуга надається як складова інших послуг ТОВ «АТС», відомості про умови її надання, у тому числі щодо оплати, можуть оприлюднюватися на рекламно-інформаційному веб-сайті ТОВ «АТС».

У разі надання кваліфікованих електронних довірчих послуг через відокремлені пункти реєстрації КНЕДП ТОВ "АТС" або представництв може стягуватися додаткова плата за надання кваліфікованих електронних довірчих послуг.

Поновлення заблокованих кваліфікованих сертифікатів здійснюється на безоплатній основі.

Відповідні Положення сертифікаційних практик КНЕДП ТОВ "АТС" щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

9.1.2. Плата за доступ до сертифіката

Немає плати за доступ до кваліфікованого сертифіката.

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

КНЕДП ТОВ "АТС" може надавати користувачам додаткові послуги за плату, серед яких:

- надання засобів кваліфікованого електронного підпису чи печатки користувачам;
- виїзна генерація пари ключів користувача;
- зберігання особистих ключів в хмарному сховищі КНЕДП ТОВ "АТС";
- інші послуги.

9.1.5. Політика відшкодування

КНЕДП ТОВ "АТС" не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Діяльність КНЕДП ТОВ "АТС" відповідає вимогам частини п'ятої статті 16 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” щодо надання кваліфікованих електронних довірчих послуг за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. Розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менше 1 тисячі розмірів мінімальної заробітної плати.

Надавач має право укладати договори страхування професійної відповідальності. Відповідальність Надавача перед Користувачами за шкоду, завдану неналежним наданням

кваліфікованих електронних довірчих послуг, обмежується прямими документально підтвердженими збитками, що безпосередньо спричинені діями чи бездіяльністю Надавача, та не включає упущену вигоду.

Максимальний розмір відповідальності Надавача за одним договором або кваліфікованим сертифікатом не може перевищувати сукупний розмір плати, фактично сплаченої Користувачем за користування відповідними послугами за останні 12 (дванадцять) календарних місяців, або інший розмір, прямо передбачений договором.

9.3. Конфіденційність ділової інформації

9.3.1. Обсяг конфіденційної інформації

В процесі надання послуг, КНЕДП ТОВ "АТС" обробляє конфіденційну інформацію, яка не оприлюднюється для загального ознайомлення. Захист конфіденційної інформації здійснюється відповідно чинного законодавства.

9.3.2. Інформація, що не належить до конфіденційної

Інформація та документація, яка є доступною для загального ознайомлення, публікується на веб-сайті КНЕДП ТОВ "АТС" та не належить до конфіденційної інформації.

9.3.3. Відповідальність за захист конфіденційної інформації

КНЕДП ТОВ "АТС" здійснює захист конфіденційної інформації та несе відповідальність згідно з вимогами чинного законодавства.

9.4. Конфіденційність персональної даних

9.4.1. Концепція захисту персональних даних

КНЕДП ТОВ "АТС" у процесі надання кваліфікованих електронних довірчих послуг здійснює:

- захист персональних даних користувачів відповідно до вимог Закону України "Про захист персональних даних";
- інформування КО та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання кваліфікованих електронних довірчих послуг або стосуються персональних даних користувачів, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли йому стало відомо про таке порушення;
- інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли йому стало відомо про таке порушення.

9.4.2. Визначення персональних даних

Поняття “персональні дані” розуміється у значенні, наведеному у статті 2 Закону України “Про захист персональних даних”.

9.4.3. Персональні дані, що не вважаються конфіденційними

Персональні дані можуть належати до відкритої інформації у випадках, передбачених чинним законодавством України.

9.4.4. Відповідальність за захист персональних даних

КНЕДП ТОВ "АТС" гарантує дотримання вимог законодавства щодо захисту персональних даних та несе відповідальність згідно з нормами чинного законодавства України.

Керівник КНЕДП ТОВ "АТС" забезпечує створення умов для безперервного професійного розвитку персоналу, включаючи:

- Систематичне підвищення кваліфікації у сферах інформаційних технологій, захисту інформації та персональних даних.
- Проведення навчальних програм і тренінгів для працівників, які займаються наданням електронних довірчих послуг.
- Актуалізацію знань персоналу відповідно до змін у законодавстві та міжнародних стандартах інформаційної безпеки.

Ці заходи сприяють підвищенню компетентності працівників, забезпеченню надійного захисту персональних даних та відповідності діяльності КНЕДП сучасним вимогам кібербезпеки.

9.4.5. Інформація та згода на використання персональних даних

Відповідно до Закону України "Про захист персональних даних" КНЕДП ТОВ "АТС" надає кваліфіковані довірчі послуги відповідно до укладеного договору з користувачем та здійснює обробку персональних даних користувача в межах виконання договору чи для здійснення заходів, що передують укладанню договору на вимогу користувача.

9.4.6. Розкриття персональних даних

КНЕДП ТОВ "АТС" надає доступ до персональних даних користувачів лише у випадках, передбачених Законом України "Про захист персональних даних".

Керівник КНЕДП ТОВ "АТС" та персонал КНЕДП ТОВ "АТС" дотримуються вимог законодавства України в сфері захисту персональних даних та підписують договір про конфіденційність та нерозголошення інформації.

9.5. Права інтелектуальної власності

Питання прав інтелектуальної власності КНЕДП ТОВ "АТС" врегульовані відповідно до вимог чинного законодавства України.

9.6. Зобов’язання та гарантії

9.6.1. Зобов’язання та гарантії

Надавача КНЕДП ТОВ "АТС" надає кваліфіковані електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг, цієї Політики сертифіката та відповідних Положень сертифікаційних практик.

9.6.2. Зобов’язання та гарантії відокремлених пунктів реєстрації

На підставі договору, укладеного з КНЕДП ТОВ "АТС" (ТОВ "АТС"), реєстрацію користувачів здійснюють відокремлені пункти реєстрації КНЕДП ТОВ "АТС" або представництва, які виконують свої функції згідно з цією Політикою сертифіката та відповідними Положеннями сертифікаційних практик.

До працівників відокремлених пунктів реєстрації КНЕДП ТОВ "АТС", на яких покладено обов’язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації КНЕДП ТОВ "АТС".

9.6.3. Зобов’язання та гарантії користувачів

КНЕДП ТОВ "АТС" забезпечує можливість користувачів підписувати та перевіряти підписані файли за допомогою віджетів підписання та перевірки підписів, та за допомогою спеціалізованого програмного забезпечення, що розміщені на веб-сайті Надавача.

Користувачі зобов'язані:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

- невідкладно повідомляти КНЕДП ТОВ "АТС" про підозру або факт компрометації особистого ключа;

- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;

- своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між КНЕДП ТОВ "АТС" та користувачем;

- своєчасно надавати КНЕДП ТОВ "АТС" інформацію про зміну ідентифікаційних даних, які містить кваліфікований сертифікат;

- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування кваліфікованого сертифіката.

Користувач гарантує, що:

- для підписання використовує особистий ключ, що відповідає відкритому ключу в кваліфікованому сертифікаті;

- на момент підписання кваліфікований сертифікат є чинним (не перебуває в статусі блокований або скасований);

- особистий ключ та пароль від нього не скомпрометовані і не використовуються іншими особами;

- вся інформація зазначена в кваліфікованому сертифікаті є коректною;

- кваліфікований сертифікат використовується за призначенням, відповідно до положень цієї Політики сертифіката;

- до договору про надання електронних довірчих послуг можуть бути включені додаткові умови. Зміст договору про надання електронних довірчих послуг публікується на веб-сайті КНЕДП ТОВ "АТС" .

9.6.4. Зобов’язання та гарантії суб’єктів, які довіряють Надавачу

Суб’єкт, який довіряє КНЕДП ТОВ "АТС" , повинен перевірити чинність кваліфікованого сертифіката сформованого КНЕДП ТОВ "АТС" за допомогою послуг перевірки та підтвердження електронного підпису чи печатки, перед використанням кваліфікованого сертифіката.

9.6.5. Зобов’язання та гарантії інших учасників

ЦЗО перш ніж прийняти рішення про внесення КНЕДП ТОВ "АТС" до Довірчого списку та надання йому кваліфікованого статусу пересвідчився щодо наявності в КНЕДП ТОВ "АТС":

- документа, що підтверджує відповідність системи захисту інформації КНЕДП ТОВ "АТС" вимогам положень статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

- документів, які підтверджують право власності та право користування КНЕДП ТОВ "АТС" нежилими приміщеннями, які використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання кваліфікованих електронних довірчих послуг;

- належного персоналу КНЕДП ТОВ "АТС";

- документів, які підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи за фахом персоналу КНЕДП ТОВ "АТС";

- документів, які підтверджують право власності або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються КНЕДП ТОВ "АТС" для надання кваліфікованих електронних довірчих послуг;

- документів, що підтверджують внесення коштів на поточний рахунок КНЕДП ТОВ "АТС" із спеціальним режимом використання у банку (рахунок в органі, що здійснює

казначейське обслуговування бюджетних коштів) для забезпечення відшкодування збитків, які можуть бути заподіяні користувачам унаслідок неналежного виконання КНЕДП ТОВ "АТС" своїх обов'язків;

- цієї Політики сертифіката та відповідних Положень сертифікаційних практик;

- відомостей про відокремлені пункти реєстрації та їхніх працівників, обов'язки яких будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг.

9.7. Відмова від гарантій

КНЕДП ТОВ "АТС" не надає жодних гарантій щодо послуг, які ним надаються, крім тих, які були чітко визначені в пункті 9.6.1 цієї Політики сертифіката.

9.8. Обмеження відповідальності

У разі, якщо КНЕДП ТОВ "АТС" заздалегідь та належним чином повідомить користувачів про обмеження щодо використання електронних довірчих послуг, які він надає, і ці обмеження є зрозумілими для користувачів, КНЕДП ТОВ "АТС" не несе відповідальності за шкоду, що виникла внаслідок використання електронних довірчих послуг з порушенням зазначених обмежень.

Це означає, що користувач самостійно відповідає за правильність застосування довірчих послуг у межах визначених правил та умов їх використання.

9.9. Відшкодування збитків

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

9.10. Термін дії та припинення дії

Ця Політика сертифіката застосовується з моменту її публікації та діє до закінчення строку дії останнього сертифіката, виданого відповідно до цієї Політики сертифіката або до моменту припинення діяльності КНЕДП ТОВ "АТС".

9.11. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

КНЕДП ТОВ "АТС" здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на веб-сайті КНЕДП ТОВ "АТС";

- 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 до цієї Політики сертифіката здійснюється КНЕДП ТОВ "АТС" у разі:

- змін вимог, процесів та процедур описаних в цій Політиці сертифіката;

- змін в законодавстві;

- змін у вимогах до надавачів щодо надання послуг.

Нові версії цієї Політики сертифіката після внесення змін до неї, публікуються на веб-сайті КНЕДП ТОВ "АТС".

Будь-які зміни, не зазначені в історії цієї Політики сертифіката, є граматичними і орфографічними змінами, які не впливають на суть та не стосуються процесів та процедур описаних в цій Політиці сертифіката.

9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей, КНЕДП ТОВ "АТС" (ТОВ "АТС") 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 цією Політикою сертифіката, поширюється чинне законодавство України.

9.15. Дотримання чинного законодавства

Під час надання електронних довірчих послуг КНЕДП ТОВ "АТС" повинен дотримуватися вимог:

- Закону України “Про електронну ідентифікацію та електронні довірчі послуги”;
- Закону України “Про захист інформації в інформаційно-комунікаційних системах”;
- Закону України “Про захист персональних даних”;
- постанови КМУ від 27.01.2010 р. № 55 “Про впорядкування транслітерації українського алфавіту латиницею”;
- постанови КМУ від 12.12.2023 № 1298 “Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів”;
- постанови КМУ від 01.08.2023 № 798 “Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності”;
- постанови КМУ від 04.12.2019 № 1137 “Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг”;

постанови Кабінету Міністрів України від 10.12.2024 №1408 “Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг”;

- постанови КМУ від 10.12.2024 №1408 “Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг”;

- постанови Кабінету Міністрів України від 28.06.2024 р. № 764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 13.09.2024 р. № 1062 “Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг”;
- постанови КМУ від 23.06.2024 р. № 842 “Про затвердження переліку документів та електронних даних, отриманих у зв’язку з наданням електронних довірчих послуг, що підлягають постійному зберіганню, та Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав

договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг”;

- постанови Правління Національного банку України від 17.03.2020 р. № 32 “Про затвердження Положення про Систему BankID Національного банку України”;

- наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 1.02.2019 р. № 316/5/57 “Про позначку кваліфікованого сертифіката відкритого ключа”, зареєстрованого в Міністерстві юстиції України 5.02.2019 р. за № 123/33094;

- наказу Міністерства цифрової трансформації України від 17.11.2023 р. № 149 “Про затвердження Порядку ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, які сформовані центральним засвідчувальним органом”, зареєстрованого в Міністерстві юстиції України 05 грудня 2023 р. за № 2110/41166;

- наказу Міністерства цифрової трансформації України від 25.08.2020 р. № 125 “Про Вимог до формату реєстрів сформованих кваліфікованих сертифікатів відкритих ключів, а також носіїв інформації та порядку запису на них документів в електронній формі”, зареєстрованого в Міністерстві юстиції України 6 листопада 2020 р. за № 1086/35369;

- наказу Міністерства цифрової трансформації України від 06.04.2024 р. №54 “Про затвердження форми плану припинення діяльності з надання кваліфікованих електронних довірчих послуг”, зареєстрованого в Міністерстві юстиції України 23 квітня 2024 р. за № 588/41933;

- наказу Міністерства цифрової трансформації України від 28.02.2024 р. № 33 “Про затвердження Регламенту роботи центрального засвідчувального органу”, зареєстрованого в Міністерстві юстиції України 15 березня 2024 р. за № 393/41738.