

ЗАТВЕРДЖЕНО

Наказ Міністерства цифрової
трансформації України

_____ 2023 року № _____

**Особливості
надання кваліфікованої електронної довірчої послуги формування,
перевірки та підтвердження чинності кваліфікованого сертифіката
шифрування**

1. Ці Особливості визначають вимоги до кваліфікованих сертифікатів відкритих ключів, призначених виключно для використання в протоколі узгодження ключа шифрування (далі – кваліфікований сертифікат шифрування), вимоги до процедур формування, зберігання, скасування, блокування, поновлення, надання інформації про статус кваліфікованих сертифікатів шифрування, надання доступу до сформованих кваліфікованих сертифікатів шифрування, а також вимоги до засобів криптографічного захисту інформації, які забезпечують використання кваліфікованих сертифікатів шифрування (далі – засоби шифрування).

Дія цих Особливостей не поширюється на надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (далі – Закон).

2. У цих Особливостях терміни вживаються у значеннях, наведених у Законі та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.

3. Фізичні та юридичні особи, яким кваліфікований надавач електронних довірчих послуг видав кваліфікований сертифікат шифрування (далі – користувачі), зобов'язані використовувати цей кваліфікований сертифікат шифрування та відповідний йому особистий ключ виключно в протоколах шифрування (узгодження ключа шифрування).

4. Кваліфікований надавач електронних довірчих послуг та його відокремлені пункти реєстрації, що забезпечують формування та видачу кваліфікованих сертифікатів шифрування, зобов'язані:

1) виконувати під час формування, зберігання, скасування, блокування, поновлення, надання інформації про статус кваліфікованих сертифікатів

шифрування, надання доступу до сформованих кваліфікованих сертифікатів шифрування вимоги до таких самих процедур для кваліфікованих сертифікатів електронного підпису чи печатки, установлені Кабінетом Міністрів України відповідно до частини третьої статті 20 Закону;

2) установлювати під час формування кваліфікованого сертифіката шифрування в розширенні “використання ключа” об’єктний ідентифікатор `id-ce-keyUsage OBJECT IDENTIFIER ::= {id-ce 15}` виключно із значенням “узгодження ключа” (“keyAgreement”);

3) використовувати та надавати користувачам засоби шифрування, що відповідають вимогам пункту 5 цих Особливостей.

5. Засоби шифрування повинні реалізувати формат згідно з RFC 5652 “Cryptographic Message Syntax (CMS)” з використання криптографічних алгоритмів згідно з RFC 3370 “Cryptographic Message Syntax (CMS) Algorithms” або формат згідно з Технічними специфікаціями до RFC 5652, затвердженими наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27.10.2020 № 687, зареєстрованими в Міністерстві юстиції України 21.12.2020 за № 1273/35556 (далі – формат криптоповідомлення).

У засобах кваліфікованого електронного підпису додатково до функцій, реалізованих згідно з вимогами, установленими частинами першою – четвертою статті 19 Закону, можуть реалізовуватися формати криптоповідомлень.

Реалізація форматів криптоповідомлень у засобах шифрування, засобах кваліфікованого електронного підпису повинна бути підтверджена за результатами державної експертизи у сфері криптографічного захисту інформації або сертифікації відповідно до вимог законодавства у сфері захисту інформації.

**Директор директорату
розвитку цифровізації**

Анастасія ХАЛЄЄВА