Додаток 1
до Регламенту роботи центрального
засвідчувального органу
(пункт 1 глави 1 розділу IV)

Обов’язкові реквізити надавача в запиті на формування сертифіката ключа

Таблиця 1

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту
countryName	назва країни	країна, в якій зареєстрована організація, - юридична особа або фізична особа – підприємець id-at-countryName AttributeType**: : =** {id-at 6} X520countryName **: : =** PrintableString (SIZE (2)) код згідно з міжнародним стандартом ISO 3166 (для України - UA)
organizationName	найменування організації	повне (або офіційне скорочене) найменування організації - юридичної особи або прізвище та ініціали фізичної особи – підприємця за установчими документами або відомостями про державну реєстрацію id-at-organizationName AttributeType**: : =** {id-at 10} X520organizationName **: : =** DirectoryString (SIZE (64))
serialNumber	серійний номер	серійний номер надавача id-at-serialNumber AttributeType**: : =** {id-at 5} serialNumber**: :** =PrintableString (SIZE (64)) Формується за правилом: для юридичної особи: UA-<код за ЄДРПОУ>-<2-4 цифри(за потреби)> для фізичної особи - підприємця: UA-<РНОКПП>-<2-4 цифри(за потреби)>

Продовження додатка 1

stateOrProvinceName	назва області [1]	область, у якій зареєстрована організація, - юридична особа або фізична особа – підприємець id-at-stateOrProvinceName AttributeType **: :** = {id-at 8} X520stateOrProvinceName **: :** = DirectoryString (SIZE (64))
localityName	назва міста	місто, в якому зареєстрована організація, - юридична особа або фізична особа – підприємець id-at-localityName AttributeType**: :** = {id-at 7} X520localityName **: :** = DirectoryString (SIZE (64))
commonName	найменування надавача	найменування надавача id-at-commonName AttributeType**: :** = {id-at 3} X520commonName **: :** = DirectoryString (SIZE (64))
organizationIdentifier [2]	ідентифікатор організації [2]	унікальний ідентифікатор організації, що є надавачем. Правила заповнення цього реквізиту наведені у пункті 5.1.4 глави 5 ДСТУ ETSI EN 319 412-1:2016 id-at-organizationIdentifier OBJECT IDENTIFIER ::= {id-at 97}
signature	алгоритм кваліфікованого електронного підпису	значення реквізиту для алгоритмів кваліфікованого електронного підпису за ДСТУ 4145-2002 визначається згідно з вимогами, встановленими технічними вимогами до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та

Продовження додатка 1

		реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації; значення реквізиту для алгоритму кваліфікованого електронного підпису ECDSA з алгоритмом гешування SHA256: ecdsa-with-SHA256 OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 2}; значення реквізиту для алгоритму кваліфікованого електронного підпису ECDSA з алгоритмом гешування SHA512: ecdsa-with-SHA512 OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) 4}; значення реквізиту для алгоритму кваліфікованого електронного підпису RSA з алгоритмом гешування SHA256: sha-256WithRSAEncryption OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}; значення реквізиту для алгоритму кваліфікованого електронного підпису RSA з алгоритмом гешування

Продовження додатка 1

		SHA512: sha-512WithRSAEncryption OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
subjectPublicKeyInfo	інформація про відкритий ключ надавача	у структурі цього реквізиту, крім значення відкритого ключа та параметрів криптоперетворень (для ДСТУ 4145-2002 та ECDSA), має міститися ознака алгоритму обчислення відкритого ключа; значення ознаки алгоритму обчислення відкритого ключа для алгоритмів кваліфікованого електронного підпису за ДСТУ 4145-2002 визначається згідно з вимогами, встановленими технічними вимогами до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації; значення ознаки алгоритму обчислення відкритого ключа для алгоритму кваліфікованого електронного підпису ECDSA: id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1)

		member-body(2) us(840) ansi-X9.62(10045) id-publicKeyType(2) 1}; значення ознаки алгоритму обчислення відкритого ключа для алгоритму кваліфікованого електронного підпису RSA: rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
signatureAlgorithm	найменування криптоалгоритму, що використовується надавачем	значення реквізиту має бути ідентичним значенню реквізиту signature

[1] Якщо місцем реєстрації юридичної особи або фізичної особи – підприємця є місто Київ або Севастополь, реквізит stateOrProvinceName не заповнюється.

[2] Поле встановлюється у кваліфікованих сертифікатах для відкритих ключів, що згенеровані за криптографічними алгоритмами згідно з ДСТУ ETSI EN 119 312:2015.

Таблиця 2

Обов’язкові реквізити самопідписаного сертифіката електронної печатки ЦЗО

Назва реквізиту англійською мовою	**Назва реквізиту українською мовою**	**Значення реквізиту**
countryName	назва країни	код згідно з міжнародним стандартом ISO 3166 для України. Значення: UA
organizationName	найменування державного органу, на який покладено виконання функцій ЦЗО	значення українською мовою: Міністерство цифрової трансформації України. Значення англійською мовою, що застосовується для транскордонної взаємодії: Ministry of Digital Transformation of Ukraine [1]
serialNumber	серійний номер	формується за правилом: UA-<код за ЄДРПОУ>-<4 цифри>
localityName	назва міста	значення українською мовою:

Продовження додатка 1

		Київ. Значення англійською мовою, що застосовується для транскордонної взаємодії: Kyiv [1]
commonName	загальне найменування органу	значення українською мовою: Центральний засвідчувальний орган. Значення англійською мовою, що застосовується для транскордонної взаємодії: Central certification authority [1]
organizationalUnitName	найменування структурного підрозділу, відповідального за технічне та технологічне забезпечення виконання функцій ЦЗО	значення українською мовою: Адміністратор ІТС ЦЗО. Значення англійською мовою, що застосовується для транскордонної взаємодії: Administrator ITS CCA [1]
cps [2]	положення сертифікаційних практик [2]	встановлюється в об'єктному ідентифікаторі політики сертифіката iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) qt(2) cps(1) PolicyQualifierId ::= OBJECT IDENTIFIER (id-qt-cps | id-qt-unotice) Qualifier ::= CHOICE {cPSuriCPSuri, userNoticeUserNotice} CPSuri ::= IA5String. Значення: https://czo.gov.ua/cps

[1] Значення встановлюється у кваліфікованих сертифікатах для відкритих ключів, що згенеровані за криптографічними алгоритмами згідно з ДСТУ ETSI EN 119 312:2015.

[2] Поле встановлюється у кваліфікованих сертифікатах для відкритих ключів, що згенеровані за криптографічними алгоритмами згідно з ДСТУ ETSI EN 119 312:2015.