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

## Обов’язкові реквізити

Таблиця 1

## Обов’язкові реквізити кваліфікованого надавача електронних довірчих послуг в запиті на формування сертифіката ключа

| **Назва реквізиту англійською мовою** | **Назва реквізиту українською мовою** | **Значення реквізиту** |
|---|---|---|
| countryName | назва країни | країна, в якій зареєстрована організація, юридична особа або фізична особа – підприємець<br><br>id–at–countryName<br>AttributeType: : = {id–at 6}<br>X520countryName: : = PrintableString (SIZE (2))<br><br>код згідно з ДСТУ ISO 3166-1:2009 «Коди назв країн світу», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 року № 471 (для України – UA) |
| organizationName | найменування організації | повне (або офіційне скорочене) найменування організації – юридичної особи або прізвище, власне ім’я, по–батькові (за наявності) та фізичної особи – підприємця за установчими документами або відомостями про державну реєстрацію<br><br>id–at–organizationName<br>AttributeType: : = {id–at 10}<br>X520organizationName: : = DirectoryString (SIZE (64)) |
| serialNumber | серійний номер | серійний номер надавача<br><br>id–at–serialNumber<br>AttributeType: : = {id–at 5} |

Продовження додатка 1

| | | |
|---|---|---|
| | | serialNumber: : = PrintableString (SIZE (64))<br><br>Формується за правилом:<br><br>для юридичної особи:<br><br>UA–<код за ЄДРПОУ>–<24 цифри (у разі потреби)><br><br>для фізичної особи – підприємця:<br><br>UA–<РНОКПП>–<2–4 цифри (у разі потреби)> |
| stateOrProvinceName | назва області [1] | область, в якій зареєстрована організація, юридична особа або фізична особа – підприємець<br><br>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<br><br>id–at–localityName AttributeType: : = {id–at 7} X520localityName: : = DirectoryString (SIZE (64)) |
| commonName | найменування надавача | найменування надавача<br><br>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 в пункті 5.1.4 глави 5 ДСТУ ETSI EN 319 412–1:2021 (ETSI EN 319 412–1 V1.4.4 (2021–05), IDT) «Електронні підписи та |

Продовження додатка 1

| | | |
|---|---|---|
| | | інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних», затвердженого наказом державного підприємства «Український науково–дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16 грудня 2021 року № 512<br>id–at–organizationIdentifier OBJECT IDENTIFIER: : = {id–at 97} |
| signature | алгоритм кваліфікованого електронного підпису | значення реквізиту для алгоритмів кваліфікованого електронного підпису за ДСТУ 4145–2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженим наказом Державного комітету з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145–2002), визначається згідно з переліком стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг для надання кваліфікованих електронних довірчих послуг, та стандартами, у тому числі щодо забезпечення сумісності, перелік яких затверджується відповідно до абзацу другого частини п’ятої статті 19 Закону;<br><br>значення реквізиту для алгоритму кваліфікованого електронного підпису ECDSA з алгоритмом гешування SHA256:<br><br>ecdsa–with–SHA256 OBJECT IDENTIFIER: : = {iso(1) member–body(2) us(840) |

Продовження додатка 1

| | | |
|---|---|---|
| | | ansi–x962(10045) signatures(4) ecdsa–with–SHA2(3) 2};<br><br>значення реквізиту для алгоритму кваліфікованого електронного підпису ECDSA з алгоритмом гешування SHA512:<br><br>ecdsa–with–SHA512 OBJECT IDENTIFIER: : = {iso(1) member–body(2) us(840) ansi–x962(10045) signatures(4) ecdsa–with–SHA2(3) 4};<br><br>значення реквізиту для алгоритму кваліфікованого електронного підпису RSA з алгоритмом гешування SHA256:<br><br>sha–256WithRSAEncryption OBJECT IDENTIFIER: : = {iso(1) member–body(2) us(840) rsadsi(113549) pkcs(1) pkcs–1(1) 11};<br><br>значення реквізиту для алгоритму кваліфікованого електронного підпису RSA з алгоритмом гешування SHA512:<br><br>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;<br><br>значення ознаки алгоритму |

Продовження додатка 1

| | | |
|---|---|---|
| | | 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–комунікаційних систем, які встановлюються центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сферах електронної ідентифікації та електронних довірчих послуг, 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;<br><br>значення ознаки алгоритму обчислення відкритого ключа для алгоритму кваліфікованого електронного підпису ECDSA:<br><br>id–ecPublicKey OBJECT IDENTIFIER: : = {iso(1) member–body(2) us(840) ansi–X9.62(10045) id–publicKeyType(2) 1};<br><br>значення ознаки алгоритму обчислення відкритого ключа для алгоритму кваліфікованого електронного підпису RSA:<br><br>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 м. Київ або м. Севастополь, то реквізит stateOrProvinceName не заповнюється.

[2] Поле встановлюється у кваліфікованих сертифікатах для відкритих ключів, що згенеровані за криптографічними алгоритмами згідно з ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022–02), IDT) «Електронні підписи та інфраструктури (ESI). Криптографічні пакети», затвердженим наказом державного підприємства «Український науково–дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 29 листопада 2022 року № 232 (далі – ДСТУ ETSI TS 119 312:2022).

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 ДСТУ ISO 3166-1:2009 «Коди назв країн світу», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 року № 471 для України.<br>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> |

Продовження додатка 1

| | | |
|---|---|---|
| localityName | назва міста | значення українською мовою: Київ.<br>Значення англійською мовою, що застосовується для транскордонної взаємодії: Kyiv[1] |
| commonName | загальне найменування органу | значення українською мовою: Центральний засвідчувальний орган.<br>Значення англійською мовою, що застосовується для транскордонної<br>взаємодії: Central certification authority [1] |
| organizationalUnitName | найменування структурного підрозділу, відповідального за технічне та технологічне забезпечення виконання функцій ЦЗО | значення українською мовою: Адміністратор ІКС ЦЗО.<br>Значення англійською мовою, що застосовується для транскордонної<br>взаємодії: Administrator ITS CCA[1] |
| cps [2] | положення сертифікаційних практик [2] | встановлюється в об'єктному ідентифікаторі політики сертифіката<br>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)<br>Qualifier: : = CHOICE {cPSuriCPSuri, userNoticeUserNotice}<br>CPSuri: : = IA5String.<br>Значення: https://czo.gov.ua/cps |
| QCStatement | Кваліфікована ознака, яка стверджує, що закритий ключ пов'язаний із сертифікатом відкритого ключа міститься в кваліфікованому засобі створення електронного підпису/печатки (QSCD) | Якщо особистий ключ, згенерований відповідно до ДСТУ 4145–2002, в кваліфікованому засобі створення електронного підпису /печатки (QSCD) та зберігається в такому засобі, в полі OBJECT IDENTIFIER |

Продовження додатка 1

| | | |
|---|---|---|
| | | повинна бути ознака {itu–t(0) identified–organization(4) etsi(0) qc–profile(1862) qcs(1) qcs–QcSSCD(4)} (0.4.0.1862.1.4)<br><br>Якщо особистий ключ, згенерований відповідно до міжнародних алгоритмів і протоколів (RSA ECDSA), визначених ДСТУ ETSI TS 119 312:2022 та зберігається в засобі кваліфікованого електронного підпису, який не є сертифікованим відповідними державними або приватними органами, призначеними державами – членами Європейського Союзу відповідно до статті 30 Регламенту (ЄС) № 910/2014, то в полі OBJECT IDENTIFIER повинна бути ознака {itu–t(0) identified–organization(4) etsi(0) qc–profile(1862) qcs(1) qcs–QcCompliance(1)} (0.4.0.1862.1.1) |

[1] Значення встановлюється у кваліфікованих сертифікатах для відкритих ключів, що згенеровані за криптографічними алгоритмами згідно з ДСТУ ETSI TS 119 312:2022.

[2] Поле встановлюється у кваліфікованих сертифікатах для відкритих ключів, що згенеровані за криптографічними алгоритмами згідно з ДСТУ ETSI TS 119 312:2022.