Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ
АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАКАЗ

20.08.2012 № 1236/5/453

Зареєстровано в Міністерстві юстиції України 20 серпня 2012 р. за № 1398/21710

{Наказ втратив чинність на підставі Наказу Міністерства юстиції № 3563/5/610 від 18.11.2019}

Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису

{Із змінами, внесеними згідно з Наказами Міністерства юстиції
№ 1716/5/667 від 22.11.2012
№ 873/5/269 від 05.06.2014
№ 3354/5/730 від 24.11.2016
№ 1017/5/206 від 29.03.2017
№ 3599/5/618 від 17.11.2017}

На виконання пункту 3 Плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні, затвердженого розпорядженням Кабінету Міністрів України від 26 вересня 2011 року № 1014-р, відповідно до Закону України "Про електронний цифровий підпис", підпунктів 65 і 66 пункту 4 Положення про Міністерство юстиції України, затвердженого Указом Президента України від 06 квітня 2011 року № 395, підпунктів 7 і 11 пункту 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого Указом Президента України від 30 червня 2011 року № 717, та з метою створення умов технологічної сумісності програмно-технічних комплексів акредитованих центрів сертифікації ключів та надійних засобів електронного цифрового підпису **НАКАЗУЄМО:**

1. Затвердити такі, що додаються, вимоги до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису (далі - Вимоги):

1.1. Вимоги до формату посиленого сертифіката відкритого ключа,

1.1. Вимоги до формату кваліфікованого сертифіката відкритого ключа.

1.2. Вимоги до структури об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами.

1.3. Вимоги до формату списку відкликаних сертифікатів.

1.4. Вимоги до формату підписаних даних.

1.5. Вимоги до протоколу фіксування часу.

1.6. Вимоги до протоколу визначення статусу сертифіката.

2. Установити, що:

2.1. Акредитовані центри сертифікації ключів, замовники, розробники, виробники та організації, які експлуатують надійні засоби електронного цифрового підпису в системах електронного документообігу, що створюються на виконання Плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні, затвердженого розпорядженням Кабінету Міністрів України від 26 вересня 2011 року № 1014-р, забезпечують застосування положень Вимог у програмно-технічних комплексах акредитованих центрів сертифікації ключів та надійних засобах електронного цифрового підпису з 31 грудня 2012 року.

2.2. Акредитовані центри сертифікації ключів, замовники, розробники, виробники та організації, які експлуатують надійні засоби електронного цифрового підпису, крім визначених у підпункті 2.1 пункту 2 цього наказу, забезпечують застосування у програмно-технічних комплексах акредитованих центрів сертифікації ключів та надійних засобах електронного цифрового підпису положень Вимог з 01 червня 2013 року.

2.3. Акредитовані центри сертифікації ключів, які здійснили заходи, визначені у підпунктах 2.1, 2.2 пункту 2 цього наказу, надають послуги електронного цифрового підпису з моменту проходження повторної акредитації відповідно до пункту 13 Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903.

2.4. Суб'єкти правових відносин у сфері послуг електронного цифрового підпису, що використовують у своїй діяльності посилені сертифікати відкритих ключів, застосовують електронний цифровий підпис:

1) в межах країни з метою забезпечення електронного документообігу та електронної автентифікації осіб відповідно до:

{Абзац перший підпункту 1 підпункту 2.4 пункту 2 із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

національного стандарту України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31, з функцією гешування за міждержавним стандартом ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 21 жовтня 1997 року № 640. Ці стандарти застосовуються для накладення електронного цифрового підпису до 01 січня 2022 року та для накладення електронного цифрового підпису з метою надання послуг електронного цифрового підпису з перевірки статусу сертифікатів відкритих ключів до завершення терміну їх дії та перевірки електронного цифрового підпису;

{Абзац другий підпункту 1 підпункту 2.4 пункту 2 із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

національного стандарту України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31, з функцією гешування за національним стандартом України ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування», затвердженим наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431. Ці стандарти застосовуються для накладення електронного цифрового підпису з 01 січня 2022 року та для перевірки електронного цифрового підпису;

{Абзац третій підпункту 1 підпункту 2.4 пункту 2 із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від

17.11.2017}

національного стандарту України ДСТУ ISO/IEC 14888-3:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, із застосуванням алгоритму ECDSA зі ступенем розширення основного поля еліптичної кривої не менше 256 з функціями гешування sha256 або sha512 відповідно до FIPS PUB 180-4 «Secure Hash Standard»;

{Підпункт 1 підпункту 2.4 пункту 2 доповнено новим абзацом згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

{Підпункт 2 підпункту 2.4 пункту 2 виключено на підставі Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

2) для транскордонного співробітництва з будь-якою метою відповідно до вимог:

ДСТУ ETSI EN 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 07 вересня 2016 року № 265, та в межах країни з іншою метою, ніж зазначена у підпунктах 1, 2 цього пункту, шляхом застосовування алгоритмів електронного цифрового підпису:

RSA відповідно до RFC 3447 «Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1» з довжиною ключа не менше 4096 бітів з функціями гешування sha256 відповідно до FIPS PUB 180-4;

зазначених у підпункті 1 цього підпункту.

{Абзац четвертий підпункту 2 підпункту 2.4 пункту 2 в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

{Пункт 2 доповнено новим підпунктом 2.4 згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

3. Адміністрації Державної служби спеціального зв’язку та захисту інформації України вжити заходів для впровадження Вимог у програмно-технічних комплексах акредитованих центрів сертифікації ключів та надійних засобах електронного цифрового підпису в строки, визначені у підпунктах 2.1, 2.2 пункту 2 цього наказу.

4. Департаменту нотаріату, банкрутства та функціонування центрального засвідчувального органу Міністерства юстиції України (Чижмарь К.І.) розмістити цей наказ на офіційному веб-сайті Міністерства юстиції України.

5. Цей наказ набирає чинності з дня його офіційного опублікування.

6. Контроль за виконанням цього наказу покласти на заступника Міністра юстиції України Ворону М.Д. та першого заступника Голови Державної служби спеціального зв’язку та захисту інформації України Цуркана О.Г.

Міністр юстиції України **О.В. Лавринович**

Голова Державної служби спеціального зв’язку та захисту інформації України **Г.А. Резніков**

ПОГОДЖЕНО:

В.о. Голови Державної служби України
з питань регуляторної політики
та розвитку підприємництва О.Ю. Потімков

Перший заступник Міністра освіти і науки,
молоді та спорту України Є.М. Суліма

Голова Національної комісії,
що здійснює державне регулювання
у сфері зв’язку та інформатизації П.П. Яцук

ЗАТВЕРДЖЕНО
Наказ Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України
20.08.2012 № 1236/5/453

Зареєстровано в Міністерстві юстиції України
20 серпня 2012 р.
за № 1398/21710

ВИМОГИ
до формату посиленого сертифіката відкритого ключа

I. Загальні положення

1.1. Ці Вимоги визначають формат посиленого сертифіката відкритого ключа (далі - сертифікат).

1.2. Формати даних представлено у нотації ASN.1, визначеній у міжнародному стандарті ISO/IEC 8824 “Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)” / ДСТУ ISO/IEC 8824-3:2008 “Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1)” - частина 3. Специфікація обмежень (ISO/IEC 8824-3:2002, IDT), затвердженому наказом Державного комітету України з питань технічного регулювання та споживчої політики від 26 грудня 2008 року № 508 (із змінами).

1.3. Усі структури даних кодують за правилами DER згідно з міжнародним стандартом 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)” & AMD1:2004 “Support for EX-TENDED-XER”.

1.4. Ці Вимоги засновані на вимогах до змісту сертифіката ключа, встановлених статтею 6 Закону України «Про електронний цифровий підпис», національному стандарті України ДСТУ ISO/IEC 9594-8:2014 «Інформаційні технології. Взаємозв’язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів», затвердженому наказом Міністерства економічного розвитку і торгівлі України від 30 грудня 2014 року № 1493 (далі - ДСТУ ISO/IEC 9594-8:2014), ДСТУ ETSI EN 319 412-1:2016 «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних», затвердженому наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (далі - ДСТУ ETSI EN 319 412-1:2016), Європейських стандартах ETSI EN 319 412-2 V2.1.1 (2016-02) «Electronic

Signaturesand Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificate sissued to natural persons» (далі - ETSI EN 319 412-2), ETSI EN 319 412-3 V1.1.1 (2016-02) «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificate sissued to legal persons» (далі - ETSI EN 319 412-3), ETSI EN 319 412-5 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements» (далі - ETSI EN 319 412-5) та на вимогах до застосування міжнародних криптографічних алгоритмів, встановлених національним стандартом України ДСТУ ETSI EN 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти», затвердженим наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 07 вересня 2016 року № 265 (далі - ДСТУ ETSI EN 119 312:2015).

{Пункт 1.4 розділу I в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

1.5. Ці Вимоги не дублюють стандарт ДСТУ ISO/IEC 9594-8:2006, а описують положення цього стандарту та формати полів. У разі виникнення розбіжностей між положеннями зазначеного стандарту та положеннями цих Вимог застосовуються положення цих Вимог.

1.5^{1}. Для перевірки електронного цифрового підпису, створеного відповідно до національного стандарту України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002), повинен застосовуватися сертифікат відкритого ключа, що відповідає вимогам ДСТУ ISO/IEC 9594-8:2014 та цим Вимогам.

{Абзац перший пункту 1.5^{1} розділу I в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

Для перевірки електронного цифрового підпису, створеного відповідно до алгоритмів ECDSA, визначеного національним стандартом України ДСТУ ISO/IEC 14888-3:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні», затвердженим наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, або RSA, визначеного рекомендаціями RFC 3447 «Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1», повинен застосовуватися сертифікат відкритого ключа, що відповідає вимогам стандартів ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5.

{Абзац другий пункту 1.5^{1} розділу I із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

{Розділ I доповнено новим пунктом 1.5^{1} згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

1.6. Положення цих Вимог є обов’язковими для програмно-технічних комплексів акредитованих центрів сертифікації ключів та надійних засобів електронного цифрового підпису. Правильність реалізації формату посиленого сертифіката відкритого ключа у надійних засобах електронного цифрового підпису підтверджується сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

II. Подання сертифіката для перевірки електронного цифрового підпису в інформаційно-телекомунікаційних системах з метою електронного документообігу та електронної взаємодії інформаційних систем в межах України

{Назва розділу II в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

Сертифікат ключа подається в такому вигляді:

```
Certificate ::= SEQUENCE {
   tbsCertificate          TBSCertificate,
   signatureAlgorithm      AlgorithmIdentifier,
```

signatureValue BIT STRING }

Поле “TBSCertificate” - це частина сертифіката, на яку за допомогою особистого ключа центрального засвідчувального органу, засвідчувального центру, акредитованого центру сертифікації ключів (далі - Центр) накладається електронний цифровий підпис (далі - ЕЦП) за криптографічним алгоритмом (далі - криптоалгоритм), об’єктний ідентифікатор якого міститься у полі “signatureAlgorithm”. Значення ЕЦП містить поле “signatureValue”.

TBSCertificate ::= SEQUENCE {

version	[0] Version,
serialNumber	CertificateSerialNumber,
signature	AlgoritmIdentifier,
issuer	Name,
validity	Validity,
subject	Name,
subjectPublicKeyInfo	SubjectPublicKeyInfo,
issuerUniqueID	[1] IMPLICIT UniqueIdentifier OPTIONAL,
subjectUniqueID	[2] IMPLICIT UniqueIdentifier OPTIONAL,
extensions	[3] EXPLICIT Extensions }

Для усіх строкових даних та полів сертифіката, що мають універсальний тип “DirectoryString”, використовується кодування UTF-8. Для набору символів ASCII може використовуватися кодування PrintableString. Символ “;” використовується як роздільник даних у полі сертифіката.

III. Основні поля сертифіката для перевірки електронного цифрового підпису в інформаційно-телекомунікаційних системах з метою електронного документообігу, електронної взаємодії інформаційних систем та автентифікації в межах України

{Назва розділу III в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

3.1. Основні поля сертифіката наведено в таблиці 1.

Таблиця 1

Назва поля англійською мовою	Назва поля українською мовою
version	номер версії сертифіката
serialNumber	унікальний реєстраційний номер сертифіката
issuer	найменування та реквізити Центру
signature	алгоритм ЕЦП
validity	строк чинності сертифіката
subject	власник сертифіката
subjectPublicKeyInfo	інформація про відкритий ключ підписувача
signatureAlgorithm	найменування криптоалгоритму, що використовується Центром
signatureValue	значення ЕЦП

3.2. Поле “Номер версії сертифіката” (“version”) повинно містити значення “2” (1 байт), яке означає, що формат сертифіката відповідає версії 3 згідно з національним стандартом ДСТУ ISO/IEC 9594-8:2006.

Version ::= INTEGER {v3 (2)}

3.3. Значення поля “Унікальний реєстраційний номер сертифіката” (“serialNumber”) повинно бути додатним цілим числом, розмір якого не перевищує 20 байт (0<serialNumber<2^{160}).

Унікальність реєстраційного номера сертифіката повинна дотримуватися у рамках всіх сертифікатів, сформованих Центром.

CertificateSerialNumber::= INTEGER

3.4. Поле “Найменування та реквізити Центру” (“issuer”) повинно містити найменування та реквізити Центру.

Name ::= CHOICE {

rdnSequence RDNSequence }

RDNSequence::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName::= SET OF AttributeTypeAndValue

AttributeTypeAndValue::= SEQUENCE {

type AttributeType,

value AttributeValue }

AttributeType::= OBJECT IDENTIFIER

AttributeValue::= ANY DEFINED BY AttributeType
DirectoryString::=CHOICE {

printableString PrintableString,

utf8String UTF8String,

bmpString BMPString }

id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt (2) ds (5) 4}

3.5. У полі “Найменування та реквізити Центру” (“issuer”) повинні міститися реквізити Центру, що наведені у таблиці 2.

Таблиця 2

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту	Обов’язковість[1] реквізиту
countryName	назва країни	країна, в якій зареєстрована організація - юридична особа або фізична особа, яка є суб’єктом підприємницької діяльності 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, яка є суб'єктом підприємницької діяльності, за установчими документами або відомостями про державну реєстрацію id-at-organizationName AttributeType ::= {id-at 10} X520organizationName ::= DirectoryString (SIZE (64))	
serialNumber	серійний номер	унікальний реєстраційний номер Центру id-at-serialNumber AttributeType ::= {id-at 5} serialNumber::= PrintableString (SIZE (64)) Значення цього реквізиту задається згідно з підпунктом 3.5.2 цього пункту	+
stateOrProvinceName	назва області[2]	область, у якій зареєстрована організація - юридична особа або фізична особа, яка є суб’єктом підприємницької діяльності id-at-stateOrProvinceName AttributeType ::= {id-at 8} X520stateOrProvinceName ::= DirectoryString (SIZE (64))	+/-
localityName	назва міста	місто, в якому зареєстрована організація - юридична особа або фізична особа, яка є суб’єктом підприємницької діяльності id-at- localityName AttributeType ::= {id-at 7} X520localityName ::= DirectoryString (SIZE (64))	+
commonName	найменування Центру	найменування Центру id-at-commonName AttributeType ::= {id-at 3} X520commonName ::= DirectoryString (SIZE (64))	+
organizationalUnit Name	назва підрозділу організації	назва підрозділу організації, що є Центром та забезпечує надання послуг електронного цифрового підпису id-at-organizationalUnitName AttributeType ::= {id-at 11}	+

		X520 organizationalUnitName ::= DirectoryString (SIZE (64))	

_____

[1]Обов’язковість визначається таким чином:
+ - реквізит обов’язковий;
- - реквізит повинен бути відсутній;
+/- - реквізит може бути присутнім або відсутнім.
[2]Якщо місцем реєстрації юридичної особи або фізичної особи, яка є суб’єктом підприємницької діяльності, є місто Київ або Севастополь, реквізит “stateOrProvinceName” повинен бути відсутнім.

{Таблиця 2 пункту 3.5 розділу III із змінами, внесеними згідно з Наказом Міністерства юстиції № 1716/5/667 від 22.11.2012}

3.5.1. Поля “Найменування та реквізити Центру” (“issuer”) та “Унікальний реєстраційний номер сертифіката” (“serialNumber”) у структурі “TBSCertificate” разом ідентифікують унікальний сертифікат.

3.5.2. Реквізит “Унікальний реєстраційний номер сертифіката” (“serialNumber”) у таблиці 2 містить унікальний реєстраційний номер Центру.

Формування унікального реєстраційного номера здійснюється згідно з нижченаведеними правилами.

Реквізит містить цифри “0”-“9”, великі латинські літери “A”-“Z” та символ “-”;

UA-[Код Установи] {-[Додаток]}, де:

Код Установи - 8, 9 або 10 цифр, що містять код за ЄДРПОУ організації - юридичної особи або реєстраційний номер облікової картки платника податку - фізичної особи, яка є суб'єктом підприємницької діяльності за установчими документами або відомостями про державну реєстрацію;

Додаток - необов’язкова послідовність від 1 до 4 цифр, що містить додаткову частину ідентифікатора. У разі використання Додатка він відокремлюється від реквізиту [Код Установи] символом “-”.

Вищезазначений реквізит шляхом його додавання до розпізнавального імені Центру забезпечує унікальність його розпізнавального імені в межах України. Унікальність цього розпізнавального імені забезпечується центральним засвідчувальним органом.

3.6. Поле “Алгоритм ЕЦП” (“signature”) повинно містити тільки об’єктний ідентифікатор криптоалгоритму, що використовується Центром для накладання електронного цифрового підпису на сертифікат ключа.

```
AlgorithmIdentifier ::= SEQUENCE {

    algorithm       OBJECT IDENTIFIER,

    parameters    ANY DEFINED BY algorithm OPTIONAL }
```

Значення поля “Алгоритм ЕЦП” (“signature”) повинно співпадати із значенням, що міститься у полі “Найменування криптоалгоритму, що використовується Центром” (“signatureAlgorithm”).

Поле “parameters” повинно бути відсутнє.

3.7. Поле “Строк чинності сертифіката” (“validity”) повинно містити значення дати і часу початку та закінчення строку чинності сертифіката.

```
Validity ::= SEQUENCE {

   notBefore        Time,

   notAfter         Time}

Time ::= CHOICE {

   utcTime          UTCTime,
```

generalTime GeneralizedTime}

Поле “Time” зі значенням до 31 грудня 2049 року (включно) кодується у форматі “UTCTime”; починаючи з 01 січня 2050 року - у форматі “GeneralizedTime”.

3.8. Поле “Підписувач” (“subject”) повинно містити реквізити підписувача, що наведені у таблиці 3.

Таблиця 3

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту	Обов’язковість[1] реквізиту для фізичних осіб	Обов’язковість[1] реквізиту для юридичних осіб
countryName	назва країни	країна, в якій зареєстрована організація - юридична особа або фізична особа, що є підписувачем id-at-countryName AttributeType ::= {id-at 6} X520countryName ::= PrintableString (SIZE (2)) код згідно з ISO 3166 (для України - UA)	+	+
commonName	реквізити підписувача	повне (або офіційне скорочене) найменування організації - юридичної особи - підписувача або прізвище ім’я та (за наявності) по батькові фізичної особи - підписувача, що відповідають формату «commonName», визначеному у пункті 3.5 цього розділу	+	+
Surname	прізвище	прізвище підписувача за паспортними даними id-at-surName AttributeType ::= {id-at 4} X520surname ::= DirectoryString (SIZE (64))	+	-
givenName	ім’я та по батькові	ім’я та (за наявності) по батькові підписувача за паспортними даними id-at-givenName AttributeType ::= {id-at 42} X520givenName ::= DirectoryString (SIZE (64))	+	-
serialNumber	серійний номер	унікальний реєстраційний номер підписувача, що надається Центром під час реєстрації підписувача id-at-serialNumber AttributeType ::= {id-at 5} serialNumber ::= PrintableString (SIZE (64))	+	+
organizationName	найменування організації	найменування організації - юридичної особи, що є	-	+

		підписувачем. Відповідає формату «organizationName», визначеному у пункті 3.5 цього розділу		
organizationalUnitName	назва підрозділу організації	назва підрозділу організації, який пов’язаний з фізичною особою-підписувачем. Відповідає формату “organizationalUnitName”, визначеному у пункті 3.5 цього розділу	+/-	+/-
stateOrProvinceName	назва області[2]	область, у якій зареєстрована організація - юридична особа, що є підписувачем, або організація, яка пов’язана з фізичною особою-підписувачем, або область, у якій зареєстрована фізична особа-підписувач. Відповідає формату “stateOrProvinceName”, визначеному у пункті 3.5 цього розділу	+/-	+/-
localityName	назва міста	місто, в якому зареєстрована організація - юридична особа, що є підписувачем, або організація, яка пов’язана з фізичною особою-підписувачем, або місто, в якому зареєстрована фізична особа-підписувач. Відповідає формату “localityName”, визначеному у пункті 3.5 цього розділу	+	+
Title	посада	посада фізичної особи-підписувача в організації id-at-title AttributeType ::= {id-at 12} X520title ::= DirectoryString (SIZE (64))	+/-	-

_____

[1]Обов’язковість визначається таким чином:

\+ - реквізит обов’язковий;

\- - реквізит повинен бути відсутній;

+/- - реквізит може бути присутнім або відсутнім.

[2]Якщо місцем реєстрації юридичної особи є місто Київ або Севастополь, реквізит “stateOrProvinceName” повинен бути відсутнім.

{Таблиця 3 пункту 3.8 розділу III із змінами, внесеними згідно з Наказами Міністерства юстиції № 1017/5/206 від 29.03.2017, № 3599/5/618 від 17.11.2017}

3.8.1. Реквізити юридичної особи-підписувача визначаються в таких атрибутах поля “Підписувач” (“subject”):

organizationName,

countryName,

stateOrProvinceName,

localityName,

commonName.

3.8.2. Реквізити фізичної особи - підписувача (прізвище, ім’я та по батькові за паспортними даними) визначаються в таких атрибутах поля “Підписувач” (“subject”):

commonName,

givenName,

surname.

Обов’язково повинні бути визначені дані в атрибутах “countryName” та “serialNumber” (унікальний реєстраційний номер підписувача).

3.8.3. Реквізити фізичної особи - підписувача, що представляє юридичну особу, визначаються в таких атрибутах поля “Підписувач” (“subject”):

commonName,

givenName,

surname,

organizationName,

organizationalUnitName,

localityName,

stateOrProvinceName,

Title.

Обов’язково повинні бути визначені дані в атрибутах “countryName” та “serialNumber” (унікальний реєстраційний номер підписувача).

{Підпункт 3.8.3 пункту 3.8 розділу III із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

3.8.4. Інші реквізити підписувача можуть бути зазначені у розширеннях (extensions) “Додаткові дані підписувача“ (“subjectAltName”) або “Персональні дані підписувача“ (“subjectDirectoryAttributes”) залежно від типу реквізиту.

3.9. Додаткові дані про підписувача можуть бути зазначені в інших полях згідно з форматом, визначеним у національному стандарті ДСТУ ISO/IEC 9594-8:2006.

3.10. Поле “Інформація про відкритий ключ підписувача” (“subjectPublicKeyInfo”) повинно містити ідентифікатор криптоалгоритму, що використовується підписувачем, а також відкритий ключ, який відповідає особистому ключу підписувача у DER-кодуванні.

```
SubjectPublicKeyInfo ::= SEQUENCE {

   Algorithm            AlgorithmIdentifier,

   subjectPublicKey     BIT STRING }
```

Ідентифікатор криптоалгоритму (поле “AlgorithmIdentifier”) містить об’єктний ідентифікатор (поле “algorithm”) та відповідні параметри криптоалгоритму.

```
AlgorithmIdentifier ::= SEQUENCE {

     algorithm OBJECT IDENTIFIER,

     parameters ANY DEFINED BY algorithm OPTIONAL}
```

Об’єктний ідентифікатор (поле «algorithm») повинен вказувати на криптоалгоритм ДСТУ 4145-2002.

{Абзац дев'ятий пункту 3.10 розділу III в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

{Абзац десятий пункту 3.10 розділу III виключено на підставі Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

{Абзац одинадцятий пункту 3.10 виключено на підставі Наказу

{Абзац обов'язковий пункту 3.10 виключено на підставі Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

Структура параметрів криптоалгоритму (поле “parameters”) та структура відкритого ключа (поле “subjectPublicKey”) визначаються об’єктним ідентифікатором криптоалгоритму.

3.11. Параметри криптоалгоритмів

3.11.1. Параметри криптоалгоритму ДСТУ 4145-2002

```
DSTU4145Params::= SEQUENCE {
  CHOICE {
  ecbinary        ECBinary,                       параметри еліптичної кривої загального виду
  namedCurve      OBJECT IDENTIFIER },            об’єктний ідентифікатор стандартної еліптичної кривої, що рекомендована ДСТУ 4145-2002
  dke             OCTET STRING OPTIONAL }         довгостроковий ключовий елемент (ДКЕ)
ECBinary ::= SEQUENCE {
  version         [0] EXPLICIT INTEGER DEFAULT 0,
  f               BinaryField,                    основне поле
  a               INTEGER (0..1),                 коефіцієнт А еліптичної кривої
  b               OCTET STRING,                   коефіцієнт В еліптичної кривої
  n               INTEGER,                        порядок базової точки (додатне)
  bp              OCTET STRING,                   базова точка еліптичної кривої
BinaryField ::= SEQUENCE {
  m               INTEGER,                        ступінь розширення основного поля
  CHOICE {
  Trinomial,                                      примітивний тричлен
  Pentanomial } OPTIONAL }                        примітивний п’ятичлен
Trinomial ::= INTEGER
Pentanomial::= SEQUENCE {
  k               INTEGER,
  j               INTEGER,
  l               INTEGER }
```

Значення довгострокового ключового елемента (далі - ДКЕ) повинні відповідати правилам постачання ДКЕ, які визначаються Інструкцією про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженою наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованою в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (із змінами) (далі - Інструкція № 114). У разі відсутності ДКЕ як необов’язкового параметра криптоалгоритму повинен використовуватися ДКЕ № 1 із додатка 1 до Інструкції № 114.

Для отримання випадкових даних, необхідних для побудови загальних параметрів криптоалгоритму ДСТУ 4145-2002, використовується генератор

випадкових двійкових послідовностей:

{Підпункт 3.11.1 пункту 3.11 розділу III доповнено новим абзацом згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

відповідно до додатка А до ДСТУ 4145-2002 - у разі застосування геш-функції за ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 21 жовтня 1997 року № 640 (далі - ГОСТ 34.311-95);

{Підпункт 3.11.1 пункту 3.11 розділу III доповнено новим абзацом згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

відповідно до додатка до цих Вимог +- у разі застосування геш-функції за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування», затвердженим наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431 (далі - ДСТУ 7564-2014).

{Підпункт 3.11.1 пункту 3.11 розділу III доповнено новим абзацом згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

Приклади обчислень генератора випадкових двійкових послідовностей розміщуються на офіційному веб-сайті Державної служби спеціального зв'язку та захисту інформації України.

{Підпункт 3.11.1 пункту 3.11 розділу III доповнено новим абзацом згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

3.11.1.1. Допускається кодування полів (розташування внутрішньої послідовності байтів) параметрів еліптичної кривої, що мають тип OCTET STRING, зокрема коефіцієнта B еліптичної кривої, базової точки еліптичної кривої bp, а також відкритого ключа "subjectPublicKey" за двома форматами:

Little-Endian - прямий порядок представлення байтів;

Big-Endian - зворотний порядок представлення байтів (відповідно до правил кодування, визначених в ДСТУ 4145-2002).

3.11.1.2. Об'єктні ідентифікатори для ДСТУ 4145-2002.

3.11.1.2.1. Для формату Little-Endian (при визначенні параметрів еліптичної кривої у сертифікаті):

поліноміальний базис	1.2.804.2.1.1.1.1.3.1.1
оптимальний нормальний базис	1.2.804.2.1.1.1.1.3.1.2.

Для формату Big-Endian:

поліноміальний базис	1.2.804.2.1.1.1.1.3.1.1.1.1
оптимальний нормальний базис	1.2.804.2.1.1.1.1.3.1.2.1.1.

3.11.1.2.2. Використання об'єктних ідентифікаторів, що визначені у пункті 3.11.1.2.1, у полі «subjectPublicKeyInfo» не передбачає будь-яких обмежень щодо використання функції гешування при обчисленні електронного цифрового підпису.

{Підпункт 3.11.1.2 підпункту 3.11.1 пункту 3.11 розділу III в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

3.11.1.3. Базова точка ДСТУ 4145-2002.

Для зображення базової точки використовується формат:

bp OCTET STRING

Базова точка ДСТУ 4145-2002 - це послідовність байтів, яка являє собою елемент основного поля (згідно з пунктом 5.3 ДСТУ 4145-2002), який є стиснутим зображенням (згідно з пунктом 6.9 ДСТУ 4145-2002) точки на еліптичній кривій (залежить від базису, що використовується). Розмір зображення в байтах дорівнює m/8, заокругленому до найближчого цілого у більшу сторону.

3.11.1.4. Коефіцієнт B еліптичної кривої.

Для зображення коефіцієнта B еліптичної кривої згідно з ДСТУ 4145-

2002 використовується формат:

b OCTET STRING

Коефіцієнт B еліптичної кривої ДСТУ 4145-2002 - це послідовність байтів, яка являє собою елемент основного поля (згідно з пунктом 5.3 ДСТУ 4145-2002). Розмір зображення в байтах дорівнює m/8, заокругленому до найближчого цілого у більшу сторону.

3.11.1.5. Відкритий ключ ДСТУ 4145-2002.

Для зображення відкритого ключа згідно з ДСТУ 4145-2002 використовується формат (інкапсульовано у поле “subjectPublicKey”):

PublicKey:: = OCTET STRING

Відкритий ключ ДСТУ 4145-2002 - це послідовність байтів, яка являє собою елемент основного поля (згідно з пунктом 5.3 ДСТУ 4145-2002), який є стиснутим зображенням (згідно з пунктом 6.9 ДСТУ 4145-2002) точки на

еліптичній кривій, що відображає відкритий ключ ЕЦП. Розмір зображення в байтах дорівнює значенню m/8, заокругленому до найближчого цілого у більшу сторону.

3.11.1.6. ЕЦП за ДСТУ 4145-2002.

ЕЦП за ДСТУ 4145-2002 - це рядок октетів OCTET STRING (інкапсульовано у поле “signatureValue”), що містить цифровий підпис, зображений згідно з пунктами 5.7 та 5.10 ДСТУ 4145-2002:

DSTU4145Signature::= OCTET STRING

Для зберігання зображення ЕЦП використовується мінімально можлива довжина зображення для відповідного ступеня m.

{Підпункт 3.11.2 пункту 3.11 розділу III виключено на підставі Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

3.12. ДКЕ - таблиці заповнення вузлів заміни блоків підстановки для алгоритму ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495, який використовується під час генерування псевдовипадкових послідовностей (ДСТУ 4145-2002, додаток А) та обчислення геш-функції ГОСТ 34.311-95.

{Абзац перший пункту 3.12 розділу III в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

Кодування ДКЕ виконується як:

dke OCTET STRING

ДКЕ може кодуватися в розгорнутому або упакованому форматі залежно від алгоритму:

для ДСТУ 4145-2002 - упакований формат.

У разі відсутності ДКЕ в параметрах криптоалгоритму використовується ДКЕ № 1, що наведено у додатку 1 до Інструкції № 114.

{Пункт 3.12 розділу III із змінами, внесеними згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

3.12.1. Упакований формат ДКЕ (масив 64 байт).

Формат розташування елементів ДКЕ - масив фіксованої довжини розміром 64 байт.

ДКЕ - це матриця, що має стовпці K1…K8 (p^1…p^8) по 16 елементів (0…15) у кожному. Порядок розташування елементів:

K1.0, K1.1 … K1.15, K2.0, K2.1 … K2.15, …… K8.0, K8.1 … K8.15

Для блоку підстановки ДКЕ № 1, що наведений у додатку 1 до Інструкції № 114, має вигляд:

	K8	K7	K6	K5	K4	K3	K2	K1
0	1	3	2	F	3	F	8	A
1	2	8	8	8	8	6	0	9
2	3	B	9	E	D	5	C	D

3	E	5	7	9	9	8	4	6
4	6	6	5	7	6	E	9	E
5	D	4	F	2	B	B	6	B
6	B	E	0	0	F	A	7	4
7	8	A	B	D	0	4	B	5
8	F	2	C	C	2	C	2	F
9	A	C	1	6	5	0	3	1
A	C	1	D	1	C	3	1	3
B	5	7	E	5	A	7	F	C
C	7	9	A	B	4	2	5	7
D	9	F	3	4	E	9	E	0
E	0	D	6	3	1	1	A	8
F	4	0	4	A	7	D	D	2

ДКЕ в упакованому форматі (масив 64 байт) має вигляд:

3.12.2. Розгорнутий формат ДКЕ (масив 128 байт).

Формат розташування елементів ДКЕ - масив фіксованої довжини в 128 байт. ДКЕ - це матриця стовпців K1…K8 (p_1…p_8) по 16 елементів (0…15) у кожному. При зберіганні кожний елемент ДКЕ подано 1 байтом, які розташовані в такому порядку (від молодших байтів до старших):

K1.0, K1.1 … K1.15, K2.0, K2.1 … K2.15, …… K8.0, K8.1 … K8.15

Приклад кодування ДКЕ №1, що наведено в додатку 1 до Інструкції № 114, в розгорнутому форматі (масив 128 байт) для блоку підстановки:

3.13. Порядок використання геш-функцій при обчисленні значення електронного цифрового підпису.

3.13.1. Геш-функція може бути обчислена одним з криптоалгоритмів:

ГОСТ 34.311-95;

ДСТУ 7564:2014.

{Абзац третій підпункту 3.13.1 пункту 3.13 розділу III в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

3.13.2. При використанні функції гешування за ГОСТ 34.311-95 під час обчислення електронного цифрового підпису значення стартового вектора H встановлюється рівним 256 нульовим бітам.

3.13.3. При використанні функції гешування за ДСТУ 7564-2014 під час обчислення електронного цифрового підпису рекомендовано застосовувати режими обчислення геш-значення, що визначаються бітовою довжиною порядку базової точки еліптичної кривої та наведені в таблиці 4. Як стартовий вектор геш-функції використовується нульовий вектор. Приклади обчислень електронного цифрового підпису з використанням функції гешування за ДСТУ 7564-2014 розміщуються на офіційному веб-сайті Державної служби спеціального зв’язку та захисту інформації України.

{Абзац перший підпункту 3.13.3 пункту 3.13 розділу III в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

Таблиця 4

Бітова довжина порядку базової точки	**Режим обчислення геш-значення за ДСТУ 7564-2014**

163-383	Режим використання функції гешування з формуванням геш-значення завдовжки 256, 384 або 512 бітів
384-511	Режим використання функції гешування з формуванням геш-значення завдовжки 384 або 512 бітів
>512	Режим використання функції гешування з формуванням геш-значення завдовжки 512 бітів

{Пункт 3.13 розділу III в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

3.14. Порядок кодування окремих параметрів криптографічних алгоритмів.

При кодуванні реквізитів криптографічного алгоритму за ДСТУ 4145-2002 застосовуються такі правила:

{Абзац пункту 3.14 розділу III в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

{Абзац третій пункту 3.14 розділу III виключено на підставі Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

3.14.1. Значення типу “INTEGER”.

Всі значення типу “INTEGER” для алгоритмів ДСТУ 4145-2002 кодуються як цілі числа >=0.

Наприклад, значення для типу “INTEGER” кодуються такою послідовністю байтів:

а) позитивне число 18A3h кодується в DER як послідовність байтів 02 02 18 A3;

б) позитивне число FA10h кодується як послідовність байтів 02 03 00 FA 10 (додається 00 як додатковий старший байт, оскільки старший біт старшого байта FAh дорівнює 1);

в) число 0 кодується в DER як послідовність байтів 02 01 00.

{Підпункт 3.14.1 пункту 3.14 розділу III із змінами, внесеними згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

3.14.2. Кодування двійкових рядків в складі ASN.1-типу OCTET STRING у форматі Little-Endian.

Математичне кодування двійкових рядків (бітових послідовностей) виконується за схемою - молодший байт (що містить менші за номерами біти) за молодшою адресою (ближче до початку потоку).

Біти в байті нумеруються від 0 до 7 за вагою розряду: біт i має вагу 2^i.

Наприклад: біт 0 має вагу 1 (01h), біт 1 має вагу 2 (02h), біт 7 має вагу 128 (80h).

Біт n двійкового рядка кодується як біт i байта j, де i та j обчислюються за формулами:

i = n mod 8,

j = n div 8,

де:

x mod y - операція обчислення залишку від ділення x на y,

x div y - операція ділення x на y із заокругленням до найближчого цілого в меншу сторону.

Якщо кількість бітів у двійковому рядку не кратна 8, біти останнього байта, які не використовуються, мають містити нульове значення.

Наприклад:

бітовий рядок 11100011 кодується як байт E3h;

бітовий рядок 1111000110111 кодується як послідовність байт 37h 1Eh.

3.15. Під час формування електронного цифрового підпису за ДСТУ 4145-2002 з функцією гешування за ДСТУ 7564-2014 як генератор випадкових двійкових послідовностей необхідно застосовувати алгоритм криптографічного перетворення відповідно до національного стандарту України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення», затвердженого наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484, у режимі «Калина-256/256-ECB».

{Розділ III доповнено новим пунктом 3.15 згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

IV. Розширення сертифіката (extensions) для перевірки електронного цифрового підпису в інформаційно-телекомунікаційних системах з метою електронного документообігу та електронної взаємодії інформаційних систем в межах України

{Назва розділу IV в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

4.1. Формат розширень сертифіката має такий вигляд:

Extensions ::= SEQUENCE SIZE (1…MAX) of Extension

Extension ::= SEQUENCE {

extnID OBJECT IDENTIFIER,

critical BOOLEAN DEFAULT FALSE,

extnvalue OCTET STRING}

Базовий об’єктний ідентифікатор розширень сертифіката має такий вигляд:

id-ce OBJECT IDENTIFIER::= {joint-iso-ccitt (2) ds (5) 29}

Сертифікат може містити будь-які додаткові розширення, які не визначені в цьому документі, за умови, що вони визначені як некритичні. Об’єктні ідентифікатори таких розширень повинні бути зареєстровані у встановленому порядку.

4.2. Розширення сертифіката наведені у таблиці 5.

Таблиця 5

Назва поля англійською мовою	Назва поля українською мовою	Обов’язковість[1]
Стандартні розширення сертифіката		
authorityKeyIdentifier	ідентифікатор відкритого ключа Центру	+
subjectKeyIdentifier	ідентифікатор відкритого ключа підписувача	+
keyUsage	призначення відкритого ключа, що міститься в сертифікаті	+
extKeyUsage	уточнене призначення відкритого ключа, що міститься в сертифікаті	+/-
certificatePolicies	політика сертифікації	+
subjectAltName	додаткові дані підписувача	+/-

issuerAlternativeName	додаткові дані Центру	+/-
basicConstraints	основні обмеження	+/-
subjectDirectoryAttributes	персональні дані підписувача	+/-[2]
crlDistributionPoints	точки доступу до списків відкликаних сертифікатів	+
Freshest CRL	точки доступу до часткового списку відкликаних сертифікатів	+/-
Нестандартні розширення сертифіката		
qcStatements	ознаки посиленого сертифіката	+/-

[1] + - розширення обов'язкове;

+/- - розширення може бути присутнім або відсутнім;

[2]- розширення умовно обов'язкове. У разі відсутності інформації про фізичну особу в Єдиному державному демографічному реєстрі та відповідного сформованого запису реквізит, визначений у підпункті 4 пункту 4.12 розділу IV цих Вимог, не зазначається.

{Таблиця 4 пункту 4.2 розділу IV із змінами, внесеними згідно з Наказом Міністерства юстиції № 3354/5/730 від 24.11.2016}

{Пункт 4.2 розділу IV із змінами, внесеними згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

4.3. Розширення "Ідентифікатор відкритого ключа Центру" ("authorityKeyIdentifier") використовується для ідентифікації відкритого ключа, що відповідає особистому ключу, яким підписано сертифікат або список відкликаних сертифікатів.

Об'єктний ідентифікатор даного розширення має такий вигляд:

id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= (id-ce 35)

authorityKeyIdentifier ::= SEQUENCE {

keyIdentifier [0] keyIdentifier

authorityCertIssuer [1] GeneralNames OPTIONAL,

authorityCertSerialNumber [2] CertSerialNumber OPTIONAL}

KeyIdentifier::= OCTET STRING

Атрибут "KeyIdentifier" повинен обов'язково бути присутнім.

Поле "authorityKeyIdentifier" не повинно визначатися як критичне.

4.4. Розширення "Ідентифікатор відкритого ключа підписувача" ("subjectKeyIdentifier") використовується для ідентифікації відкритого ключа, що відповідає особистому ключу, за допомогою якого підписувач здійснює накладання електронного цифрового підпису.

Об'єктний ідентифікатор даного розширення має такий вигляд:

id-ce-subjectIdentifier OBJECT IDENTIFIER :: = (id-ce 14)

SubjectKeyIdentifier ::= KeyIdentifier

Поле "Ідентифікатор відкритого ключа підписувача" ("subjectKeyIdentifier") не повинно визначатися як критичне.

4.5. Обчислення "keyIdentifier" для алгоритмів ДСТУ 4145-2002.

{Абзац перший пункту 4.5 розділу IV із змінами, внесеними згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

Значення “keyIdentifier” в розширеннях “subjectKeyIdentifier” та “authorityKeyIdentifier” обчислюються відповідно засобами ЕЦП підписувача та Центром під час генерації та обробки запиту на формування сертифіката таким чином.

Із кодованого як BIT STRING зображення відкритого ключа вилучаються байт, що містить ознаку типу даних, байти, що містять довжину блоку даних, та байт, що містить число невикористаних бітів.

Обчислюється значення геш-функції згідно з пунктом 3.13 розділу III цих Вимог.

{Абзац четвертий пункту 4.5 розділу IV в редакції Наказу Міністерства юстиції № 1017/5/206 від 29.03.2017}

Якщо параметри криптоалгоритму у полі “Інформація про відкритий ключ підписувача” (“subjectPublicKeyInfo”) містять таблицю заповнення вузлів заміни блоку підстановки (ДКЕ), то при обчисленні геш-функції

використовується саме цей ДКЕ, інакше використовується ДКЕ № 1, що наведений у додатку 1 до Інструкції № 114.

4.6. Розширення “Призначення відкритого ключа” (“keyUsage”) визначає призначення відкритого ключа, що міститься в сертифікаті та повинно визначатися як критичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

id-ce-keyUsage OBJECT IDENTIFIER::= {id-ce 15}

keyUsage::= BIT STRING {

digitalSignature	(0),	електронний цифровий підпис
nonRepudiation	(1),	неспростовність
keyEncipherment	(2),	шифрування з метою транспортування ключа
dataEncipherment	(3),	шифрування даних
keyAgreement	(4),	відкритий ключ використовується в протоколах узгодження ключа
keyCertSign	(5),	електронний цифровий підпис у сертифікаті
crlSign	(6),	електронний цифровий підпис у списку відкликаних сертифікатів
encipherOnly	(7),	якщо біт “keyAgreement” встановлено, відкритий ключ може використовуватися тільки для шифрування даних
decipherOnly	(8)}	якщо біт “keyAgreement” встановлено, відкритий ключ може використовуватися тільки для розшифрування даних

Для сертифіката, що формується підписувачу, повинні бути встановлені біти “digitalSignature” (0) та “nonRepudiation” (1).

Для сертифіката Центру повинні бути встановлені біти “keyCertSign” (5) та “crlSign” (6).

4.7. Розширення “Уточнене призначення відкритого ключа” (“extendedKeyUsage”) може бути визначено як критичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

id-ce-extKeyUsage OBJECT IDENTIFIER::= {id-ce 37}

ExtKeyUsageSyntax ::= SEQUENCE SIZE (1.. MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER

id-kp OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 3}

Для сертифіката Центру, що використовується для перевірки підпису OCSP-відповідей та позначок часу, повинні бути зазначені об’єктні ідентифікатори {id-kp 8} або {id-kp 9}.

id-kp-timeStamping OBJECT IDENTIFIER::= {id-kp 8}	Перевірка позначки часу. Застосовується із встановленим бітом “nonRepudiation” (1) розширення “Призначення відкритого ключа” (“keyUsage”)
id-kp-OCSPSigning OBJECT IDENTIFIER::= {id-kp 9}	Перевірка підпису на відповіді протоколу визначення статусу сертифіката (OCSP-відповіді)

Для сертифіката підписувача, якщо ЕЦП застосовується як електронна печатка, розширення “Уточнене призначення відкритого ключа” (“extendedKeyUsage”) повинно містити об’єктний ідентифікатор 1.2.804.2.1.1.1.3.9.

Для сертифікатів підписувача, які використовуються для перевірки ЕЦП у визначених інформаційно-телекомунікаційних системах, в розширенні “Уточнене призначення відкритого ключа” (“extendedKeyUsage”) можуть використовуватись відповідні об’єктні ідентифікатори за умови, що ці об’єктні ідентифікатори зареєстровані у встановленому порядку.

4.8. Розширення “Політика сертифікації” (“certificatePolicies”) містить посилання на політику сертифікації, відповідно до якої Центр сформував сертифікат. Розширення повинно визначатися як критичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::= {id-ce 32}

anyPolicy OBJECT IDENTIFIER ::= {id-ce-certificatePolicies 0}

    CertificatePolicies::= SEQUENCE SIZE (1.. MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {

    policyIdentifier CertPolicyId,

    policyQualifiers SEQUENCE SIZE (1.. MAX) OF PolicyQualifierInfo
    OPTIONAL}

CertPolicyId ::= OBJECT IDENTIFIER
```

4.9. Розширення “Додаткові дані підписувача” (“subjectAlternativeName”) використовується для розширення межі ідентифікації підписувача (адреса електронної пошти, DNS, IP-адреса, URL).

Об’єктний ідентифікатор даного розширення має такий вигляд:

```
id-ce-subjectAltName OBJECT IDENTIFIER::= {id-ce 17}

SubjectAltName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE (1.. MAX) OF GeneralName

GeneralName ::= CHOICE {

    otherName                       [0] OtherName,

    rfc822Name                      [1] IA5String,

    dNSName                         [2] IA5String,

    x400Address                     [3] ORAddress,

    directoryName                   [4] Name,

    ediPartyName                    [5] EDIPartyName,

    uniformResourceIdentifier       [6] IA5String,

    iPAddress                       [7] OCTET STRING,

    registeredID                    [8] OBJECT IDENTIFIER}
```

OtherName ::= SEQUENCE {

type-id OBJECT IDENTIFIER,

value [0] EXPLICIT ANY DEFINED BY type-id}

EDIPartyName ::= SEQUENCE {

nameAssigner [0] DirectoryString OPTIONAL,

partyName [1] DirectoryString}

4.10. Розширення “Додаткові дані Центру” (“issuerAlternativeName”) дозволяє розширити межі ідентифікації Центру (адреса електронної пошти, DNS, IP-адреса, URL). Розширення повинно бути визначено як некритичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

id-ce-issuerAltName OBJECT IDENTIFIER::= {id-ce 18}

IssuerAltName::= GeneralNames

4.11. Розширення “Основні обмеження” (“basicConstraints”) дозволяє визначити, що сертифікат сформований для Центру або підписувача. Розширення повинно визначатися як критичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

id-ce-basicConstraints OBJECT IDENTIFIER::={idce 19}
BasicConstraints ::= SEQUENCE {

cA BOOLEAN DEFAULT FALSE, cA=TRUE указує, що сертифікат сформований для Центру

cA=FALSE указує, що сертифікат сформований для підписувача

pathLenConstraint INTEGER (0.. MAX) OPTIONAL}

Поле “pathLenConstraint” використовується, якщо поле cA встановлено в TRUE. У цьому разі воно визначає максимально допустиму кількість проміжних сертифікатів, що знаходяться між цим сертифікатом та сертифікатом підписувача.

У сертифікаті акредитованого центру сертифікації ключів розширення “pathLenConstraint” повинно мати значення “0”.

У сертифікаті засвідчувального центру розширення “pathLenConstraint” повинно мати значення “1”.

У сертифікаті центрального засвідчувального органу розширення “pathLenConstraint” повинно мати значення “2”.

4.12. Розширення «Персональні дані підписувача» («subjectDirectoryAttributes») має містити додаткові персональні дані підписувача та бути визначено як некритичне. Поле не використовується для зберігання даних про підписувача, що визначені в полі «subject».

Об’єктний ідентифікатор цього розширення має такий вигляд:

id-ce-subjectDirectoryAttributes OBJECTIDENTIFIER::= {id-ce 9}

SubjectDirectoryAttributes::= SEQUENCESIZE (1.. MAX) OFAttribute

Attribute ::= SEQUENCE {

Type

Attributetype,

Values

SETOFAttributeValue}

Кодування національних реквізитів у розширенні «Персональні дані підписувача» («SubjectDirectoryAttributes») виконується за такими правилами:

1) код за Єдиним державним реєстром підприємств та організацій України юридичної особи - резидента використовується для сертифікатів електронних печаток юридичних осіб - резидентів та для сертифікатів

ключів їх посадових осіб. Для сертифікатів ключів посадових осіб у цьому реквізиті вказується код за Єдиним державним реєстром підприємств та організацій України юридичної особи, представником якої (в межах повноважень) є посадова особа.

{Абзац перший підпункту 1 пункту 4.12 розділу IV із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

Для кодування цього реквізиту використовується об'єктний ідентифікатор 1.2.804.2.1.1.1.11.1.4.2.1. Формат реквізиту - «PrintableString», що містить 8, 9 або 10 цифр;

2) реквізит реєстраційного номера облікової картки платника податків - фізичної особи - резидента використовується для сертифікатів ключів, підписувачами у яких є фізичні особи, у тому числі посадові особи. У цьому реквізиті вказується реєстраційний номер облікової картки платника податків - фізичної особи - підписувача.

Для кодування цього реквізиту використовується об'єктний ідентифікатор 1.2.804.2.1.1.1.11.1.4.1.1. Формат реквізиту - «PrintableString», що містить 10 цифр;

3) для фізичних осіб - резидентів, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті, до реквізитів, яким відповідають об'єктні ідентифікатори 1.2.804.2.1.1.1.11.1.4.1.1 та 1.2.804.2.1.1.1.11.1.4.2.1, вносяться серія (за наявності) та номер паспорта громадянина України. Формат реквізиту - «PrintableString», що містить від 2 до 8 літер серії паспорта (за наявності) та 6 або 9 цифр номера паспорта.

Кодування літерної частини реквізиту здійснюється відповідно до таблиці транслітерації українського алфавіту латиницею, затвердженої постановою Кабінету Міністрів України від 27 січня 2010 року № 55;

4) реквізит унікального номера запису в Єдиному державному демографічному реєстрі використовується для сертифікатів, підписувачами у яких є фізичні особи - резиденти, у тому числі посадові особи. У цьому реквізиті вказується унікальний номер запису в Єдиному державному демографічному реєстрі фізичної особи - підписувача. Для кодування цього реквізиту використовується об'єктний ідентифікатор 1.2.804.2.1.1.1.11.1.4.11.1. Формат реквізиту - «PrintableString», що містить послідовність з 8 цифр, символу «-» та 5 цифр.

{Абзац перший підпункту 4 пункту 4.12 розділу IV із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

Кодування реквізитів у розширенні «Персональні дані підписувача» («SubjectDirectoryAttributes») для юридичних осіб - нерезидентів та фізичних осіб - нерезидентів здійснюється за тими самими правилами з урахуванням особливостей форматів ідентифікаційних даних юридичних осіб та фізичних осіб, прийнятих у державі нерезидента, які підтверджено офіційними документами, наданими підписувачем.

{Пункт 4.12 розділу IV в редакції Наказів Міністерства юстиції № 873/5/269 від 05.06.2014, № 3354/5/730 від 24.11.2016, № 1017/5/206 від 29.03.2017}

4.13. У розширенні "Точки доступу до списків відкликаних сертифікатів" ("CRL Distribution Points") повинна зазначатися принаймні одна загальнодоступна точка розповсюдження списків відкликаних сертифікатів (CRL), яка визначається http (http://) або ldap (ldap://). Розширення не повинно визначатися як критичне.

Об'єктний ідентифікатор даного розширення має такий вигляд:

id-ce-CRLDistributionPoints OBJECT IDENTIFIER::= {id-ce 31}

CRLDistributionPoints ::= SEQUENCE SIZE (1.. MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {

distributionPoint	[0]	DistributionPointName OPTIONAL,
reasons	[1]	ReasonFlags OPTIONAL,
crlIssuer	[2]	GeneralNames OPTIONAL}

DistributionPointName::= CHOICE {

fullName [0] GeneralNames,

nameRelativeToCRLIssuer [1] RelativeDistinguishedName}

ReasonFlags::= BIT STRING {

unused (0),

keyCompromise (1),

cACompromise (2),

affiliationChanged (3),

superseded (4),

cessationOfOperation (5),

certificateHold (6),

privilegeWithdrawn (7)}

Дозволяється використання лише атрибута “distributionPoint” і тільки у форматі URI, який вказує на відповідний CRL.

4.14. Якщо Центр разом із базовим CRL формує і частковий CRL, то посилання на нього вказується у розширенні “Точка доступу до часткового списку відкликаних сертифікатів” (“Freshest CRL”). Розширення не повинно визначатися як критичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

id-ce-freshestCRL OBJECT IDENTIFIER ::= {id-ce 46}

FreshestCRL ::= CRLDistributionPoints

Формування цього розширення здійснюється за правилами формування розширення “Точки доступу до списків відкликаних сертифікатів” (“CRL Distribution Points”).

Це розширення не є обов’язковим. Якщо посилання на частковий CRL не вказується в сертифікаті, то воно обов’язково вказується у відповідному розширенні в структурі базового CRL.

Вимоги щодо формату CRL визначені у Вимогах до формату списку відкликаних сертифікатів, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1400/21712.

4.15. Розширення “Ознаки посиленого сертифіката” (“qualified certificate statement”) повинно бути визначено як критичне.

Об’єктний ідентифікатор даного розширення має такий вигляд:

id-pe OBJECT IDENTIFIER::= {iso(1) identified-organization(3)dod(6)internet(1) security(5) mechanisms(5) pkix(7) pe(1)}

id-pe-qcStatements OBJECT IDENTIFIER::= {id-pe 3}

QCStatements ::= SEQUENCE OF QCStatement

QCStatement ::= SEQUENCE {

statementId OBJECT IDENTIFIER,

statementInfo ANY DEFINED BY statementId OPTIONAL}

4.15.1. Ознака того, що сертифікат сформований як посилений (обов’язкова):

{Абзац перший підпункту 4.15.1 пункту 4.15 розділу IV із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

ua-qcStatement-1 QC-STATEMENT ::= {IDENTIFIED BY id_ua-diglow-qcs-QcCompliance}

id-ua-diglaw-qcs-QcCompliance OBJECT IDENTIFIER ::= {1.2.804.2.1.1.1.2.1}

Для зазначення того, що сертифікат є посиленим, використовується таке заповнення реквізитів сертифіката підписувача:

обов'язково: в розширенні "Політика сертифікації" ("certificate policies") вказується об'єктний ідентифікатор політики посиленої сертифікації 1.2.804.2.1.1.1.2.2, який визначає, що сертифікат сформовано як посилений згідно із Законом України "Про електронний цифровий підпис". Якщо сертифікат підписувача відповідає вимогам додаткових політик сертифікації Центру, у ньому можуть бути вказані додатково об'єктні ідентифікатори цих політик сертифікації;

додатково: може бути присутнім розширення "qualified certificate statement", у якому за допомогою стандартного об'єктного ідентифікатора 1.2.804.2.1.1.1.2.1 ("Qualified certificate statement id-ua-diglow-qcs-QcCompliance") позначено відповідність Закону України "Про електронний цифровий підпис".

14.15.2. Ознака наявності обмеження максимальної суми, на яку вчиняється правочин з використанням електронного цифрового підпису (необов'язкова):

esi4-qcStatement-2 QC-STATEMENT::= {SYNTAX

QcEuLimitValue IDENTIFIED BY id-etsi-qcs-QcLimitValue}

id-etsi-qcs-QcLimitValue OBJECT IDENTIFIER::= {id-etsi-qcs 2}

QcEuLimitValue::= MonetaryValue

MonetaryValue::= SEQUENCE {

currency Iso4217CurrencyCode,

amount INTEGER,

exponent INTEGER}

Iso4217CurrencyCode::= CHOICE {

alphabetic PrintableString (SIZE 3)}.

{Підпункт 4.15.2 пункту 4.15 розділу IV в редакції Наказу Міністерства юстиції № 3599/5/618 від 17.11.2017}

4.15.3. Ознака того, що генерація особистого ключа відбулася з використанням захищеного носія особистого ключа (обов'язкова у випадку використання захищеного носія особистого ключа):

esi4-qcStatement-4 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-QcSSCD}

id-etsi-qcs-QcSSCD OBJECT IDENTIFIER::= {id-etsi-qcs 4}.

{Пункт 4.15 розділу IV доповнено новим підпунктом 4.15.3 згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

V. Подання сертифіката для перевірки електронного цифрового підпису відповідно до міжнародних стандартів

Під час формування сертифікатів відкритих ключів підписувачів повинні використовуватись алгоритми електронного цифрового підпису ECDSA відповідно до національного стандарту ДСТУ ISO/IEC 14888-3:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193, зі ступенем розширення основного поля еліптичної кривої не менше 256 бітів або RSA відповідно до рекомендацій RFC 3447 «Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1».

{Абзац перший розділу V із змінами, внесеними згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

Для обчислення значення геш-функції під час формування сертифікатів відкритих ключів підписувачів повинен використовуватись алгоритм SHA-256 або SHA-512 відповідно до FIPS PUB 180-4 «Secure Hash Standard».

Параметри особистих ключів, які використовуються під час формування сертифікатів відкритих ключів підписувачів, визначаються регламентом роботи центрального засвідчувального органу.

{Вимоги доповнено новим розділом V згідно з Наказом Міністерства юстиції № 1017/5/206 від 29.03.2017}

Директор Департаменту нотаріату, банкрутства та функціонування центрального засвідчувального органу Міністерства юстиції України **К.І. Чижмарь**

Директор Департаменту криптографічного захисту інформації Адміністрації Державної служби спеціального зв’язку та захисту інформації України **А.І. Пушкарьов**

Додаток
до Вимог до формату посиленого
сертифіката відкритого ключа
(підпункт 3.11.1 пункту 3.11 розділу III)

ОПИС
генератора випадкових послідовностей

Робота генератора випадкових двійкових послідовностей (далі - Генератор) базується на вимогах додатка А до національного стандарту України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002), із застосуванням криптографічного перетворення відповідно до національного стандарту України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення», затвердженого наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484 (далі - ДСТУ 7624:2014).

Генератор використовується для отримання випадкових цілих чисел, випадкових елементів основного поля і випадкових точок еліптичних кривих.

Генератор за одне звернення до нього видає випадковий рядок довжини t = 1.

Як криптографічне перетворення в Генераторі застосовується алгоритм криптографічного перетворення згідно з ДСТУ 7624:2014 у режимі «Калина-256/256-ECB» (проста заміна відповідно до розділу 6 ДСТУ 7624:2014).

Умови отримання та використання особистого ключа мають унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення.

Особистий ключ криптографічного перетворення згідно з ДСТУ 7624:2014, що використовується в Генераторі, не можна використовувати для іншої мети.

Позначимо через $E_k(.)$ шифрування двійкового рядка завдовжки 256 двійкових розрядів алгоритмом ДСТУ 7624:2014 в режимі «Калина-256/256-ECB» на ключі k завдовжки 256 двійкових розрядів. Нехай s, I, x - двійкові рядки завдовжки 256 двійкових розрядів, D - двійковий рядок завдовжки 64 двійкові розряди. Перед застосуванням задають початковий стан Генератора випадкових послідовностей.

Встановлення початкового стану Генератора

Встановлення початкового стану Генератора здійснюється за таким алгоритмом:

задають початкове значення s Генератора.

Для цього використовують фізичне джерело випадковості.

Як фізичне джерело випадковості можна використовувати, наприклад, квантові ефекти в напівпровідниках (шумові діоди тощо), сигнал від мікрофонного входу з відключеним мікрофоном, часові інтервали між натисканнями на клавіші клавіатури, часові інтервали між натисканнями на клавіші миші.

Початковий стан Генератора є таємним.

Умови отримання початкового стану Генератора мають унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення;

задають значення двійкового рядка D.

Для цього використовують поточні значення дати і часу з точністю 64 двійкові розряди;

обчислюють двійковий рядок $I = E_k(0^{192} || D)$.

Використання Генератора

При кожному зверненні до Генератора виконують такі обчислення (символ ⊕ позначає порозрядне додавання за модулем 2 двійкових рядків завдовжки 256 двійкових розрядів):

Випадковим двійковим рядком є двійковий рядок довжини 1, який складається з крайнього правого розряду x_0 двійкового рядка $x = (x_{255},...,x_0)$.

{Вимоги доповнено Додатком згідно з Наказом Міністерства юстиції № 3599/5/618 від 17.11.2017}

Програмно-технічна підтримка — Управління комп'ютеризованих систем

Інформаційне наповнення — Відділ баз даних нормативно-правової інформації