ЗАТВЕРДЖЕНО

Наказ
Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України
Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України,
від "11" вересня 2006 р.
№ *99 / 166*

НАЦІОНАЛЬНА СИСТЕМА ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Технічні специфікації форматів представлення базових об'єктів

Зміст

1 Формат посиленого сертифіката відкритого ключа 3

1.1 Загальні положення 3
1.2 Подання сертифіката 3
1.3 Основні поля сертифіката 4
1.4 Розширені поля сертифіката (extensions**)** 14

2 Структура об'єктних ідентифікаторів для криптоалгоритмів, що є національними стандартами 20

2.1 Загальні положення 20
2.2 Структура об'єктних ідентифікаторів 21
2.3 Стандартні еліптичні криві в поліноміальному та оптимальному нормальному базисах 22
2.4 Пояснення 24

3 Формат списку відкликаних сертифікатів 25

3.1 Загальні положення 25
3.2 Подання списку відкликаних сертифікатів 25
3.3 Структура "`TBSCertList`" списку відкликаних сертифікатів 26

1 Формат посиленого сертифіката відкритого ключа

1.1 Загальні положення

1.1.1 Формат посиленого сертифіката відкритого ключа (надалі – сертифіката), наведений у цьому документі, засновується на міжнародному стандарті ISO/IEC 9594-8: "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks" з урахуванням вимог до змісту сертифіката, визначених у Законі України "Про електронний цифровий підпис".

1.1.2 Визначення формату сертифіката не дублює зазначений стандарт, а лише описує особливості змісту сертифіката та форматів його полів. У разі, якщо існують розходження із зазначеним стандартом, використовуються положення, що визначені у цьому документі.

1.1.3 Формат сертифіката описано у нотації ASN.1, визначеній у ISO/IEC 8824 "Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)". Усі структури даних кодують за правилами DER згідно з 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 EXTENDED-XER".

1.2 Подання сертифіката

1.2.1 Сертифікат ключа подається у такому вигляді:

```
Certificate::= SEQUENCE  {
      tbsCertificate          TBSCertificate,
      signatureAlgorithm      AlgorithmIdentifier,
      signatureValue          BIT  STRING}
```

Поле "`TBSCertificate`" – це частина сертифіката, на яку за допомогою особистого ключа центру сертифікації ключів (далі – ЦСК) накладається електронний цифровий підпис за криптографічним алгоритмом (далі – криптоалгоритм), ідентифікатор якого міститься у полі "`signatureAlgorithm`". Значення електронного цифрового підпису 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 тип "`DirectoryString`", використовується універсальне кодування UTF-8 (тип `UTF8String`). Символ ";" використовується в якості роздільника даних у полі сертифіката.

1.3 Основні поля сертифіката

1.3.1 Основні поля сертифіката наведено у таблиці 1.3.1.

Таблиця 1.3.1. Основні поля сертифіката

Назва поля англійською мовою	Назва поля Українською мовою
version	номер версії сертифіката
serialNumber	унікальний реєстраційний номер сертифіката
issuer	найменування та реквізити центру
signature	алгоритм електронного цифрового підпису
validity	строк чинності сертифіката
subject	власник сертифіката
subjectPublicKeyInfo	інформація про відкритий ключ підписувача
signatureAlgorithm	найменування криптографічного алгоритму, що використовується власником особистого ключа
signatureValue	значення електронного цифрового підпису

1.3.2 Поле "Номер версії сертифіката" ("version") повинно містити значення 2 (1 байт), яке означає, що формат сертифіката відповідає версії 3 згідно із стандартом ISO/IEC 9594-8.

```
version::= INTEGER {v3 (2)}
```

1.3.3 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 акредитованим центром.

```
CertificateSerialNumber::= INTEGER
```

1.3.4 Поле "Найменування та реквізити акредитованого центру" ("issuer") повинно містити найменування та реквізити акредитованого 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              AttributeType::= {joint-iso-ccitt (2) ds (5) 4}
```

1.3.5 Реквізити акредитованого центру наведено у таблиці 1.3.2.

Таблиця 1.3.2. Реквізити акредитованого центру

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту	Обов'язковість
countryName	назва країни	країна, в якій зареєстрована організація-юридична особа або фізична особа, яка є суб'єктом підприємницької діяльності, що є акредитованим центром id-at-countryName OBJECT IDENTIFIER:: = {id-at 6} X520countryName::= PrintableString (SIZE (2)) код, згідно з ISO 3166 (для України – UA)	+
organizationName	назва організації	повна назва організації-юридичної особи або фізичної особи, яка є суб'єктом підприємницької діяльності, що є акредитованим центром, за установчими документами або відомостями про державну реєстрацію id-at-organizationName OBJECT IDENTIFIER:: = {id-at 19} X520organizationName::= DirectoryString (SIZE (64))	+
serialNumber	серійний номер	унікальний реєстраційний номер акредитованого центру, id-at-serialNumber OBJECT IDENTIFIER:: = {id-at 5} serialNumber::= PrintableString (SIZE (64)) Значення цього реквізиту задається згідно пункту 1.3.5.3 цього документу.	+
stateOrProvinceName	назва області	область, в якій зареєстрована організація-юридична особа або фізична особа, яка є суб'єктом підприємницької діяльності, що є акредитованим центром id-at- stateOrProvinceName OBJECT IDENTIFIER:: = {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, що є акредитованим центром id-at- localityName OBJECT IDENTIFIER:: = {id-at 7} X520localityName::= DirectoryString (SIZE (64))	+
commonName	повне найменування організації	Реквізити організації-юридичної особи або фізичної особи, яка є суб'єктом підприємницької діяльності, що є акредитованим центром, за установчими документами або відомостями про державну реєстрацію id-at-commonName OBJECT IDENTIFIER::	+

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту	Обов'язковість
		= {id-at 3} X520commonName::= DirectoryString (SIZE (64))	
organizationalUnitName	назва підрозділу організації	Підрозділ організації, що є акредитованим центром та забезпечує надання послуг електронного цифрового підпису id-at-organizationalUnitName OBJECT IDENTIFIER:: = {id-at 11} X520 organizationalUnitName::= DirectoryString (SIZE (64))	+

1.3.5.1 З метою надання додаткової інформації про акредитований центр допускається визначати інші поля згідно з форматом сертифіката, визначеному у стандарті ISO/IEC 9594-8.

1.3.5.2 Поля "issuer" та "serialNumber" у структурі TBSCertificate разом ідентифікують унікальний сертифікат.

1.3.5.3 Реквізит serialNumber у таблиці 1.3.2. містить унікальний реєстраційний номер акредитованого центру, що надається центральним засвідчувальним органом (ЦЗО) під час акредитації центру сертифікації ключів.

Реквізит може містити цифри "0"-"9", та великі латинські літери "A"-"Z" та символ "–".

Значення цього реквізиту може бути погоджено ЦЗО, якщо його сформовано згідно нижченаведених правил (за умови забезпечення його унікальності в межах України):

UA-[КодУстанови]{-[Додаток]}

де:

КодУстанови – 8,9 або 10 цифр, що містять код ЄДРПОУ організації - юридичної особи або код ДРФО фізичної особи – підприємця, яка є суб'єктом підприємницької діяльності, що є центром сертифікації ключів, за установчими документами або відомостями про державну реєстрацію.

Додаток – необов'язкова послідовність від 1 до 4 цифр, що містить додаткову частину ідентифікатора. В разі використання додатку, він відокремлюється від КодуУстанови символом "-".

1.3.6 Поле "Алгоритм електронного цифрового підпису" ("signature") повинно містити тільки ідентифікатор криптоалгоритму, що використовується акредитованим центром для накладання електронного цифрового підпису на сертифікат ключа.

```
AlgorithmIdentifier ::=  SEQUENCE  {
          algorithm     OBJECT IDENTIFIER,
          parameters         ANY DEFINED BY algorithm  OPTIONAL}
```

Значення поля "signature" повинно співпадати із значенням, що міститься у полі "signatureAlgorithm".

1.3.7 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}
```

У сертифікаті ключа, що формується до 2049 року, поле "validity" кодується у форматі UTCTime. Сертифікат ключа, що формується з 2050 року – у форматі GeneralizedTime.

1.3.8 Поле "Власник сертифіката" ("subject") повинно містити основні дані про підписувача-власника особистого ключа, що наведені у таблиці 1.3.3.

Таблиця 1.3.3. Основні дані про підписувача-власника особистого ключа

Назва англійською мовою	Назва українською мовою	Значення	Обов'язковість для фізичних осіб	Обов'язковість для юридичних осіб
countryName	назва країни	країна, в якій зареєстрована організація-юридична особа або фізична особа, що є підписувачем власником особистого ключа id-at-countryName OBJECT IDENTIFIER:: = {id-at 6} X520countryName::= PrintableString (SIZE (2)) код, згідно з ISO 3166 (для України – UA)	+	+
commonName	реквізити підписувача	реквізити підписувача відповідають формату "commonName", визначеному у пункті 1.3.5 цього документу	+	+
surname	прізвище	прізвище підписувача-власника особистого ключа за паспортними даними id-at-surName OBJECT IDENTIFIER:: = {id-at 4} X520surName::= DirectoryString (SIZE (64))	+	-
givenName	ім'я та по-батькові	ім'я та по батькові підписувача-власника особистого ключа за паспортними даними id-at-givenName OBJECT IDENTIFIER:: = {id-at 42} X520givenName::= DirectoryString (SIZE (64))	+	-
serialNumber	серійний номер	унікальний реєстраційний номер підписувача, що надається акредитованим центром під час реєстрації підписувача. id-at-subscriberserialNumber OBJECT IDENTIFIER:: =	+	+

Назва англійською мовою	Назва українською мовою	Значення	Обов'язковість для фізичних осіб	Обов'язковість для юридичних осіб
		{id-at 5} serialNumber::= PrintableString (SIZE (64))		
organizationName	назва організації	назва організації юридичної особи, що є підписувачем, або організації, яка пов'язана з фізичною особою-підписувачем. Відповідає формату "organizationName", визначеному у пункті 1.3.5 цього документу	+\-	+
OrganizationalUnitName	назва підрозділу організації	назва підрозділу організації, який пов'язаний з фізичною особою-підписувачем. Відповідає формату "organizationalUnitName", визначеному у пункті 1.3.5 цього документу	+\-	+\-
stateOrProvinceName	назва області	область, в якій зареєстрована організація-юридична особа, що є підписувачем, або організація, яка пов'язана з фізичною особою-підписувачем, або область, в якій зареєстрована фізична особа- підписувач. Відповідає формату "stateOrProvinceName", визначеному у пункті 1.3.5 цього документу	+	+
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 1.3.5 цього документу	+	+
Title	посада	Посада фізичної особи-підписувача в організації, з якою він пов'язаний id-at-title OBJECT IDENTIFIER:: = {id-at 12} X520title::= DirectoryString (SIZE (64))	+\-	-

Примітки:

+ – атрибут обов'язковий;

Назва англійською мовою	Назва українською мовою	Значення	Обов'язковість для фізичних осіб	Обов'язковість для юридичних осіб
- – атрибут повинен бути відсутній; +\- – атрибут може бути присутнім або відсутнім.				

1.3.8.1 Реквізити юридичної особи підписувача-власника особистого ключа мають бути визначені в наступних атрибутах поля "subject": "organizationName", "countryName", "stateOrProvinceName", "localityName", "commonName". Розширене поле (extensions) "extendedKeyUsage" повинно містити об'єктний ідентифікатор "1.2.804.2.1.1.1.3.9", який вказує, що електронний цифровий підпис застосовується в якості печатки.

1.3.8.2 Реквізити фізичної особи підписувача-власника особистого ключа (прізвище, ім'я та по батькові за паспортними даними) можуть бути визначені в атрибутах поля "subject": "givenName" та "surname" або "commonName". Крім зазначених атрибутів, обов'язково повинні бути визначені дані в атрибутах "countryName" та "serialNumber" (унікальний реєстраційний номер підписувача).

1.3.8.3 Реквізити фізичної особи підписувача - власника особистого ключа, що представляє юридичну особу (або фізичну особу – суб'єкта підприємницької діяльності) можуть бути визначені в атрибутах "givenName", "surname" та "organizationName", "countryName", "stateOrProvinceName", "localityName" і "commonName". Крім зазначених атрибутів, обов'язково повинні бути визначені дані в атрибутах "countryName" та "serialNumber" (унікальний реєстраційний номер підписувача).

1.3.8.4 Інші реквізити підписувача-власника особистого ключа можуть бути зазначені у розширених полях (extensions) "subjectAltName" або "subjectDirectoryAttributes" в залежності від типу реквізиту.

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

1.3.10 Поле "Інформація про відкритий ключ підписувача" ("subjectPublicKeyInfo") повинно містити ідентифікатор криптоалгоритму, що використовується підписувачем, а також відкритий ключ, який відповідає особистому ключу підписувача.

```
SubjectPublicKeyInfo ::=  SEQUENCE  {
          algorithm                 AlgorithmIdentifier,
          subjectPublicKey          BIT STRING}
```

"AlgorithmIdentifier" для ДСТУ 4145-2002 "Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих" та ГОСТ 31.310-95 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма".

```
  AlgorithmIdentifier ::=  SEQUENCE  {
          algorithm          OBJECT IDENTIFIER,
          parameters         ANY DEFINED BY algorithm  OPTIONAL}
```

Поле "parameters" послідовності "AlgorithmIdentifier" містить параметри алгоритму, структура яких визначається ідентифікатором алгоритму, що міститься у полі "algorithm" цієї послідовності.

1.3.11 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               довгостроковий ключовий елемент.
OPTIONAL}
ECBinary  ::= SEQUENCE {
      version            [0] EXPLICIT
INTEGER    DEFAULT 0,
      f     BinaryField,                     основне поле
      a     INTEGER (0..1),                  коефіцієнт A еліптичної кривої
      b     OCTET STRING,                    коефіцієнт B еліптичної кривої
      n     INTEGER,                         порядок базової точки (додатне ціле)
      bp    CHOICE {OCTET STRING,            базова точка еліптичної кривої або ознака її відсутності
NULL}}
BinaryField ::= SEQUENCE {
   m  INTEGER,                               ступінь розширення основного поля
   CHOICE {
              Trinomial,                     примітивний тричлен
              Pentanomial}                   примітивний п'ятичлен
OPTIONAL}
        Trinomial::= INTEGER
        Pentanomial::= SEQUENCE {
           k  INTEGER,
           j  INTEGER,
           l  INTEGER}
```

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

- `Little-Endian` – прямий порядок представлення байтів;
- відповідно до вимог кодування, визначених ДСТУ 4145-2002 (зворотний порядок представлення байтів).

1.3.11.2 Об'єктні ідентифікатори (OID) для ДСТУ 4145 -2002

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 ДСТУ 4145-2002

- 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

1.3.11.3 Базова точка

Для зображення базової точки використовується формат:

```
bp OCTET STRING
```

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

1.3.11.4 Коефіцієнт B еліптичної кривої

Для зображення коефіцієнта B еліптичної кривої згідно 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 п.5.3 ДСТУ 4145). Розмір зображення в байтах дорівнює m/8 заокруглене до найближчого цілого у більшу сторону.

1.3.11.5 Відкритий ключ

Для зображення відкритого ключа згідно ДСТУ 4145-2002 використовується формат (інкапсульовано у `subjectPublicKey`):

```
PublicKey:: = OCTET STRING
```

Відкритий ключ ДСТУ 4145 2002 – це послідовність байтів, яка являє собою елемент основного поля (згідно пункту 5.3 ДСТУ 4145-2002), який є стиснутим зображенням (згідно пункту 6.9 ДСТУ 4145-2002) точки на еліптичній кривій, що відображає відкритий ключ ЕЦП. Розмір зображення в байтах дорівнює m/8 заокруглене до найближчого цілого у більшу сторону.

1.3.11.6 Електронний цифровий підпис ДСТУ 4145-2002

Електронний цифровий підпис ДСТУ 4145-2002 – це рядок октетів `OCTET STRING` (інкапсульовано у полі "`signatureValue`"), що містить цифровий підпис, зображений згідно з пунктами 5.7 та 5.10 ДСТУ 4145-2002.

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

1.3.11.7 Параметри криптографічного алгоритму ГОСТ 34.310-95

```
Gost34310Params::=SEQUENCE  {SEQUENCE {
p INTEGER                                   характеристика основного поля
q INTEGER                                   порядок циклічної підгрупи
a INTEGER}                                  твірний елемент циклічної підгрупи
dke OCTET STRING optional}                  довгостроковий ключовий елемент.
```

1.3.11.8 Об’єктний ідентифікатор (OID) для ГОСТ 34.310-95

Об’єктний ідентифікатор (OID) для ГОСТ 34.310-95 - 1.2.804.2.1.1.1.1.3.2.

1.3.11.9 Відкритий ключ

Для зображення відкритого ключа згідно ГОСТ 34.310-95 використовується наступний формат (інкапсульовано у `subjectPublicKey`):

```
PublicKey:: = INTEGER
```

Відкритий ключ ГОСТ 34.310-95 кодується як ціле.

1.3.11.10 Електронний цифровий підпис

Електронний цифровий підпис згідно ГОСТ 34.310-95 має вигляд (інкапсульовано у полі "signatureValue"):

```
SEQUENCE {
r INTEGER,
s INTEGER
},
```

де r та s обчислюються згідно з ГОСТ 34.310-95, та кодуються як цілі числа.

1.3.12 Таблиці заповнення вузлів заміни блоків підстановки (ДКЕ)

Кодування таблиці заповнення вузлів заміни блоків підстановки довгострокових ключових елементів (далі – ДКЕ) виконується як:

```
dke OCTET STRING
```

Внутрішня послідовність байтів містить ДКЕ в розгорнутому або упакованому форматі, в залежності від стандарту ЕЦП (для ДСТУ 4145-2002 – упакований формат, для ГОСТ 34.310-95 – розгорнутий формат).

1.3.12.1Упакований формат

Формат розташування елементів ДКЕ – масив фіксованої довжини в 64 байти.

ДКЕ – це матриця, що має стовпці K1…K8 (p_1…p_8) по 16 елементів (0…15) в кожному стовпці. Порядок розташування елементів:

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

Елементи розташовуються попарно, утворюючи 64 пари значень.

Кожна пара кодується одним байтом, причому перший елемент пари ДКЕ є старшим напівбайтом, другий елемент пари – молодшим напівбайтом. Наприклад, якщо K1.0 = 4h, а K1.1 = Ah, перший байт масиву ДКЕ буде мати значення 4Ah.

Для блоку підстановки, що наведений у додатку А стандарту ГОСТ 34.311-95 ДКЕ має вигляд:

	K_8	K_7	K_6	K_5	K_4	K_3	K_2	K_1
0	1	D	4	6	7	5	E	4
1	F	B	B	C	D	8	B	A
2	D	4	A	7	A	1	4	9
3	0	1	0	1	1	D	C	2
4	5	3	7	5	0	A	6	D
5	7	F	2	F	8	3	D	8
6	A	5	1	D	9	4	F	0
7	4	9	D	8	F	2	A	E
8	9	0	3	4	E	E	2	6
9	2	A	6	A	4	F	3	B
A	3	E	8	9	6	C	8	1
B	E	7	5	E	C	7	1	C
C	6	6	9	0	B	6	0	7
D	B	8	C	3	2	0	7	F
E	8	2	F	B	5	9	5	5
F	C	C	E	2	3	B	9	3

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

```
4A 92 d8 0e 6b 1c 7f 53
eb 4c 6d fa 23 81 07 59
```

```
58 1d a3 42 ef c7 60 9b
7d a1 08 9f e4 6c b2 53
6c 71 5f d8 4a 9e 03 b2
4b a0 72 1d 36 85 9c fe
db 41 3f 59 0a e7 68 2c
1f d0 57 a4 92 3e 6b 8c
```

1.3.12.2 Розгорнутий формат (128 байт)

Формат розташування елементів ДКЕ – масив фіксованої довжини в 128 байт. ДКЕ – це матриця стовпців `K1…K8 (p1…p8)` по 16 елементів (0…15) у кожному стовпці. При зберіганні, кожний елемент ДКЕ подано 1 байтом, які розташовані у наступному 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 в розгорнутому вигляді (масив 128 байт) для блоку підстановки, що наведено в додатку А стандарту ГОСТ 34.311-95:

```
04 0A 09 02 0d 08 00 0e 06 0b 01 0c 07 0f 05 03
0e 0b 04 0c 06 0d 0f 0a 02 03 08 01 00 07 05 09
05 08 01 0d 0a 03 04 02 0e 0f 0c 07 06 00 09 0b
07 0d 0a 01 00 08 09 0f 0e 04 06 0c 0b 02 05 03
06 0c 07 01 05 0f 0d 08 04 0a 09 0e 00 03 0b 02
04 0b 0a 00 07 02 01 0d 03 06 08 05 09 0c 0f 0e
0d 0b 04 01 03 0f 05 09 00 0a 0e 07 06 08 02 0c
01 0f 0d 00 05 07 0a 04 09 02 03 0e 06 0b 08 0c
```

1.3.13 Стартовий вектор для обчислення значення геш-функції ГОСТ 34.311-95

Для обчислення значення геш-функції використовується алгоритм згідно стандарту ГОСТ 34.311-95. При обчисленні електронного цифрового підпису, значення стартового вектору H функції гешування за ГОСТ 34.311-95 встановлюється рівним 256-ти нульовим бітам.

1.3.14 Порядок кодування окремих параметрів криптографічних алгоритмів

При кодуванні реквізитів криптографічних алгоритмів ДСТУ 4145-2002 та ГОСТ 34.310-95 застосовуються наступні правила:

1.3.14.1Значення типу `INTEGER`

Всі значення типу `INTEGER`, для алгоритмів ДСТУ 4145-2002 та ГОСТ 34.310-95 кодуються як цілі числа >=0.

Наприклад, значення для типу `INTEGER` кодуються наступною послідовністю байтів:

1) позитивне число 18A3h кодується в DER як послідовність байтів 02 02 18 A3;
2) позитивне число FA10h кодується як послідовність байтів 02 03 00 FA 10 (додається 00 як додатковий старший байт, оскільки старший біт старшого байту FAh дорівнює 1);
3) число 0 кодується в DER як послідовність байтів 02 01 00

1.3.14.2 Кодування двійкових рядків, що кодуються в складі DER типу `OCTET STRING` для формату `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

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

Біт *n* двійкового рядку кодується як біт *i* байту *j*, де *i* та *j* обчислюються за формулами:

$i = n \bmod 8$

$j = n$ 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 у меншу сторону.

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

Наприклад:

Бітовий рядок 11100011 кодується як байт E3h

Бітовий рядок 1111000110111 кодується як послідовність байт 37h 1Eh

1.4 Розширені поля сертифіката (extensions)

1.4.1 Формат розширеного поля сертифіката має такий вигляд:

```
Extensions ::=  SEQUENCE  SIZE (1…MAX) of Extension
Extension  ::=  SEQUENCE  SIZE   {
       extnID        OBJECT IDENTIFIER,
       critical      BOOLEAN DEFAULT FALSE,
       extnvalue     OCTET  STRING}
```

Базовий ідентифікатор розширеного поля має такий вигляд:

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

Сертифікат може містити будь-які додаткові розширення, які не визначені у цьому документі, за умови того, що вони визначені як некритичні.

1.4.2 Розширені поля сертифіката наведені у таблиці 1.4.1.

Таблиця 1.4.1. Розширені поля сертифіката

Назва поля англійською мовою	Назва поля українською мовою	Обов'язковість
Стандартні розширені поля		
authorityKeyIdentifier	ідентифікатор відкритого ключа акредитованого центру	+
subjectKeyIdentifier	ідентифікатор відкритого ключа підписувача-власника особистого ключа	+
keyUsage	сфера використання 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 акредитованого центру	+/-
basicConstraints	основні обмеження	+/-
subjectDirectoryAttributes	персональні дані про підписува-	+/-

Назва поля англійською мовою	Назва поля українською мовою	Обов'язковість
	ча	
crlDistributionPoints	точка доступу до списків відкликаних сертифікатів	+/-
Нестандартні розширені поля		
qcStatements	позначка того, що сертифікат сформований як посилений	+/-
Примітки: + – поле обов'язкове; +\- – поле може бути присутнім або відсутнім.		

1.4.3 Поле "Ідентифікатор відкритого ключа акредитованого центру" ("authorityKeyIdentifier") використовується для ідентифікації відкритого ключа, що відповідає особистому ключу, за допомогою якого акредитований центр здійснює накладання електронного цифрового підпису на сертифікат та список відкликаних сертифікатів.

```
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.

1.4.4 Поле "Ідентифікатор відкритого ключа підписувача-власника особистого ключа" ("subjectKeyIdentifier") використовується для ідентифікації відкритого ключа, що відповідає особистому ключу, за допомогою якого підписувач здійснює накладання електронного цифрового підпису.

```
id-ce-subjectIdentifier  OBJECT IDENTIFIER::=   (id-ce 14)
SubjectKeyIdentifier::= KeyIdentifier
```

Поле "subjectKeyIdentifier" не повинно визначатися як критичне.

1.4.5 Обчислення keyIdentifier для алгоритмів ДСТУ 4145-2002 та ГОСТ 34.310-95

Значення keyIdentifier для алгоритмів ДСТУ 4145-2002 та ГОСТ 34.310-95 обчисляються наступним чином.

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

Обчислюється значення геш-функції ГОСТ 34.311-95 від отриманої на попередньому етапі послідовності байтів. В якості стартового вектору геш-функції використовується нульовий вектор. Якщо параметри алгоритму ЕЦП містять таблицю заповнення вузлів заміни блоку підстановки (ДКЕ), то при обчисленні функції гешування використовується саме цей ДКЕ, інакше використовуються ДКЕ, наведений у додатку А ГОСТ 34.311-95.

1.4.6 Поле "Сфера використання відкритого ключа, що міститься в сертифікаті" ("keyUsage") повинно визначатися як критичне.

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

keyUsage::= BIT STRING {	
digitalSignature (0),	електронний цифровий підпис
nonRepudation (1),	неспростовність
keyEncipherment (2),	шифрування з метою транспортування ключа
dataEncipherment (3),	шифрування даних
keyAgreement (4),	відкритий ключ використовується в протоколах погодження 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 "nonRepuduation" (1).

Для сертифіката центру сертифікації ключів повинні бути встановлені біти "keyCertSign" та "crlSign".

1.4.7 Поле "Уточнене призначення відкритого ключа, що міститься в сертифікаті" ("extendedKeyUsage") може бути визначено як критичне або некритичне.

```
id-ce-extKeyUsage OBJECT IDENTIFIER::= {id-ce 37}
    ExtKeyUsageSyntax::= SEQUENCE SIZE (1.. MAX) OF KeyPurposeId
    KeyPurposeId::= OBJECT IDENTIFIER
```

id-kp-timeStamping OBJECT IDENTIFIER::= {id. kp 8}	Позначка часу. Застосовується з встановленим бітом "nonRepudiation" поля "keyUsage"
id-kp-OCSPSigning OBJECT IDENTIFIER::= {id-kp 9}	Підпис OCSP відповідей

Для сертифікату центру сертифікації ключів, що використовується для перевірки OCSP-відповідей та послуги фіксування часу повинно бути зазначені об'єктні ідентифікатори {id. kp 8} та {id-kp 9}.

1.4.8 Поле "Політика сертифікації" ("certificatePolicies") містить посилання на політику сертифікації, відповідно до якої акредитований центр сформував сертифікат, та повинно визначатися як критичне для посиленого сертифікату ключа.

```
id-ce-certificatePolicies OBJECT IDENTIFIER::=  {id-ce 32}
   anyPolicy OBJECT IDENTIFIER::= {id-ce-certificate-policies 0}
   certificatePolicies::= SEQUENCE SIZE (1.. MAX) OF PolicyInformation
   PolicyInformation::= SEQUENCE {
        policyIdentifier  CertPolicyId,
        policyQualifiers  SEQUENCE SIZE (1.. MAX) OF PolicyQualifierInfo OPTIONAL}
   CertPolicyId::= OBJECT IDENTIFIER
```

1.4.9 Поле "Додаткові дані підписувача" ("subjectAlternativeName") використовується для розширення межі ідентифікації підписувача (адреса електронної пошти, DNS, IP адреса, URI).

```
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}
```

1.4.10 Поле "Додаткові дані центру сертифікації ключів" ("issuerAlternativeName") дозволяє розширити межі ідентифікації підписувача (адреса електронної пошти, DNS, IP адреса, URI) та повинно бути визначено як некритичне.

```
id-ce-issuerAltName OBJECT IDENTIFIER::=  {id-ce 18}
   IssuerAltName::= GeneralNames
```

1.4.11 Поле "Основні обмеження" ("basicConstraints") дозволяє визначити, що сертифікат сформований для центру сертифікації ключів або підписувача, повинно визначатися як критичне.

```
id-ce-basicConstraints OBJECT IDENTIFIER::=
{id-ce 19}
BasicConstraints::= SEQUENCE {
ca BOOLEAN DEFAULT FALSE,
```

Ca=TRUE указує, що сертифікат сформований для центру сертифікації ключів

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 кінцевим сертифікатом. У сертифікаті центру сертифікації ключів поле "pathLenConstraint" повинно мати значення "0".

1.4.12 Поле "Персональні дані про підписувача" ("subjectDirectoryAttributes") може містити додаткові персональні дані про підписувача та повинно бути визначено як некритичне. Поле не повинне використовуватись для зберігання даних про підписувача, що визначені в полі "subject".

```
id-ce-subjectDirectoryAttributes  OBJECT IDENTIFIER::=  {id-ce 9}
SubjectDirectoryAttributes::= SEQUENCE SIZE (1.. MAX) OF Attribute
Attribute::= SEQUENCE {
        type                    Attributetype,
        values                  SET OF AttributeValue}
```

1.4.12.1 Кодування національних реквізитів

1.4.12.1.1 Код ЄДРПОУ юридичної особи (код ДРФО фізичної особи – суб'єкта підприємницької діяльності). Цей реквізит використовується для сертифікатів ключів цифрових печаток юридичних осіб та для сертифікатів ключів посадових осіб. Для сертифікатів ключів посадових осіб в цьому реквізиті вказується код юридичної особи (суб'єкта підприємницької діяльності), представником якого (в межах своїх повноважень) є посадова особа. Для кодування цього реквізиту використовується об'єктний ідентифікатор атрибуту – (1.2.804.2.1.1.1.11.1.4.2.1). Формат реквізиту – `PrintableString`, що містить 8,9 або 10 цифр.

1.4.12.1.2 Код ДРФО фізичної особи – підписувача. Цей реквізит використовується для сертифікатів ключів, підписувачем в яких є фізичні особи (зокрема для сертифікатів ключів посадових осіб). В цьому реквізиті вказується код ДРФО підписувача. Для кодування цього реквізиту використовується об'єктний ідентифікатор атрибуту – (1.2.804.2.1.1.1.11.1.4.1.1). Формат реквізиту – `PrintableString`, що містить 10 цифр. Реквізит вказується за бажанням підписувача.

1.4.12.1.3 У випадку, коли підписувач є фізичною особою – суб'єктом підприємницької діяльності, і отримує сертифікат ключа як суб'єкт підприємницької діяльності, якщо в його сертифікаті зазначаються обидва реквізити (згідно пунктів 1.4.12.1.1 та 1.4.12.1.2), значення цих реквізитів мають співпадати.

1.4.13 У полі "Точка доступу до списків відкликаних сертифікатів" ("`CRL Distribution Points`") повинна зазначатися принаймні одна загальнодоступна точка розповсюдження списків відкликаних сертифікатів, яка визначається http (http://) або ldap (ldap://). Поле не повинно визначатися як критичне.

```
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),
   aACompromise                     (8)}
```

В полі дозволено використання лише атрибуту "`distributionPoint`" і тільки у форматі URL який вказує на відповідний перелік відкликаних сертифікатів (CRL).

1.4.14 Поле ("qualified certificate statement"), в разі присутності повинно бути визначено як критичне.

```
id-pe-qcStatements OBJECT IDENTIFIER::= {id-pe  3}
QCStatements::=   SEQUENCE OF QCStatement
QCStatement::=   SEQUENCE {
         statementId         OBJECT IDENTIFIER,
         statementInfo       ANY DEFINED BY statementId OPTIONAL
```

1.4.14.1 Позначка, що сертифікат сформований як посилений:

```
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 наступне заповнення реквізитів сертифіката:

1) Обов'язково: в розширенні "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 Закону України "Про електронний цифровий підпис". Якщо сертифікат задовольняє вимоги додаткових політик сертифікації акредитованого ЦСК, в ньому можуть бути вказані додатково об'єктні ідентифікатори цих політик сертифікації.

2) Додатково: може бути присутнім розширення "qualified certificate statement" в якому за допомогою стандартного об'єктного ідентифікатору "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".

3) У сертифікаті центру сертифікації ключів, що лише зареєстрований ЦЗО, в розширенні "certificate policies" об'єктний ідентифікатор політики посиленої сертифікації "1.2.804.2.1.1.1.2.2" не вказується. Також не повинно бути присутнім розширення "qualified certificate statement" за допомогою стандартного об'єктного ідентифікатору "1.2.804.2.1.1.1.2.1".

1.4.14.2 Інформація про обмеження використання сертифіката

Значення максимальної вартості трансакції, для якої сертифікат може бути використаний:

```
esi4-qcStatement-2 QC-STATEMENT::= {SYNTAX QcEuLimitValue IDENTIFIED BY id-etsi-
qcs-QcLimitValue}
QcEuLimitValue::= MonetaryValue
MonetaryValue::= SEQUENCE {
currency Iso4217CurrencyCode,
amount   INTEGER,
exponent INTEGER}
Iso4217CurrencyCode::= CHOICE {
alphabetic PrintableString (SIZE 3)}
id-etsi-qcs-QcLimitValue OBJECT IDENTIFIER::= {id-etsi-qcs 2}
```

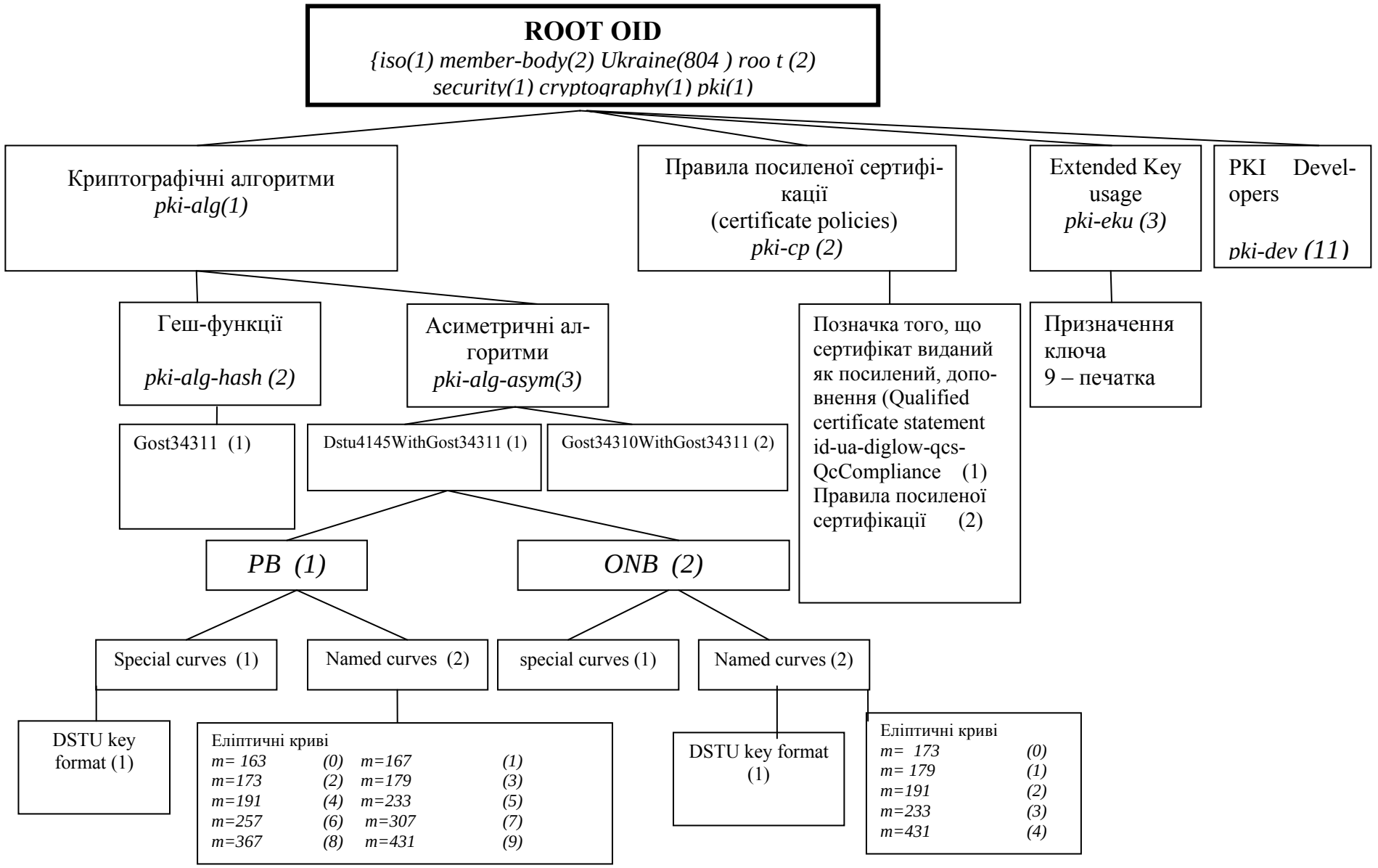
2 Структура об’єктних ідентифікаторів для криптоалгоритмів, що є національними стандартами

2.1 Загальні положення

2.1.1 Структура об’єктних ідентифікаторів (Object identifier – OID) розроблена для забезпечення представлення у сертифікаті криптоалгоритмів, що є національними стандартами їх параметрів, а також інших даних.

2.1.2 Корінь дерева об’єктних ідентифікаторів відповідає значенню, встановленому для України згідно із стандартом ISO 3166 – 804.

2.2 Структура об’єктних ідентифікаторів



2.3 Стандартні еліптичні криві в поліноміальному та оптимальному нормальному базисах

Стандартні еліптичні криві в поліноміальному та оптимальному нормальному базисах наведено відповідно у таблицях 2.1 та 2.2.

Таблиця 2.1. Стандартні еліптичні криві в поліноміальному базисі

Id	Основне поле	Еліптична крива	Базова точка
1	2	3	4
0	(163,3,6,7)	A=1 B=5FF6108462A2DC8210AB403925E638A19C1455D21 n=400000000000000000002BEC12BE2262D39BCF14D	X=2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE Y=3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
1	(167,6,0,0)	A=1 B=6EE3CEEB230811759F20518A0930F1A4315A827DAC n=3FFFFFFFFFFFFFFFFFFFFB12EBCC7D7F29FF7701F	X=7A1F6653786A68192803910A3D30B2A2018B21CD54 Y=5F49EB26781C0EC6B8909156D98ED435E45FD59918
2	(173,1,2,10)	A=0 B=108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9 n=800000000000000000000189B4E67606E3825BB2831	X=4D41A619BCC6EADF0448FA22FAD567A9181D37389CA Y=10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
3	(179,1,2,4)	A=1 B=4A6E0856526436F2F88DD07A341E32D04184572BEB710 n=3FFFFFFFFFFFFFFFFFFFFFB981960435FE5AB64236EF	X=6BA06FE51464B2BD26DC57F48819BA9954667022C7D03 Y=25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
4	(191,9,0,0)	A=1 B=7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03 n=4000000000000000000000069A779CAC1DABC6788F7474F	X=714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129 Y=29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
5	(233,1,4,9)	A=1 B=06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C n=1000000000000000000000000013E974E72F8A6922031D2603CFE0D7	X=3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96 Y=9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35
6	(257,12,0,0)	A=0 B=1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10 n=800000000000000000000000000000006759213AF182E987D3E17714907D470D	X=02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7 Y=10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
7	(307,2,4,8)	A=1 B=393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC079C2F3825DA70D390FBBA588D4604022B7B7	X=216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA Y=5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
8	(367,21,0,0)	A=1 B=43FC8AD242B0B7A6F3D1627AD56597A76413E7BE81A400	X=324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400

Id	Основне поле	Еліптична крива	Базова точка
1	2	3	4
		4447556B47BF6AA4A64 B0C2AFE42CADAB8F93D92394C79A7 9755437B56995136 n=40000000000000000000000000000000 000000000000009C300B7 5A3FA824F22428FD28CE8812245EF440 49B2D49	CA681E09639B5FE12E59A109F78BF4A373 541B3B9A1 Y=1AB597A5B4477F59E39539007C7F977D 1A567B92B043A49C6B6 1984C3FE3481AAF454CD41BA1F05162644 2B3C10
9	(431,1,3,5)	A=1 B=03CE10490F6A708FC26DFE8C3D27 C4F94E690134D5BFF988D8D28AA EAEDE975936C66BAC536B18AE2DC3 12CA493117DAA469C640CAF3 n=3FFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFFFBA 3175458009A8C0A724F02F81AA8A1FC BAF80D90C7A95110504CF	X=1A62BA79D98133A16BBAE7ED9A8E03 C32E0824D57AEF72F889 86874E5AAE49C27BED49A2A95058068426 C2171E99FD3B43C5947C857D Y=70B5E1E14031C1F70BBEFE96BDDE66F 451754B4CA5F48DA241F331A A396B8D1839A855C1769B1EA14BA53308B 5E2723724E090E02DB9

Таблиця 2.2. Стандартні еліптичні криві в оптимальному нормальному базисі

Id	Основне поле	Еліптична крива	Базова точка
1	2	3	4
0	173	A=0 B=043D7E139319F43BA00944915740E1E 6651B06E278C7 n=800000000000000000000189B4E67606E 3825BB2831	X=0A3B8B8D704089B24318CAA51917CB6 E424B4E6DEA56 Y=005A43D5EE1F400349CF35150C74F119 A39145F0CB08
1	179	A=1 B=19C9EBC4FD8308193D3A61762C547C 82F2E6B2182CBCB n=3FFFFFFFFFFFFFFFFFFFFFB9819604 35FE5AB64236EF	X=11F4112265410477159E0D3E39BC4AC4 ADE43B21B66B9 Y=2CA5F0B34C61A86216F13766591CB266 E2819EE582B3C
2	191	A=1 B=13871C9D29D6CEEA740FD57444F72F DBAE559C13A1E31EF8 n=40000000000000000000000069A779CA C1DABC6788F7474F	X=7159E0D3E39BC4AC4ADE43B21B66B94 F2AF25ABEEB1D85D3 Y=57E45D546BE6201E9705E029535D009D3 1F51D81E18226BE
3	233	A=1 B=080F920952A702C75B704A424C018EE A55AA44664F3A003E0962D4F9A8E n=1000000000000000000000000000013E9 74E72F8A6922031D2603CFE0D7	X=0A0823B8ACF069F1CDE256256F21D90 DB35CA795792D5F758E C2E9992FB Y=19DAE222AF326D33AFB7761953F624A2 3D3EB1CA7A1C300F0 AA9953CA85
4	431	A=1 B=53FB7AF7B4407000A6F226AD6BAD2 8378646BD83F1F940810A4C19536 EE65E53F40F973F2F06C5E80EFE3B4365 1BD5FF8B06BA5F9299 n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFFFFFFBA31 75458009A8C0A724F02F81AA8A1FCBAF 80D90C7A95110504CF	X=2020182CFCD7C724157B363D4ABFD4C 16251773C595D4E5C88572F A9D5EBB58142326448C08D3EE3E17E40B8 35D3090DCFBA7C5ADEA6 Y=18E1B6EFB28EEF8A1F9C1859ED57C74 CA747E4E1A60294C005D192 0E80903A432929855828DD7F21714F837E11 9A044987F00110ADAD

2.4 Пояснення

2.4.1 Стандартні криві в поліноміальному базисі взято з таблиці Г.1, а стандартні криві в оптимальному нормальному базисі з таблиці Г.2 ДСТУ 4145 -2002. Додатково наведено базові точки. Зображення еліптичних кривих та базових точок відповідає ДСТУ 4145-2002.

2.4.2 У разі поліноміального базису основне поле зображується відповідно до розділу 5.2 ДСТУ 4145-2002. У разі оптимального нормального базису надається тільки степінь розширення основного поля.

2.4.3 Об’єктний ідентифікатор стандартних еліптичних кривих у поліноміальному базисі має вигляд:

root(1.2.804.2.1.1.1.1) pki-alg(1) pki-alg-asym(3) dstu4145withgost34311(1) pb(1) namedcurve(2) id (0,2, … ,9).

2.4.4 Об’єктний ідентифікатор стандартних еліптичних кривих у оптимальному нормальному базисі має вигляд:

root(1.2.804.2.1.1.1.1) pki-alg(1) pki-alg-asym(3) dstu4145withgost34311(1) onb(2) namedcurve(2) id (0,1,2,3,4).

3 Формат списку відкликаних сертифікатів

3.1 Загальні положення

3.1.1 Формат списку відкликаних сертифікатів (англ. Certificate Revocation List – CRL), представлений у цьому документі, засновується на стандарті ISO/IEC 9594-8. Визначення формату списку відкликаних сертифікатів не дублює зазначений стандарт, а лише описує особливості його змісту та форматів полів. У разі, якщо існують розходження із стандартом, визначеним вище, використовуються положення цього документу.

3.1.2 Формат списку відкликаних сертифікатів описується у нотації ASN.1, що визначена у стандарті ISO/IEC 8824. Кодування усіх структур даних здійснюється за правилами DER згідно з рекомендаціями ITU-T X.690 "Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) ".

3.2 Подання списку відкликаних сертифікатів

3.2.1 Список відкликаних сертифікатів представляється у такому вигляді:

```
CertificateList   ::=  SEQUENCE  {
      tbsCertList            TBSCertList,
      signatureAlgorithm     AlgorithmIdentifier,
      signatureValue         BIT  STRING }
```

Поле "TBSCertList" являє собою частину списку відкликаних сертифікатів, що кодується за правилами DER, на яке за допомогою особистого ключа ЦСК накладається електронний цифровий підпис за криптоалгоритмом, ідентифікатор якого міститься у полі "signatureAlgorithm". Значення електронного цифрового підпису містить поле "signatureValue".

Формат полів "signatureAlgorithm" та "signatureValue" відповідає форматам полів "signatureAlgorithm" та "signatureValue", визначеним для сертифіката у розділі 1 цього документу.

```
TBSCertList ::= SEQUENCE      {
      Version                 Version OPTIONAL,
      signature               AlgoritmIdentifier,
      issuer                  Name,
      thisUpdate              Time,
      nextUpdate              Time OPTIONAL,

      revokedCertificates     SEQUENCE OF SEQUENCE  {
           userCertificates          CertificatesSerialnumber,
           revocationDate            Time,
           crlEntryExtensions        Extensions OPTIONAL   }  OPTIONAL,

      CrlExtensions           [0]    EXPLICIT Extensions OPTIONAL }
```

3.3 Структура "TBSCertList" списку відкликаних сертифікатів

3.3.1 Структуру "TBSCertList" наведено у таблиці 3.1.

Таблиця 3.1. Структура "TBSCertList"

Назва поля англійською мовою	Назва поля українською мовою
Інформаційні поля про CRL	
version	номер версії
signature	алгоритм електронного цифрового підпису
issuer	реквізити акредитованого центру
thisUpdate	час формування списку відкликаних сертифікатів
nextUpdate	час наступного формування списку відкликаних сертифікатів
Елементи CRL, що містять інформацію про скасовані, блоковані та поновлені сертифікати (revokedCertificates)	
revokedCertificates	елементи списку відкликаних сертифікатів
userCertificate	унікальний реєстраційний номер сертифіката
revocationDate	час відкликання сертифіката
Розширені поля елементів CRL (crlEntryExtension)	
CRLReasons	причини відкликання сертифіката
invalidityDate	час компрометації особистого ключа
Розширені поля списку відкликаних сертифікатів (crlExtensions)	
authorityKeyIdentifier	ідентифікатор відкритого ключа акредитованого центру
CRLNumber	серійний номер списку відкликаних сертифікатів

3.3.2 Поле "Номер версії" ("version") містить значення 1 (1 байт), яке означає, що формат списку відкликаних сертифікатів відповідає версії 2 згідно із стандартом ISO/IEC 9594-8.

3.3.3 Поле "Алгоритм електронного цифрового підпису" ("signature") містить тільки ідентифікатор криптоалгоритму, що використовується акредитованим центром для накладання електронного цифрового підпису на список відкликаних сертифікатів.

Формат поля "signature" відповідає формату поля "signature", визначеному для сертифіката та наведеному у розділі 1 цього документу. Значення поля "signature" повинно збігатися з даними, що містяться у полі "signatureAlgorithm".

3.3.4 Поле "Реквізити акредитованого центру" ("issuer") містить найменування та реквізити акредитованого центру, який сформував CRL.

Формат поля "issuer" відповідає формату поля "issuer", визначеному для сертифіката та наведеному у розділі 1 цього документу.

3.3.5 Поле "Час формування списку відкликаних сертифікатів" ("thisUpdate") містить дату і час формування акредитованим центром списку відкликаних сертифікатів.

Формат поля "thisUpdate" відповідає формату поля "validity", визначеному для сертифіката та наведеному у розділі 1 цього документу.

3.3.6 Поле "Час наступного формування списку відкликаних сертифікатів" ("nextUpdate") містить дату і час наступного формування акредитованим центром списку відкликаних сертифікатів.

3.3.7 Поле "Елементи списку відкликаних сертифікатів" ("revokedCertificates") містить інформацію про скасовані, блоковані та поновлені сертифікати.

3.3.8 Формат поля "Унікальний реєстраційний номер сертифіката" ("userCertificate") повинен відповідати формату поля "serialNumber", визначеному для сертифіката та наведеному у розділі 1 цього документу.

3.3.9 Поле "Час відкликання сертифіката" ("revocationDate") містить дату і час відкликання (скасування, блокування та доповнення) сертифіката.

Формат поля "revocationDate" відповідає формату поля "validity", визначеному для сертифіката та наведеному у розділі 1 цього документу.

3.3.10 Поле "Причини відкликання сертифіката" ("CRLReasons") не повинно бути визначено як критичне.

```
id-ce-crlReasons     OBJECT IDENTIFIER ::= {id-ce 21}
```

Коди причин відкликання сертифіката для поля "CRLReason":

```
::= ENUMERATED {
unspecified     (0),          точно не визначено
keyCompromise   (1),          компрометація особистого ключа
cACompromise    (2),          компрометація особистого ключа акредитованого центру
affiliationChanged(3),        зміна даних про підписувача
superseded      (4),          сертифікат ключа замінений
cessationOfOperation(5),      закінчення строку чинності сертифіката
certificateHold (6),          сертифікат ключа блоковано
removeFromCRL   (8) }         сертифікат ключа поновлено
```

3.3.11 Поле "Час компрометації особистого ключа" ("invalidityDate") не повинно бути визначено як критичне.

```
id-ce-invalidityDate OBJECT IDENTIFIER ::= { id-ce 24 }
invalidityDate ::=  GeneralizedTime
```

3.3.12 Поле "Ідентифікатор відкритого ключа акредитованого центру" "authorityKeyIdentifier" використовується для ідентифікації відкритого ключа, що відповідає особистому ключу, за допомогою якого акредитований центр здійснює накладання електронного цифрового підпису на список відкликаних сертифікатів.

Формат поля відповідає формату поля "authoritykeyidentifier", визначеному для сертифіката у розділі 1 цього документу.

Зазначене поле не повинно бути визначено як критичне.

3.3.13 Поле "Серійний номер списку відкликаних сертифікатів" ("CRLNumber") не повинно бути визначено як критичне, а його значення повинно бути додатним цілим числом, що не перевищує 20 байт ($1 <= CRLnumber < 2^{160}$).

```
id-ce- OBJECT IDENTIFIER ::=  { id-ce 20 }
CRLNumber  ::= INTEGER (0…MAX).
```