

1.2.3 Способ использования ключа субъекта (keyUsage)

Это расширение определяет способ использования ключа, например ключ обеспечивающий секретность, ключ для замены ключей, ключ для подписывания и т.д.

Допустимы различные комбинации применения одного и того же ключа. Но не все возможные комбинации битов разрешаются.

Выбор разрешенных комбинаций битов особенно зависит от типа алгоритма открытого ключа.

```
id-ce-keyUsage OBJECT IDENTIFIER ::= { id-ce 15 }
KeyUsage ::= BIT STRING {
    digitalSignature      (0), -- klucz do realizacji podpisu elektronicznego
    nonRepudiation       (1), -- klucz związany z realizacją usług
                        -- niezaprzeczalności
    keyEncipherment      (2), -- klucz do wymiany kluczy
    dataEncipherment     (3), -- klucz do szyfrowania danych
    keyAgreement         (4), -- klucz do uzgadniania kluczy
    keyCertSign          (5), -- klucz do podpisywania certyfikatów i
                        -- zaświadczeń certyfikacyjnych
    CRLSign              (6), -- klucz do podpisywania list CRL
    encipherOnly         (7), -- klucz tylko do szyfrowania
    decipherOnly         (8) -- klucz tylko do deszyfrowania }
```

(Объяснение переводчика:

- (0), -- ключ для нанесения электронной подписи,
- (1), -- ключ связанный с реализацией услуг неопровергаемости,
- (2), -- ключ для обмена ключей,
- (3), -- ключ для шифрования данных,
- (4), -- ключ для согласования ключей ,
- (5), -- ключ для подписи сертификатов и сертификационных засвидетельствований,
- (6), -- ключ только для шифрования ,
- (7), -- ключ только для расшифровки,)

Использование отдельных битов в поле **keyUsage** должно соответствовать следующими принципами (установленный бит соответственно обозначает) :

- a) **digitalSignature**: предназначение сертификата до реализации услуг удостоверения при помощи электронной подписи в иных целях чем определено в п/п b,f и g ;
- b) **nonRepudiation**: предназначение сертификата для обеспечения несомненности подписи поставленных физическими лицами,но и одновременно для иных целей,чем определены в п/п f и g . Бит nonRepudiation может содержаться только в квалифицированных сертификатах открытых ключей пользователей, служащих для проверки безопасной электронной подписи и не может быть объединен с иными предназначениями, в особенности, о которых говорится в пунктах с-е, связанных с обеспечением секретности.
- c) **keyEncipherment**: для кодирования ключей симметричных алгоритмов обеспечивающих секретность данных,

Распоряжение Совета Министров от 7 августа 2002 г. Приложения

- d) **dataEncipherment**: для кодирования данных пользователя, иных чем определено в п. “с” и “е”,
- e) **keyAgreement**: для протоколов согласования ключа,
- f) **keyCertSing**: открытый ключ употребляемый для проверки электронных удостоверений в сертификатах и электронных засвидетельствованиях выданных квалифицированными субъектами предоставляющими сертификационные услуги,
- g) **cRLSign**: открытый ключ применяемый для проверки электронных удостоверений в списках аннулированных и приостановленных сертификатов и в списках аннулированных и приостановленных сертификационных засвидетельствований выданных квалифицированным субъектом предоставляющим сертификационные услуги,
- h) **encipherOnly**: может быть использован только с битом **keyAgreement** для указания, что служит только для шифрования данных в протоколах согласования ключа.
- i) **decipherOnly**: может быть использован только с битом **keyAgreement** для указания, что служит только для расшифрования данных в протоколах согласования ключа.

Отсутствие установления какого-либо из вышеперечисленных битов свидетельствует об использовании сертификата в иных целях чем предусмотрено в п/п. а-і.

Расширение является критическим.

1.2.4 Расширение уточняющее сферу применения сертификата **extKeyUsage**

Это поле необходимо интерпретировать как сокращение допустимой сферы применения ключа, указанного в поле **keyUsage**.

Это расширение является критическим, обозначает это, что сертификат должен быть использован только в указанном диапазоне применения .

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

В особенности сформулировано следующую сферу применения:

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

id-kp OBJECT IDENTIFIER ::= [ id-pkix 3 ]
id-kp-dvcs OBJECT IDENTIFIER ::= { id-kp 10 }
-- podpisywanie dokumentów elektronicznych przez urząd notarialny w
oparciu o
-- protokół DVCS; bity pola keyUsage, które są zgodne z tym polem:
-- digitalSignature
```

Распоряжение Совета Министров от 7 августа 2002 г. Приложения

(Объяснение переводчика: подписывание электронных документов нотариальным центром полагаясь на протокол DVCS; биты поля *keyUsage*, которые согласны с этим полем: *digitalSignature*)

1.2.5 Политика сертификации (certificatePolicies)

Расширение определяющее политику сертификации содержит последовательность одной либо нескольких политик сертификации определяющих условия предоставления сертификационных услуг квалифицированным субъектом.

```
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
PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId PolicyQualifierId,
    PolicyQualifierId ::= OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )
}
Qualifier ::= CHOICE {
    cpsuri CPSuri,
    userNotice UserNotice }

CPSuri ::= IA5String
UserNotice ::= SEQUENCE {
    noticeRef NoticeReference OPTIONAL,
    explicitText DisplayText OPTIONAL }

NoticeReference ::= SEQUENCE {
    organization DisplayText,
    noticeNumbers SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
    visibleString VisibleString (SIZE (1..200)),
    bmpString BMPString (SIZE (1..200)),
    utf8String UTF8String (SIZE (1..200)) }
```

Расширение является критическим.

1.2.6 Альтернативное название субъекта(subjectAltName)

Это расширение предоставляет возможность формулировки иного названия субъекта, которому выдаётся сертификат.