

Додаток
до Вимог до форматів
контейнерів зберігання особистих
ключів електронного цифрового
підпису, особистих
ключів шифрування та сертифікатів
відкритих ключів
(підпункт 4 пункту 4
розділу IV, пункт 8 розділу V)

ПРИКЛАДИ

ASN.1 структури контейнера зберігання особистих ключів та сертифікатів

Приклад 1. Контейнер зберігання особистого ключа та сертифіката

Пароль – «password».

```
SEQUENCE :
  INTEGER : 3
  SEQUENCE :
    OBJECT IDENTIFIER : data [1.2.840.113549.1.7.1]
    CONTEXT SPECIFIC (0) :
      OCTET STRING :
        SEQUENCE :
          SEQUENCE :
            OBJECT IDENTIFIER : data [1.2.840.113549.1.7.1]
            CONTEXT SPECIFIC (0) :
              OCTET STRING :
                SEQUENCE :
                  SEQUENCE :
                    OBJECT IDENTIFIER :
                    pkcs-12-pkcs-8ShroudedKeyBag [1.2.840.113549.1.12.10.1.2]
                    CONTEXT SPECIFIC (0) :
                      SEQUENCE :
                        SEQUENCE :
                          OBJECT IDENTIFIER :
                          id-PBES2 [1.2.840.113549.1.5.13]
                          SEQUENCE :
                            SEQUENCE :
                              OBJECT IDENTIFIER :
                              id-PBKDF2 [1.2.840.113549.1.5.12]
                              SEQUENCE :
                                OCTET STRING :
```

31A58DC1462981189CF6C701E27
6C7553A5AB5F6E36D8418E4AA40
C930CF3876
INTEGER : 10000
SEQUENCE :
OBJECT IDENTIFIER :
id-hmacGost34311 [1.2.804.2.1.1.1.1.2]
NULL :
SEQUENCE :
OBJECT IDENTIFIER :
id-gost28147-cfb [1.2.804.2.1.1.1.1.1.3]
SEQUENCE :
OCTET STRING :
4BB10F5C2945D49E
OCTET STRING :
A9D6EB45F13C708280
C4967B231F5EADF658
EBA4C037291D38D96B
F025CA4E17F8E9720D
C615B43A28975F0BC1
DEA36438B564EA2C17
9FD0123E6DB8FAC579
04
OCTET STRING :
29A22E2951E632E1E444A
E38F521C890FF6377FC05
39113A66720BFC4E9107C
566A07E3EAB9AE67F337E
D9C66C021363E79508A9F
DFA09E78877DFBE765431
60DC83195427A9C7FF2F6
F40D8D0FEA26583C72EF6
E5E2045DA9512A61FBC2B
9573E8B0BDC8F034D8CDA
3ACA63B78C9877FA75C22
8756BE76083A235247A09
4C1EF2996FFBFCB45E6D1
4807B38E26A8626103513
1DEC63B37307B44EF2C0E
AFE51392CD8A2B8B50FC6
F8BC8B1A62EFD276D4E81
BB358F4931BAAA3660C0C
0B5DF52E5233D90D1F4EF

5203C40F036CF59129146
 60BF28212C9B3FD9141CB
 89B93C13522DEB33085A2
 5CC102B5B7DBA377078A6
 45E88

SEQUENCE :

OBJECT IDENTIFIER : encryptedData [1.2.840.113549.1.7.6]

CONTEXT SPECIFIC (0) :

SEQUENCE :

INTEGER : 0

SEQUENCE :

OBJECT IDENTIFIER : data [1.2.840.113549.1.7.1]

SEQUENCE :

OBJECT IDENTIFIER : id-PBES2 [1.2.840.113549.1.5.13]

SEQUENCE :

SEQUENCE :

OBJECT IDENTIFIER :

id-PBKDF2 [1.2.840.113549.1.5.12]

SEQUENCE :

OCTET STRING :

9F93C3D9B8CB403374

434DA22DFFC397488C

A2251FEB8E9DA65E64

5E594BCEC0

INTEGER : 10000

SEQUENCE :

OBJECT IDENTIFIER :

id-hmacGost34311 [1.2.804.2.1.1.1.1.2]

NULL :

SEQUENCE :

OBJECT IDENTIFIER :

id-gost28147-cfb [1.2.804.2.1.1.1.1.1.3]

SEQUENCE :

OCTET STRING :

9F11E6430C51E266

OCTET STRING :

A9D6EB45F13C708280

C4967B231F5EADF658

EBA4C037291D38D96B

F025CA4E17F8E9720D

C615B43A28975F0BC1

DEA36438B564EA2C17

9FD0123E6DB8FAC579

04

CONTEXT SPECIFIC (0) :

3B6BAC1A6C39CC80A25616FC6987A3
1EAF44E4E0D145C7B5F15B218EDA74
FCF85D8A4FF456F91DF60F170FA10B
288040E7E29759ED8076A16ABE21B7
73DA361DC04B0650A7E17981F98C4C
D35E2DAD6FCA1DA147D0983450E4F1
43E2B1CD1E3303B10AAEF1419EE174
2EC79CD41CE771ABFDC5B0CB4ADAEC
ED2586B311154BB19A2A141E1642E2
72B9DA853D1E627A003F8562571F8E
42B05CBAF2B243C9DCDBE344DB3206
7E40600BC60E958C397599F5DF47AB
92B4B62FFC9133BD460C4D52692D03
068A6058A543E4731654752037EED7
A73947E9E83BC5A74844C067712E03
2D137200FFBD9BEFDF68D559025AA5
C717FE259D8D9597A805872BF20884
0F888831AAF4213302CFFC237609BF
7AE51BC71A24CBB6C6DB03AC1F7A59
20109D410152E74A8C27DCCAEA688C
E46FF75481E8B3C1AE90EDA6B7B663
3D3AAAFAFDCA080D96F8BC600831D1
AF6F617781400188F301D69A716B08
012FB57276B4EA5A844D39A71888A7
058F47E52C5FAAC4FAC16201CFEAF9
811535FEC0FA7439A247DAFC611891
02FD00E3B340F4D1C61A18C082BDC4
700749AC609CD5532E2E295BA0302E
7E59C2A3E12B95F9EE5D90BB9DBB66
F7A9ADD26733C26A44105678342773
6F83B53B7531CCF009499FA14931FB
3F7859684B2520636CDBC4BAF6D126
8459156BCFB912DF26CE4A8224E627
072D92F20DEC249A5F27EDA67C1A39
23F5E75CA24355388E828B04FC69D3
BF08CBC4B68DA598DAA7A1665ACADE
F470E3D712E0E13E47108F06D009B1
9CB4A6131797F741B09A899EFAFED5
3FC7344064FB17676F50AE7ACBF33C
FEF973CBD7403FA3D77BF280368F97
E5AF489BB26DDC4CFFE2B821235400

8A07CB1DA400BC6B2BD3CD098FE0E2
 29D69C2C1E2103600BFFB5B459743E
 C775FC87888EF945DDE5F2D33F97D9
 2CA665FACB9EDCFC2B146E70DC0808
 02174C2F293C27E2B2819EBA82DAE7
 5F7B989E887FE9539CC5F041F1E916
 94D81DFBCC3E4945004CA962270435
 2E483E8238146C88E312C0E7C1EC14
 7A9DBB642752330ED08115606B8EB3
 1212FE29AE858BF26F8F2AEB289A0B
 36CCFA405BBA8A2F067456A2B8A5BA
 77D4BDBC0D0004C4DE6896A6A2D9E1
 B4ACCB3799129D17F46696E2994AE5
 877539761308DF7B45D2D95DB2EAC9
 D7B75EC7BF11A1AC8502CDC111D004
 16405404BB2DDB38DF37B3F6740DCF
 6647CAEB7E9FDDEBE798A87E8A5A97
 4E0730C1495E6345BE934103E6

SEQUENCE :

SEQUENCE :

SEQUENCE :

OBJECT IDENTIFIER : [1.2.804.2.1.1.1.2.1]

NULL :

OCTET STRING :

9DD623DE32AB6A09B16C442D8F34195F02182F3ED34FD09E

76F817FB648E725A

OCTET STRING :

EAB98DB1A017DF6613BCBD87501FCE27A21EC76EF00DD8DF00D

229A53B0BB67C

INTEGER : 10000

Приклад 2. Приклад структури «SafeContents»

Пароль – «password».

SEQUENCE :

SEQUENCE :

OBJECT IDENTIFIER :

pkcs-12-pkcs-8ShroudedKeyBag [1.2.840.113549.1.12.10.1.2]

CONTEXT SPECIFIC (0) :

SEQUENCE :

SEQUENCE :

CONTEXT SPECIFIC (0) :

INTEGER : 2

INTEGER :

68E9687A597F245F01000000010000002A000000

SEQUENCE :

OBJECT IDENTIFIER : id-dstu4145PB [1.2.804.2.1.1.1.3.1.1]

SEQUENCE :

SET :

SEQUENCE :

OBJECT IDENTIFIER : organizationName [2.5.4.10]

UTF8 STRING : 'Організація'

SET :

SEQUENCE :

OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]

UTF8 STRING : 'Підрозділ'

SET :

SEQUENCE :

OBJECT IDENTIFIER : commonName [2.5.4.3]

UTF8 STRING : 'ЦСК'

SET :

SEQUENCE :

OBJECT IDENTIFIER : serialNumber [2.5.4.5]

UTF8 STRING : 'UA-01'

SET :

SEQUENCE :

OBJECT IDENTIFIER : countryName [2.5.4.6]

PRINTABLE STRING : 'UA'

SET :

SEQUENCE :

OBJECT IDENTIFIER : localityName [2.5.4.7]

UTF8 STRING : 'Київ'

SEQUENCE :

```

UTC TIME : '131001210000Z'
UTC TIME : '181001210000Z'
SEQUENCE :
SET :
    SEQUENCE :
        OBJECT IDENTIFIER : organizationName [2.5.4.10]
        UTF8 STRING : 'Організація'
SET :
    SEQUENCE :
        OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
        UTF8 STRING : 'Підрозділ'
SET :
    SEQUENCE :
        OBJECT IDENTIFIER : commonName [2.5.4.3]
        UTF8 STRING : 'ЦСК'
SET :
    SEQUENCE :
        OBJECT IDENTIFIER : serialNumber [2.5.4.5]
        UTF8 STRING : 'UA-01'
SET :
    SEQUENCE :
        OBJECT IDENTIFIER : countryName [2.5.4.6]
        PRINTABLE STRING : 'UA'
SET :
    SEQUENCE :
        OBJECT IDENTIFIER : localityName [2.5.4.7]
        UTF8 STRING : 'Київ'
SEQUENCE :
    SEQUENCE :
        OBJECT IDENTIFIER : id-dstu4145PB [1.2.804.2.1.1.1.3.1.1]
    SEQUENCE :
        SEQUENCE :
            SEQUENCE :
                INTEGER : 257
                INTEGER : 12
            INTEGER : 0
        OCTET STRING :
            10BEE3DB6AEA9E1F86578C45C12594
            FF942394A7D738F9187E6515017294
            F4CE01
        INTEGER :
            00800000000000000000000000000000
            00006759213AF182E987D3E1771490

```

```

7D470D
OCTET STRING :
  B60FD2D8DCE8A93423C6101BCA91C4
  7A007E6C300B26CD556C9B0E7D20EF
  292A00
OCTET STRING :
  A9D6EB45F13C708280C4967B231F5EADF
  658EBA4C037291D38D96BF025CA4E17F8
  E9720DC615B43A28975F0BC1DEA36438B
  564EA2C179FD0123E6DB8FAC57904
BIT STRING UnusedBits:0 :
  OCTET STRING :
    ADE7A73D54E9650575BE685700C31B31823D
    2C8C131ADF24A2028F6598DD20A001
CONTEXT SPECIFIC (3) :
  SEQUENCE :
    SEQUENCE :
      OBJECT IDENTIFIER : subjectKeyIdentifier [2.5.29.14]
      OCTET STRING :
        OCTET STRING :
          E8E9687A597F245F666575A298F35B
          276FFA09696274FB63FB6D33E874A9
          F5DC
      SEQUENCE :
        OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
        OCTET STRING :
          SEQUENCE :
            CONTEXT SPECIFIC (0) :
              E8E9687A597F245F666575A298F
              35B276FFA09696274FB63FB6D33
              E874A9F5DC
        SEQUENCE :
          OBJECT IDENTIFIER : keyUsage [2.5.29.15]
          BOOLEAN : 'y'
          OCTET STRING :
            BIT STRING UnusedBits:1 :
              06
        SEQUENCE :
          OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
          BOOLEAN : 'y'
          OCTET STRING :
            SEQUENCE :
              SEQUENCE :

```


OBJECT IDENTIFIER : [1.2.804.2.1.1.1.2.2]
SEQUENCE :
OBJECT IDENTIFIER : basicConstraints [2.5.29.19]
BOOLEAN : 'y'
OCTET STRING :
SEQUENCE :
BOOLEAN : 'y'
INTEGER : 2
SEQUENCE :
OBJECT IDENTIFIER : [1.3.6.1.5.5.7.1.3]
BOOLEAN : 'y'
OCTET STRING :
SEQUENCE :
SEQUENCE :
OBJECT IDENTIFIER : [1.2.804.2.1.1.1.2.1]
SEQUENCE :
OBJECT IDENTIFIER : id-dstu4145PB [1.2.804.2.1.1.1.3.1.1]
BIT STRING UnusedBits:0 :
OCTET STRING :
E66B694671447222449D08A43EB5BADB8BD418639E
7CF545E5AD6FC3984FCA5AB02F1BA4A8DA875C7998
D9ACC6847E467C6CA340CB0A31A57EF6E11BD84ACB
19