

Додаток
до Вимог до форматів транспортних
контейнерів особистих ключів
електронного цифрового підпису та
особистих ключів шифрування
(пункт 6 розділу III, пункт 4 розділу IV)

ПРИКЛАДИ

ASN.1 структур транспортних контейнерів особистого ключа електронного цифрового підпису або особистого ключа шифрування

Приклад 1. Транспортний контейнер особистого ключа

SEQUENCE : privateKeyInfo

INTEGER : version 0

SEQUENCE : privateKeyAlgorithm

OBJECT IDENTIFIER : id-dstu4145PB [1.2.804.2.1.1.1.3.1.1]

SEQUENCE : DSTU4145Params

SEQUENCE : ecbinary

SEQUENCE : f

INTEGER : m 257

INTEGER : trinomial 12

INTEGER : a 0

OCTET STRING : b

10BEE3DB6AEA9E1F86578C45C12594FF942394A7D738F

9187E6515017294F4CE01

INTEGER : n

```
0080000000000000000000000000000000006759213AF18
```

2E987D3E17714907D470D

OCTET STRING : bp

B60FD2D8DCE8A93423C6101BCA91C47A007E6C300B26C

D556C9B0E7D20EF292A00

OCTET STRING : dke

A9D6EB45F13C708280C4967B231F5EADF658EBA4C037291D

38D96BF025CA4E17F8E9720DC615B43A28975F0BC1DEA364

38B564EA2C179FD0123E6DB8FAC57904

OCTET STRING : privateKey

5FDB9C6030A36861080C8CE90EE448C29BDBF07EE0BC78A6C2ECA2

5CEB24012C

Приклад 2. Захищений транспортний контейнер особистого ключа

Пароль – «password»

```

SEQUENCE : encryptedPrivateKeyInfo
  SEQUENCE : encryptionAlgorithm
    OBJECT IDENTIFIER : id-PBES2 [1.2.840.113549.1.5.13]
  SEQUENCE : PBES2-params
    SEQUENCE : keyDerivationFunc
      OBJECT IDENTIFIER : id-PBKDF2 [1.2.840.113549.1.5.12]
    SEQUENCE : PBKDF2-params
      OCTET STRING : salt
        31A58DC1462981189CF6C701E276C7553A5AB5F6E3
        6D8418E4AA40C930CF3876
      INTEGER : iterationCount
        10000
    SEQUENCE : prf
      OBJECT IDENTIFIER : id-hmacGost34311 [1.2.804.2.1.1.1.1.2]
      NULL : "
  SEQUENCE : encryptionScheme
    OBJECT IDENTIFIER : id-gost28147-cfb [1.2.804.2.1.1.1.1.1.3]
  SEQUENCE : GOST28147Params
    OCTET STRING : iv
      4BB10F5C2945D49E
    OCTET STRING : dke
      A9D6EB45F13C708280C4967B231F5EADF658EBA4C0
      37291D38D96BF025CA4E17F8E9720DC615B43A2897
      5F0BC1DEA36438B564EA2C179FD0123E6DB8FAC579
      04
  OCTET STRING : encryptedData
    29A22E2951E632E1E444AE38F521C890FF6377FC0539113A66720B
    FC4E9107C566A07E3EAB9AE67F337ED9C66C021363E79508A9FDFA
    09E78877DFBE76543160DC83195427A9C7FF2F6F40D8D0FEA26583
    C72EF6E5E2045DA9512A61FBC2B9573E8B0BDC8F034D8CDA3ACA63
    B78C9877FA75C228756BE76083A235247A094C1EF2996FFBFCB45E
    6D14807B38E26A86261035131DEC63B37307B44EF2C0EAFE51392C
    D8A2B8B50FC6F8BC8B1A62EFD276D4E81BB358F4931BAAA3660C0C
    0B5DF52E5233D90D1F4EF5203C40F036CF5912914660BF28212C9B
    3FD9141CB89B93C13522DEB33085A25CC102B5B7DBA377078A645E
    88

```