

ЗАТВЕРДЖЕНО

Наказ Міністерства юстиції України,
Адміністрації Державної служби
спеціального зв'язку та захисту
інформації України

27 грудня 2013 року № 2782/5/689

ВИМОГИ

**до форматів контейнерів зберігання особистих ключів електронного
цифрового підпису, особистих ключів шифрування та сертифікатів
відкритих ключів**

I. Загальні положення

1. Ці Вимоги визначають формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування, сертифікатів відкритих ключів та іншої інформації з використанням алгоритмів 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); 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 (із змінами) (далі – ГОСТ 28147:2009); ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 21 жовтня 1997 року № 640 (далі – ГОСТ 34.311-95).

2. Формати даних представлено в 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», затвердженому наказом Державного комітету України з питань технічного регулювання та споживчої політики від 26 грудня 2008 року № 508 (із змінами).

3. Усі структури даних кодують за правилами DER згідно з міжнародними стандартами 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)» та AMD1:2004 «Support for EXTENDED-XER».

4. Ці Вимоги засновані на національних стандартах України ДСТУ 4145-2002, ГОСТ 28147:2009, міждержавному стандарті ГОСТ 34.311-95 з урахуванням Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12 червня 2007 року № 114, зареєстрованої в Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (далі – Інструкція); Вимог до формату посиленого сертифіката відкритого ключа, 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 № 1398/21710 (із змінами) (далі – Вимоги до формату посиленого сертифіката відкритого ключа); Вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 грудня 2012 року № 739, зареєстрованих у Міністерстві юстиції України 14 січня 2013 року за № 108/22610 (далі – Вимоги до форматів криптографічних повідомлень); Вимог до алгоритмів формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування (далі – Вимоги до алгоритмів формування ключів шифрування ключів) та Вимог до форматів транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування (далі – Вимоги до форматів транспортних контейнерів особистих ключів); міжнародних рекомендацій RFC 5208 «Private-Key Information Syntax Specification (PKCS#8)», May 2008 (далі – міжнародні рекомендації RFC 5208), RFC 2898 «Password-Based Cryptography Specification (PKCS#5)», September 2000 (далі – міжнародні рекомендації RFC 2898) та міжнародного стандарту PKCS#12 «Personal Information Exchange Syntax», October 2012 (далі – стандарт PKCS#12).

5. Ці Вимоги не дублюють стандарти ДСТУ 4145-2002, ГОСТ 28147:2009, ГОСТ 34.311-95, міжнародні рекомендації RFC 5208, RFC 2898 та стандарт PKCS#12, а описують положення цих стандартів і рекомендацій та формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування, сертифікатів відкритих ключів та іншої інформації. У разі виникнення розбіжностей між положеннями зазначених стандартів і рекомендацій та положеннями цих Вимог застосовуються положення цих Вимог.

6. Правильність реалізації форматів контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування, сертифікатів відкритих ключів та іншої інформації у надійних засобах електронного цифрового підпису та у засобах шифрування підтверджується позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

II. Особливості формування контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів

1. Контейнер зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів може містити особисті ключі підписувачів або відправників, сертифікати відкритих ключів підписувачів або відправників, акредитованих центрів сертифікації ключів, засвідчувальних центрів і центрального засвідчувального органу (ланцюжок сертифікатів), списки відкликаних сертифікатів (далі – СВС) акредитованих центрів сертифікації ключів, засвідчувальних центрів і центрального засвідчувального органу та повинен забезпечувати конфіденційність та цілісність зазначених даних.

2. Відповідно до стандарту PKCS#12 для забезпечення конфіденційності даних контейнера зберігання особистих ключів та сертифікатів повинен використовуватися режим захисту даних на основі паролльної інформації (password privacy mode).

3. Відповідно до стандарту PKCS#12 для забезпечення цілісності даних контейнера зберігання особистих ключів та сертифікатів повинен використовуватися режим контролю цілісності даних на основі паролльної інформації (password integrity mode).

4. Для забезпечення конфіденційності та контролю цілісності даних контейнера зберігання особистих ключів та сертифікатів повинен використовуватися однаковий пароль.

5. Сертифікати відкритих ключів та СВС повинні зберігатися у структурі «AuthenticatedSafe» як дані типу «зашифровані дані».

6. Особисті ключі користувача повинні зберігатися у структурі «AuthenticatedSafe» як дані типу «дані», які містять об'єкт «PKCS8ShroudedKeyBag».

7. Контейнер зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів може бути збережений у файловій системі. Кожний контейнер повинен бути поданий у вигляді DER-кодованих байтів та міститися в окремому файлі з розширенням «.pfx».

III. Формат контейнера зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів

1. Формат контейнера зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів має такий вигляд:

```
PFX ::= SEQUENCE {
version          INTEGER {v3(3)}(v3,...),
authSafe        ContentInfo,
macData         MacData OPTIONAL}.
```

2. Поле «version» містить версію формату контейнера зберігання електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів. Це поле повинно мати значення «3».

3. Поле «authSafe» визначається структурою «ContentInfo», яка подана в нотації ASN.1 та визначена у ДСТУ ISO/IEC 8824-1:2009 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 1. Специфікація базової нотації», ДСТУ ISO/IEC 8824-2:2009 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкта», ДСТУ ISO/IEC 8824-3:2009 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 3. Специфікація обмежень», ДСТУ ISO/IEC 8824-4:2009 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 4. Параметризація специфікацій ASN.1» (далі – ISO/IEC 8824).

Цими Вимогами дозволяється використання даних у структурі «ContentInfo» типу «дані», що визначаються об'єктним ідентифікатором:

id-data OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)

rsadsi(113549) pkcs(1) pkcs7(7) 1}

Поле «content» структури «authSafe» містить структуру типу «AuthenticatedSafe»:

AuthenticatedSafe ::= SEQUENCE OF ContentInfo.

4. Поле «macData» є необов'язковим та використовується для контролю цілісності структури «authSafe»:

```
MacData ::= SEQUENCE {
    mac          DigestInfo,
    macSalt      OCTET STRING,
    iterations   INTEGER DEFAULT 1}
```

Відповідно до цих Вимог поле «macData» повинно завжди бути присутнім.

IV. Типи даних структури «AuthenticatedSafe»

1. Цими Вимогами дозволяється використання даних у структурі «AuthenticatedSafe» типу «дані» або «зашифровані дані». Тип даних «дані» визначається ідентифікатором «id-data», а тип даних «зашифровані дані» – ідентифікатором:

```
pkcs-7 OBJECT IDENTIFIER ::= {iso(1) member-body(2) US(840)
rsadsi(113549) pkcs(1) 7}
encryptedData OBJECT IDENTIFIER ::= {pkcs-7 6}.
```

2. Формат даних типу «зашифровані дані» задається структурою «EncryptedData»:

```
EncryptedData ::= SEQUENCE {
    version          CMSVersion,
    encryptedContentInfo EncryptedContentInfo,
    unprotectedAttrs[1] IMPLICIT UnprotectedAttributes OPTIONAL}
```

1) поле «version» містить версію формату «EncryptedData». У разі наявності поля «unprotectedAttrs» це поле повинно мати значення «2», в іншому випадку – значення «0»;

2) поле «encryptedContentInfo» визначається Вимогами до форматів криптографічних повідомлень та містить зашифровані дані. Об'єктний ідентифікатор повинен вказувати на криптоалгоритм PBES2, параметри кри-

птоалгоритму повинні бути представлені структурою «PBES2-params», як наведено у Вимогах до алгоритмів формування ключів шифрування ключів;

3) поле «unprotectedAttrs» є необов'язковим та містить набір незашифрованих атрибутів.

3. Дані у структурі «AuthenticatedSafe» типу «дані» або «зашифровані дані» містять об'єкт «SafeContents», який зберігається у відкритому або зашифрованому вигляді:

SafeContents ::= SEQUENCE OF SafeBag

SafeBag ::= SEQUENCE {

bagId BAG-TYPE.&id ({PKCS12BagSet})
 bagValue [0] EXPLICIT BAG-TYPE.&Type
 ({PKCS12BagSet}{@bagId}),
 bagAttributes SET OF PKCS12Attribute OPTIONAL }

1) поле «bagId» визначає тип даних структури «SafeBag»;

2) поле «bagValue» містить об'єкт даних зазначеного типу в підпункті 3 цього пункту;

3) поле «bagAttributes» є необов'язковим та містить набір атрибутів:

PKCS12Attribute ::= SEQUENCE {

attrId ATTRIBUTE.&id ({PKCS12AttrSet}),
 attrValues SET OF ATTRIBUTE.&Type ({PKCS12AttrSet}{@attrId}) }

4) контейнер зберігання особистого ключа та сертифіката визначається відповідно до прикладу 1 Прикладів ASN.1 структури контейнера зберігання особистих ключів та сертифікатів, наведених у додатку до цих Вимог.

V. Типи даних структури «SafeBag»

1. Відповідно до PKCS#12 цими Вимогами визначається шість типів даних, які можуть бути використані у структурі «SafeContents»:

PKCS12BagSet BAG-TYPE ::= {

keyBag |
 pkcs8ShroudedKeyBag |
 certBag |
 crlBag |
 secretBag |
 safeContentsBag }.

2. Тип даних «KeyBag» визначається як KeyBag ::= PrivateKeyInfo та може містити лише один контейнер з особистим ключем, формат якого відповідає Вимогам до форматів транспортних контейнерів особистих ключів. На тип даних «KeyBag» вказує ідентифікатор:

```
pkcs-12 OBJECT IDENTIFIER ::= {iso(1) member-body(2) US(840)
rsadsi(113549) pkcs(1) 12}
bagtypes OBJECT IDENTIFIER ::= {pkcs-12 10 1}
BAG-TYPE ::= TYPE-IDENTIFIER
keyBag BAG-TYPE ::= {KeyBag IDENTIFIED BY {bagtypes 1}}.
```

3. Тип даних «PKCS8ShroudedKeyBag» визначається як PKCS8ShroudedKeyBag ::= EncryptedPrivateKeyInfo та може містити лише один захищений контейнер з особистим ключем, формат якого відповідає Вимогам до форматів транспортних контейнерів особистих ключів. На тип даних «PKCS8ShroudedKeyBag» вказує ідентифікатор:

```
pkcs8ShroudedKeyBag BAG-TYPE ::=
{PKCS8ShroudedKeyBag IDENTIFIED BY {bagtypes 2}}.
```

4. Тип даних «CertBag» використовується для зберігання сертифіката відкритого ключа:

```
CertBag ::= SEQUENCE {
    certId      BAG-TYPE.&id ({CertTypes}),
    certValue   [0] EXPLICIT BAG-TYPE.&Type ({CertTypes}{@certId})}
pkcs-9 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-9(9)}
certTypes OBJECT IDENTIFIER ::= {pkcs-9 22}
x509Certificate BAG-TYPE ::= {
    OCTET STRING IDENTIFIED BY {certTypes 1}}
sdsiCertificate BAG-TYPE ::= {
    IA5String IDENTIFIED BY {certTypes 2}}
CertTypes BAG-TYPE ::= {
    x509Certificate |
    sdsiCertificate}
```

На тип даних «CertBag» вказує ідентифікатор:

```
certBag BAG-TYPE ::= {CertBag IDENTIFIED BY {bagtypes 3}}
```

1) поле «certId» містить ідентифікатор типу сертифіката. Цими Вимогами дозволяється використання сертифіката типу «x509Certificate»;

2) поле «certValue» містить рядок октетів з DER-кодованим значенням сертифіката відкритого ключа відповідно до Вимог до формату посиленого сертифіката відкритого ключа.

5. Тип даних «CRLBag» використовується для зберігання списку відкликаних сертифікатів (CBC):

```
CRLBag ::= SEQUENCE {
    crlId      BAG-TYPE.&id ({CRLTypes}),
    crlValue   [0] EXPLICIT BAG-TYPE.&Type ({CRLTypes}{@crlId})}
crlTypes OBJECT IDENTIFIER ::= {pkcs-9 23}
x509CRL BAG-TYPE ::= {OCTET STRING IDENTIFIED BY {crlTypes 1}}
CRLTypes BAG-TYPE ::= {x509CRL}
```

На тип даних «CRLBag» вказує ідентифікатор:

```
crlBag BAG-TYPE ::= {CRLBag IDENTIFIED BY {bagtypes 4}}
```

- 1) поле «crlId» містить ідентифікатор типу CBC;
- 2) поле «crlValue» містить рядок октетів з DER-кодованим значенням CBC відповідно до Вимог до формату списку відкликаних сертифікатів.

6. Тип даних «SecretBag» призначений для зберігання особистої інформації користувача та не є предметом цих Вимог.

7. Тип даних «SafeContents» містить структуру «SafeContents» та призначений для рекурсивного зберігання вкладених типів «SafeBag». Тип даних «SafeContents» не є предметом цих Вимог.

8. Структура «SafeContents» визначається відповідно до прикладу 2 Прикладів ASN.1 структури контейнера зберігання особистих ключів та сертифікатів, наведених у додатку до цих Вимог.

VI. Параметри структури «SafeBag»

1. Цими Вимогами дозволяється використання атрибута «localKeyId» для даних типу «PKCS8ShroudedKeyBag» та «KeyBag» у полі «bagAttributes»:

```
localKeyId ATTRIBUTE ::= {
    WITH SYNTAX OCTET STRING
    EQUALITY MATCHING RULE octetStringMatch
    SINGLE VALUE TRUE
    ID pkcs-9-at-localKeyId}
pkcs-9-at-localKeyId OBJECT IDENTIFIER ::= {pkcs-9 21}.
```


2. Атрибут «localKeyId» не є обов'язковим та містить ідентифікатор відкритого ключа відповідно до Вимог до формату посиленого сертифіката відкритого ключа.

У випадку відсутності розширення «localKeyId» отримання ідентифікатора відкритого ключа для забезпечення перевірки відповідності особистого ключа електронного цифрового підпису або особистого ключа шифрування відкритому ключу, що міститься в сертифікаті відкритого ключа підписувача або відправника, здійснюється у порядку, визначеному в розділі V Вимог до форматів транспортних контейнерів особистих ключів.

**Начальник Управління
функціонування центрального
засвідчувального органу
Міністерства юстиції України**

Д.В. Журавльов

**Директор Департаменту криптографічного
захисту інформації Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України**

А.І. Пушкарьов