

ЗАТВЕРДЖЕНО

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

27 грудня 2013 року № 2782/5/689

Зареєстровано

в Міністерстві юстиції України

27 грудня 2013 року за № 2228/24760

## **ВИМОГИ**

**до форматів транспортних контейнерів особистих ключів електронного  
цифрового підпису та особистих ключів шифрування**

### **I. Загальні положення**

1. Ці Вимоги визначають формати транспортних контейнерів та захищених транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування 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 у 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 міжнародним стандартом 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».

4. Ці Вимоги засновані на національних стандартах України ДСТУ 4145-2002, ГОСТ 28147:2009, міждержавному стандарті ГОСТ 34.311-95 та міжнародних рекомендаціях RFC 5208 «Private-Key Information Syntax Specification (PKCS#8)», May 2008 (далі – RFC 5208) та RFC 2898 «Password-Based Cryptography Specification (PKCS#5)», September 2000 (далі – RFC 2898).

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

6. Правильність реалізації форматів транспортних контейнерів та захищених транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування у надійних засобах електронного цифрового підпису та у засобах шифрування підтверджується

позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації.

## **II. Порядок формування транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування**

1. При здійсненні процедури формування контейнерів особистих ключів електронного цифрового підпису або особистих ключів шифрування виконуються такі дії:

формується формат транспортного контейнера особистого ключа електронного цифрового підпису або особистого ключа шифрування та отримується DER-кодований рядок байтів;

шифрується DER-кодований рядок байтів та формується захищений контейнер особистого ключа.

2. Захищений транспортний контейнер особистого ключа електронного цифрового підпису або особистого ключа шифрування може бути збережений у файловій системі. Кожний захищений контейнер повинен бути поданий у вигляді DER-кодованих байтів та міститися в окремому файлі з розширенням «.pk8».

## **III. Формат транспортного контейнера особистого ключа електронного цифрового підпису та особистого ключа шифрування**

1. Формат транспортного контейнера особистого ключа електронного цифрового підпису або особистого ключа шифрування має такий вигляд:

```
PrivateKeyInfo ::= SEQUENCE {
    version                [0] Version,
    privateKeyAlgorithm    PrivateKeyAlgorithmIdentifier,
    privateKey             PrivateKey,
    attributes              [0] IMPLICIT Attributes OPTIONAL }
```

Version ::= INTEGER

PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier

PrivateKey ::= OCTET STRING

Attributes ::= SET OF Attribute

2. Поле «version» містить версію формату типу «PrivateKeyInfo». Це поле повинно мати значення «0».

3. Ідентифікатор криптоалгоритму в полі «AlgorithmIdentifier» містить об'єктний ідентифікатор та відповідні параметри криптоалгоритму. Об'єктний ідентифікатор повинен вказувати на криптоалгоритм ДСТУ 4145-2002 відповідно до 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). Параметри криптоалгоритму повинні бути представлені структурою «DSTU4145Params», як наведено у Вимогах до формату посиленого сертифіката відкритого ключа.

4. Поле «privateKey» містить особистий ключ алгоритму DSTU 4145-2002 у форматі Little-Endian, який кодується як OCTET STRING.

5. Поле «attributes» є необов'язковим та містить набір атрибутів.

6. Транспортний контейнер особистого ключа визначається відповідно до прикладу 1 Прикладів ASN.1 структур транспортних контейнерів особистого ключа електронного цифрового підпису або особистого ключа шифрування, наведених у додатку до цих Вимог.

#### **IV. Формат захищеного транспортного контейнера особистого ключа електронного цифрового підпису та особистого ключа шифрування**

1. Формат захищеного транспортного контейнера особистого ключа електронного цифрового підпису або особистого ключа шифрування має такий вигляд:

```
EncryptedPrivateKeyInfo ::= SEQUENCE {
    encryptionAlgorithm      EncryptionAlgorithmIdentifier,
    encryptedData             EncryptedData }
    EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
    EncryptedData ::= OCTET STRING
```

2. Поле «encryptionAlgorithm» містить об'єктний ідентифікатор та відповідні параметри алгоритму шифрування контейнера особистого ключа «PrivateKeyInfo». Об'єктний ідентифікатор повинен вказувати на криптоалгоритм PBES2 відповідно до RFC 2898. Параметри криптоалгоритму повинні бути представлені структурою «PBES2-params» відповідно до 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).

3. Поле «encryptedData» містить дані, які зашифровані відповідно до Вимог до алгоритмів формування ключів шифрування ключів.

4. Захищений транспортний контейнер особистого ключа (пароль – «password») визначається відповідно до прикладу 2 Прикладів ASN.1

структур транспортних контейнерів особистого ключа електронного цифрового підпису або особистого ключа шифрування, що додаються до цих Вимог.

## **V. Порядок формування ідентифікатора відкритого ключа**

1. 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 формування ідентифікатора відкритого ключа з виконанням таких дій:

з поля «privateKey» вилучається особистий ключ алгоритму ДСТУ 4145-2002;

з поля «AlgorithmIdentifier» вилучаються загальні параметри, що визначаються алгоритмом ДСТУ 4145-2002;

як значення функції від особистого ключа та загальних параметрів відповідно до ДСТУ 4145-2002 обчислюється відкритий ключ;

отримується стиснене зображення відкритого ключа;

обчислюється значення геш-функції за ГОСТ 34.311-95 від отриманої на попередньому етапі послідовності байтів. Як стартовий вектор геш-функції використовується нульовий вектор.

2. Якщо параметри криптоалгоритму в полі «AlgorithmIdentifier» містять таблицю заповнення вузлів заміни блока підстановки (довгостроковий ключовий елемент), то при обчисленні геш-функції використовується саме цей довгостроковий ключовий елемент, інакше використовується довгостроковий ключовий елемент № 1, наведений у додатку 1 до 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 (із змінами).

**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**