

ЗАТВЕРДЖЕНО

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

27 грудня 2013 року № 2782/5/689

ВИМОГИ

до інтерфейсів засобів криптографічного захисту інформації

I. Загальні положення

1. Ці Вимоги визначають вимоги до інтерфейсів засобів криптографічного захисту інформації, що реалізують алгоритми 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), 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).

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 національному стандарті ГОСТ 28147:2009, міждержавному стандарті ГОСТ 34.311-95, ДСТУ 4145-2002 та міжнародному стандарті «Public Key Cryptography Standard #11 v2.30: Cryptographic Token Interface Standard» (далі – PKCS#11).

5. Ці Вимоги не дублюють стандарти ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002, PKCS#11, а описують положення цих стандартів та інтерфейси засобів криптографічного захисту інформації. У разі виникнення розбіжностей між положеннями зазначених стандартів та положеннями цих Вимог застосовуються положення цих Вимог.

6. Правильність реалізації вимог до інтерфейсів засобів криптографічного захисту 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. Використання національних криптоалгоритмів

1. Шифрування/розшифрування за ГОСТ 28147:2009

1. Ключі згенеровані для шифрування/розшифрування за ГОСТ 28147:2009 (далі – ключі за ГОСТ 28147:2009) – об'єкти типу «СКО_SECRET_KEY», їх атрибут «СКА_KEY_TYPE» повинен мати значення «СКК_GOST28147»:

СКК_GOST28147 = 0x80420111;

окрім атрибутів типу «СКО_SECRET_KEY», ключі за ГОСТ 28147:2009 повинні мати атрибути, що наведені в таблиці 1 цих Вимог.

Таблиця 1

Атрибути ключів за ГОСТ 28147:2009

Атрибут	Тип даних	Значення
СКА_VALUE	Byte array	Значення ключа (32 байти), LSB-порядок байт
СКА_GOST_SBOXES	Byte array	DER-кодоване представлення довгострокового ключового елемента

Атрибут «СКА_GOST_SBOXES» визначається константою:

СКА_GOST_SBOXES = 0x80420311;

атрибут «СКА_GOST_SBOXES» містить довгостроковий ключовий елемент для алгоритму ГОСТ 28147:2009, який використовується разом із заданим ключем. Значення довгострокового ключового елемента кодується як «OCTET STRING» або як «OBJECT IDENTIFIER».

Якщо значення закодовано як «OCTET STRING», атрибут містить довгостроковий ключовий елемент аналогічно представленню поля «dke» структури «DSTU4145Params», як це визначено у підпункті 3.11.1 пункту 3.11 розділу III 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 (далі – Вимоги до формату посиленого сертифіката відкритого ключа).

Якщо значення закодовано як «OBJECT IDENTIFIER», атрибут містить об'єктний ідентифікатор криптографічних параметрів типу «СКО_DOMAIN_PARAMETERS» (тип ключа «СКК_GOST28147»), який визначає довгостроковий ключовий елемент для використання із заданим ключем. Криптографічні параметри алгоритму шифрування ГОСТ 28147:2009 наведено в пункті 2 цієї глави.

Атрибут «СКА_GOST_SBOXES» не може змінюватися користувачем.

2. Криптографічні параметри алгоритму шифрування за ГОСТ 28147:2009 зберігаються в об'єктах типу «СКО_DOMAIN_PARAMETERS» (тип ключа «СКК_GOST28147»). Криптографічні параметри, окрім атрибута типу «СКО_DOMAIN_PARAMETERS», можуть мати атрибути, наведені в таблиці 2 цих Вимог.

Атрибути криптографічних параметрів за ГОСТ 28147:2009

Атрибут	Тип даних	Значення
СКА_GOST_SBOXES	Byte array	DER-кодоване представлення довгострокового ключового елемента
СКА_ID	Byte array	Об'єктний ідентифікатор криптографічних параметрів

Для об'єктів типу «СКО_DOMAIN_PARAMETERS» атрибут «СКА_GOST_SBOXES» як значення приймає DER-кодоване представлення довгострокового ключового елемента відповідно до поля «dke» структури «DSTU4145Params», яка визначена у підпункті 3.11.1 пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа.

У випадку використання довгострокового ключового елемента, що не підтримується токеном, під час відкриття сесії створюються об'єкти з параметрами, які ним підтримуються. Для знаходження цих об'єктів забезпечується можливість їх пошуку за шаблоном:

```
СКА_CLASS      = СКО_DOMAIN_PARAMETERS
СКА_KEY_TYPE   = СКК_GOST28147
СКА_TOKEN      = TRUE
```

Якщо значення довгострокового ключового елемента не підлягає розголошенню, об'єкт типу «СКО_DOMAIN_PARAMETERS» у відповіді повертається тільки код помилки «СКР_ATTRIBUTE_SENSITIVE».

3. Алгоритм шифрування за ГОСТ 28147:2009 визначає перший (ECB), другий (CNT) та третій (CFB) режими роботи шифратора, а також режим вироблення імітовставки (MAC) та режим шифрування ключів (WRAP), що використовуються при формуванні криптографічних повідомлень (далі – механізми шифрування), які задаються такими ідентифікаторами:

```
СКМ_GOST28147_ECB    = 0x80420011;
СКМ_GOST28147_CNT    = 0x80420012;
СКМ_GOST28147_CFB    = 0x80420013;
СКМ_GOST28147_MAC    = 0x80420014;
СКМ_GOST28147_WRAP   = 0x80420016;
```

інформація про механізми шифрування, що повертається у відповіді структурою «СК_MECHANISM_INFO», повинна бути такою:

для механізмів шифрування «СКМ_GOST28147_ECB», «СКМ_GOST28147_CNT» та «СКМ_GOST28147_CFB»:

```

ulMinKeySize    = 32;
ulMaxKeySize    = 32;
Flags           = CKF_ENCRYPT | CKF_DECRYPT;

```

для механізму шифрування «CKM_GOST28147_MAC»:

```

ulMinKeySize    = 32;
ulMaxKeySize    = 32;
Flags           = CKF_SIGN | CKF_VERIFY;

```

для механізму шифрування «CKM_GOST28147_WRAP»:

```

ulMinKeySize    = 32;
ulMaxKeySize    = 32;
Flags           = CKF_WRAP | CKF_UNWRAP;

```

при використанні можливостей апаратної підтримки у полі «Flags» повинна бути встановлена додатково відмітка «CKF_HW».

Механізм шифрування «CKM_GOST28147_ECB» не має параметрів.

Параметри механізмів шифрування «CKM_GOST28147_CNT» та «CKM_GOST28147_CFB» задаються такою структурою:

```

typedef struct CK_GOST28147_PARAMS {
    CK_BYTE synchro[8];
} CK_GOST28147_PARAMS;

```

```

typedef CK_GOST28147_PARAMS* CK_GOST28147_PARAMS_PTR;

```

поле «synchro» містить значення синхропосилки (LSB-порядок байтів) для алгоритму ГОСТ 28147:2009.

Механізм шифрування «CKM_GOST28147_MAC» не має параметрів і обчислює імітовставку довжиною у 4 байти.

Для реалізацій алгоритму ГОСТ 28147:2009 передбачено нульове значення синхропосилки як параметр за умовчанням. Параметри за умовчанням використовуються при відсутності явно визначених параметрів алгоритму.

4. Пристрої, що підтримують шифрування та вироблення імітовставки за ГОСТ 28147:2009, у сформованій відповіді на запит щодо підтримуваних пристроєм механізмів шифрування (функція «C_GetMechanismList()») повинні вказати список механізмів шифрування, які підтримуються, із зазначенням їх ідентифікаторів.

При використанні можливостей апаратної підтримки у структурі «СК_MECHANISM_INFO» в полі «Flags» повинна бути встановлена додатково відмітка «СКF_HW».

При шифруванні (розшифруванні) використовується функція «C_EncryptInit()», у якій у якості механізму шифрування, що використовується, вказується один із механізмів шифрування «СКM_GOST28147_ECB», «СКM_GOST28147_CNT» чи «СКM_GOST28147_CFB», а у якості параметрів – покажчик на структуру «СК_GOST28147_PARAMS». У разі коли необхідно використовувати параметри за умовчанням, застосовується «NULL». Ключ, який використовується функцією ініціалізації, повинен мати тип «СКК_GOST28147».

Для обчислення (перевірки) імітовставки використовується функція «C_SignInit()», у якій у якості механізму шифрування, що використовується, вказується механізм «СКM_GOST28147_MAC», а у якості параметрів – покажчик на структуру «СК_GOST28147_PARAMS». У разі коли необхідно використовувати параметри за умовчанням, застосовується «NULL».

Подальше обчислення імітовставки здійснюється за алгоритмом, визначеним ГОСТ 28147:2009, з використанням функцій «C_Sign()» та «C_SignUpdate()» / «C_SignFinal()», а перевірка імітовставки – з використанням функцій «C_Verify()» та «C_VerifyUpdate()» / «C_VerifyFinal()».

В обох випадках у якості ключа у функцію ініціалізації необхідно передавати ключ типу «СКК_GOST28147».

2. Гешування за ГОСТ 34.311-95

1. Алгоритм гешування за ГОСТ 34.311-95 (далі – механізм гешування) задається таким ідентифікатором:

СКM_GOST34311 = 0x80420021;

інформація про механізм гешування, що повертається у відповіді структурою «СК_MECHANISM_INFO», повинна бути такою:

```
ulMinKeySize  = 0;
ulMaxKeySize  = 0;
Flags         = SKF_DIGEST;
```

параметри алгоритму задаються DER-кодованою структурою «Gost34311Params».

```
Gost34311Params ::= CHOICE {
    dke Dke,
    params SEQUENCE {
```

dke	Dke,
iv	OCTET STRING (SIZE(8)) OPTIONAL }

Поле «dke» визначає довгостроковий ключовий елемент, який використовується при гешуванні.

```
Dke ::= CHOICE {
    dkeValue    OCTET STRING (SIZE(64)),
    dkeId       OBJECT IDENTIFIER }
```

Поле «dkeValue» містить довгостроковий ключовий елемент для функції гешування в упакованому форматі, описаному в підпункті 3.12.1 пункту 3.12 розділу III Вимог до формату посиленого сертифіката відкритого ключа.

Поле «dkeId» містить об'єктний ідентифікатор, що ідентифікує довгостроковий ключовий елемент для функції гешування.

Поле «iv» визначає стартовий вектор гешування (LSB-порядок байт).

Для реалізації алгоритму гешування за ГОСТ 34.311-95 передбачені параметри за умовчанням:

довгостроковий ключовий елемент № 1 додатка 1 до пункту 2.2 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 у Міністерстві юстиції України 25 червня 2007 року за № 729/13996 (далі – Інструкція);

нульовий стартовий вектор гешування.

Параметри за умовчанням застосовуються за відсутності явно вказаних параметрів алгоритму гешування за ГОСТ 34.311-95.

2. Пристрої, що підтримують гешування за ГОСТ 34.311-95, при формуванні відповіді повинні включати до неї список механізмів (функція «C_GetMechanismList()») із зазначенням ідентифікатора цього алгоритму.

При використанні можливостей апаратної підтримки у структурі «CK_MECHANISM_INFO» в полі «Flags» встановлена додатково відмітка «CKF_HW».

Для ініціалізації обчислення геш-функції за ГОСТ 34.311-95 необхідно застосовувати функцію «C_DigestInit()», вказавши її у якості механізму гешування, що використовується, механізм гешування «CKM_GOST34311», а в якості параметрів – покажчик на структуру «CK_GOST34311_PARAMS» або «NULL», якщо необхідно використовувати параметри за умовчанням.

3. Формування та перевірки підпису за ДСТУ 4145-2002

1. Ключами, що генеруються за алгоритмом ДСТУ 4145-2002, є ключова пара (особистий та відповідний йому відкритий ключ) об'єктів,

особистий ключ має тип «СКО_PRIVATE_KEY», відповідний йому відкритий ключ має тип «СКО_PUBLIC_KEY». Атрибут «СКА_KEY_TYPE» особистого та відповідного йому відкритого ключа повинен мати значення «СКК_DSTU4145»:

СКК_DSTU4145 = 0x80420131;

особистий ключ, окрім атрибутів типу «СКО_PRIVATE_KEY», може мати атрибути, наведені в таблиці 3 цих Вимог.

Таблиця 3

Атрибути особистого ключа, ключової пари, що генеруються за алгоритмом ДСТУ 4145-2002

Атрибут	Тип даних	Значення
СКА_EC_PARAMS	Byte array	DER-кодоване значення криптографічних параметрів – структури «DSTU4145Params» (відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа елементи базового поля зберігаються в LSB-форматі)
СКА_VALUE	Big integer	Власне значення особистого ключа (довге ціле відповідно до ДСТУ 4145-2002)

Відкритий ключ, окрім атрибутів типу «СКО_PUBLIC_KEY», може мати атрибути, наведені в таблиці 4 цих Вимог.

Таблиця 4

Атрибути відкритого ключа, ключової пари, що генеруються за алгоритмом ДСТУ 4145-2002

Атрибут	Тип даних	Значення
СКА_EC_PARAMS	Byte array	DER-кодоване значення криптографічних параметрів – структури DSTU4145Params (відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа елементи базового поля зберігаються в LSB-форматі)
СКА_EC_POINT	Byte array	DER-кодоване представлення відкритого ключа – OCTET STRING, яке містить стиснене представлення точки еліптичної

		кривої в LSB-форматі (тип PublicKey відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа)
--	--	---

2. Криптографічні параметри ключової пари, що генеруються за алгоритмом ДСТУ 4145-2002, зберігаються в об'єктах типу «СКО_DOMAIN_PARAMETERS» (тип ключа «СКК_DSTU4145»). Криптографічні параметри, окрім атрибутів типу «СКО_DOMAIN_PARAMETERS», можуть мати атрибути, наведені в таблиці 5 цих Вимог.

Таблиця 5

Атрибути криптографічних параметрів ключової пари, що генеруються за алгоритмом ДСТУ 4145-2002

Атрибут	Тип даних	Значення
СКА_EC_PARAMS	Byte array	DER-кодоване значення криптографічних параметрів – структури DSTU4145Params (відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа елементи базового поля зберігаються в LSB-форматі)

У випадку використання криптографічних параметрів ключової пари, що генеруються за алгоритмом ДСТУ 4145-2002, що не підтримується токеном, під час відкриття сесії створюються об'єкти типу «СКО_DOMAIN_PARAMETERS» з параметрами, які ним підтримуються. У цьому випадку створені об'єкти типу «СКО_DOMAIN_PARAMETERS» використовують такі параметри:

СКА_CLASS = СКО_DOMAIN_PARAMETERS
СКА_KEY_TYPE = СКК_DSTU4145
СКА_TOKEN = TRUE

3. Алгоритм генерування ключової пари за ДСТУ 4145-2002 (далі – механізм генерування) задається таким ідентифікатором:

СКМ_DSTU4145 = 0x80420031;

інформація про механізм генерування («СК_MECHANISM_INFO») має бути такою:

```

ulMinKeySize    = 163;
ulMaxKeySize    = 509;
Flags           = CKF_SIGN | CKF_VERIFY | CKF_EC_F_2M |
                  CKF_EC_ECPARAMETERS | CKF_EC_NAMEDCURVE |
                  CKF_EC_COMPRESS;

```

алгоритм генерування ключової пари за ДСТУ 4145-2002 з використанням алгоритму гешування за ГОСТ 34.311-95 як механізм генерування задається таким ідентифікатором:

```
CKM_GOST34311_DSTU4145 = 0x80420032;
```

інформація про механізм генерування («CK_MECHANISM_INFO») має бути такою:

```

ulMinKeySize    = 163;
ulMaxKeySize    = 509;
Flags           = CKF_SIGN | CKF_VERIFY | CKF_EC_F_2M |
                  CKF_EC_ECPARAMETERS | CKF_EC_NAMEDCURVE |
                  CKF_EC_COMPRESS;

```

механізм генерування використовує тільки точки еліптичної кривої у стислому зображенні відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа.

Цей механізм генерування не має параметрів, всі необхідні параметри мають зберігатися в атрибуті «СКА_EC_PARAMS» особистого та відповідного йому відкритого ключів.

4. Застосування механізму генерування

Пристрої, що підтримують формування та перевірку підпису за ДСТУ 4145-2002, при формуванні відповіді повинні включати до неї список механізмів (функція «C_GetMechanismList()») із зазначенням ідентифікаторів наявних алгоритмів.

При використанні можливостей апаратної підтримки у структурі «CK_MECHANISM_INFO» в полі «Flags» встановлена додатково відмітка «CKF_HW».

Для формування (перевірки) підпису необхідно застосовувати функцію «C_SignInit()», вказавши її у якості механізму генерування, що використовується, механізм генерування «CKM_GOST34311_DSTU4145», а в полі параметрів зазначити «NULL».

Подальше формування підпису здійснюється з використанням функцій «C_Sign()» та «C_SignUpdate()» / «C_SignFinal()», а перевірка підпису – з використанням функцій «C_Verify()» та «C_VerifyUpdate()» / «C_VerifyFinal()».

Для формування (перевірки) підпису до обчисленого значення функції гешування необхідно застосувати функцію «C_SignInit()», вказавши її у якості механізму генерування, що використовується, механізм «СКМ_DSTU4145», а у полі параметрів зазначити «NULL».

Подальше формування підпису здійснюється за алгоритмом DSTU 4145-2002. У якості даних передається обчислене значення функції гешування (LSB-порядок байтів).

Під час формування підпису необхідно вказувати особистий ключ, а під час перевірки – відповідний йому відкритий ключ. Ключі повинні мати тип «СКК_DSTU4145».

III. Механізми генерації ключів

1. Механізми генерації ключів за ГОСТ 28147:2009

1. Механізм «СКМ_GOST28147_KEY_GEN» здійснює генерацію ключа шифрування згідно з ГОСТ 28147:2009 за допомогою генератора (псевдо)випадкових послідовностей.

Механізм визначається таким ідентифікатором:

СКМ_GOST28147_KEY_GEN = 0x80420041;

інформація про механізм («СК_MECHANISM_INFO») має бути такою:

```
ulMinKeySize    = 32;
ulMaxKeySize    = 32;
Flags           = CKF_GENERATE;
```

при використанні можливостей апаратної підтримки в полі «Flags» повинна бути проставлена відмітка «CKF_HW».

Цей механізм не має параметрів.

Ключі шифрування створюються функцією «C_GenerateKey()» за допомогою цього механізму. Окрім стандартних атрибутів класу, у шаблоні ключа, що створюється, можуть бути присутні атрибути, що наведені в таблиці 6 цих Вимог. Значення за умовчанням для деяких атрибутів наведені в таблиці 7 цих Вимог.

Таблица 6

Атрибути шаблону ключів шифрування, які створюються механізмом
«СКМ_GOST28147_KEY_GEN»

Атрибут	Значення
СКА_CLASS	Якщо присутній, повинен бути «СКО_SECRET_KEY»

CKA_KEY_TYPE	Якщо присутній, повинен бути «СКК_GOST28147»
CKA_GOST_SBOXES	Довгостроковий ключовий елемент або об'єктний ідентифікатор з довгострокового ключового елемента – за умовчанням довгостроковий ключовий елемент № 1 згідно з Інструкцією

Таблиця 7

Значення атрибутів, які уточнюють сферу використання ключа,
що приймаються за умовчанням

Атрибут	Значення
CKA_ENCRYPT	«TRUE» або «FALSE» (за умовчанням – «TRUE»)
CKA_DECRYPT	«TRUE» або «FALSE» (за умовчанням – «TRUE»)
CKA_SIGN	«TRUE» або «FALSE» (за умовчанням – «TRUE»)
CKA_VERIFY	«TRUE» або «FALSE» (за умовчанням – «TRUE»)
CKA_WRAP	«TRUE» або «FALSE» (за умовчанням – «TRUE»)
CKA_UNWRAP	«TRUE» або «FALSE» (за умовчанням – «TRUE»)

2. Механізм «СКМ_DSTUDH_DERIVE» призначено для отримання ключа шифрування ключа (далі – КШК) на основі протоколу Діффі-Геллмана для еліптичних кривих, як це визначено в розділі V 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 № 108/22640 (далі – Вимоги до форматів криптографічних повідомлень) («id-dhSinglePass-stdDH-gost34311kdf-scheme»).

Механізм визначається таким ідентифікатором:

СКМ_DSTUDH_DERIVE = 0x80420043;

інформація про механізм («СК_MECHANISM_INFO») має бути такою:

```
ulMinKeySize  = 163;
ulMaxKeySize  = 509;
Flags          = CKF_DERIVE | CKF_EC_F_2M | CKF_EC_COMPRESS;
```

при використанні можливостей апаратної підтримки у полі «Flags» повинна бути проставлена відмітка «CKF_HW».

Параметри алгоритму задаються стандартною структурою «СК_ECDH1_DERIVE_PARAMS»:

```
typedef struct CK_ECDH1_DERIVE_PARAMS {
```

```

        CK_EC_KDF_TYPE          kdf;
        CK_ULONG                ulSharedDataLen;
        CK_BYTE_PTR             pSharedData;
        CK_ULONG                ulPublicDataLen;
        CK_BYTE_PTR             pPublicData;
    } CK_ECDH1_DERIVE_PARAMS;

```

де поля мають такі значення:

«kdf» – ідентифікатор функції формування ключа повинен мати значення «CKD_GOST34311_KDF»;

«ulSharedDataLen» – довжина одноразових даних, які використовуються під час генерації КШК, згідно з розділом V Вимог до форматів криптографічних повідомлень повинна дорівнювати 0 або 64;

«pSharedData» – одноразові дані, які використовуються при генерації КШК;

«ulPublicDataLen» – довжина в байтах відкритого ключа іншої сторони;

«pPublicData» – відкритий ключ іншої сторони, формат збігається з форматом атрибута «СКА_EC_POINT».

КШК формується функцією «C_DeriveKey()» за допомогою цього механізму. Параметр функції «hBaseKey» повинен вказувати на особистий ключ.

У шаблоні КШК, який створюється, вказуються атрибути, зазначені в таблиці 8 цих Вимог.

Таблиця 8

Атрибути, що зазначаються у шаблоні КШК

Атрибут	Значення
СКА_CLASS	«CKO_SECRET_KEY»
СКА_KEY_TYPE	«CKK_GOST28147», атрибут повинен бути присутній
СКА_WRAP	«TRUE»
СКА_UNWRAP	«TRUE»

Об'єкт «hBaseKey» повинен бути або діючим на цей час особистим ключем користувача, або спеціально згенерованим для цього протоколу на боці відправника «віртуальним» особистим ключем. У будь-якому випадку значення атрибутів «СКА_EC_PARAMS» об'єктів «pPublicData» та «hBaseKey» повинні збігатися.

Для обчислення геш-значення за ГОСТ 34.311-95, що використовується під час вироблення КШК, застосовується довгостроковий ключовий елемент, який взято з атрибута «СКА_EC_PARAMS» об'єкта «hBaseKey».

Створений ключ алгоритму ГОСТ 28147:2009 отримує значення довгострокового ключового елемента (атрибут «СКА_GOST_SBOXES») з атрибута «СКА_EC_PARAMS» об'єкта «hBaseKey».

3. Механізм «CKM_DSTUDH_COFACTOR_DERIVE»

Цей механізм призначено для отримання КШК на основі протоколу Діффі-Геллмана для еліптичних кривих, як це визначено в розділі V Вимог до форматів криптографічних повідомлень («id-dhSinglePass-cofactorDH-gost34311kdf-scheme»).

Механізм визначається таким ідентифікатором:

CKM_DSTUDH_COFACTOR_DERIVE = 0x80420044;

інформація про механізм («CK_MECHANISM_INFO») має бути такою:

```
ulMinKeySize  = 163;
ulMaxKeySize  = 509;
Flags         = CKF_DERIVE | CKF_EC_F_2M | CKF_EC_COMPRESS;
```

при використанні можливостей апаратної підтримки в полі «Flags» повинна бути проставлена відмітка «CKF_HW».

Параметри алгоритму та порядок його використання визначаються так, як і в механізмі «CKM_DSTUDH_DERIVE».

4. Механізм «CKM_GOST_WRAP»

Цей механізм призначений для шифрування та розшифрування особистих ключів з використанням алгоритму, як це визначено у розділі VI Вимог до форматів криптографічних повідомлень. Механізм визначається таким ідентифікатором:

CKM_GOST_WRAP = 0x80420016;

інформація про механізм («CK_MECHANISM_INFO») повинна бути такою:

```
ulMinKeySize  = 32;
ulMaxKeySize  = 32;
Flags         = CKF_WRAP | CKF_UNWRAP;
```

При використанні можливостей апаратної підтримки в полі «Flags» повинна бути проставлена відмітка «CKF_HW».

Механізм не має параметрів.

Шифрування ключів здійснюється функцією «C_WrapKey()». КШК, який передається у функцію, має задовольняти такі вимоги:

```
атрибут SKA_CLASS = SKO_SECRET_KEY;
атрибут SKA_KEY_TYPE = CKK_GOST28147;
атрибут SKA_WRAP = TRUE.
```

Розшифрування ключів здійснюється функцією «C_UnwrapKey()». КШК, який передається у функцію шифрування, має задовольняти такі вимоги:

атрибут CKA_CLASS = CKO_SECRET_KEY;
 атрибут CKA_KEY_TYPE = CKK_GOST28147;
 атрибут CKA_UNWRAP = TRUE;

у шаблоні атрибутів КШК, який буде вміщувати розшифрований ключ, повинен бути присутній атрибут «СКА_KEY_TYPE». Також можуть бути присутніми стандартні атрибути класу та атрибути, що наведені в таблиці 6 цих Вимог.

2. Механізми генерації ключів за ДСТУ 4145-2002

1. Механізм «CKM_DSTU4145_KEY_PAIR_GEN»

Механізм генерації «CKM_DSTU4145_KEY_GEN» описує генерацію ключової пари відповідно до розділу 9 ДСТУ 4145-2002. Механізм визначається таким ідентифікатором:

CKM_DSTU4145_KEY_PAIR_GEN = 0x80420042;

інформація про механізм («CK_MECHANISM_INFO») має бути такою:

ulMinKeySize = 163;
 ulMaxKeySize = 509;
 Flags = CKF_GENERATE_KEY_PAIR | CKF_EC_F_2M |
 CKF_EC_ECPARAMETERS |
 CKF_EC_NAMEDCURVE |
 CKF_EC_COMPRESS; .

2. При використанні можливостей апаратної підтримки в полі «Flags» повинна бути проставлена відмітка «CKF_HW».

Цей механізм не має параметрів.

Ключові пари створюються функцією «C_GenerateKeyPair()» за допомогою цього механізму.

У шаблоні атрибутів особистого ключа, який створюється, повинні бути присутні обов'язкові атрибути, які наведені в таблиці 9 цих Вимог.

У шаблоні атрибутів відкритого ключа, який створюється, повинні бути присутні обов'язкові атрибути, які наведені у таблиці 10 цих Вимог.

В обох шаблонах дозволяється вказувати стандартні атрибути, що впливають на місце розміщення ключів та доступ до них: «СКА_TOKEN», «СКА_PRIVATE», «СКА_SENSITIVE», «СКА_EXTRACTABLE».

Атрибути «СКА_SIGN_RECOVER», «СКА_VERIFY_RECOVER», «СКА_WRAP», «СКА_UNWRAP», «СКА_ENCRYPT» та «СКА_DECRYPT» із значенням «TRUE» у шаблонах не вказуються, оскільки ці операції не підтримуються базовим алгоритмом.

Якщо у шаблоні присутні перераховані атрибути із значенням «TRUE», функція повинна у відповіді повернути інформацію про помилку: «CKR_TEMPLATE_INCONSISTENT».

Обов'язково необхідно вказати значення атрибута «СКА_DERIVE».

Якщо атрибути «СКА_EC_PARAMS» визначені для обох ключів, їх значення повинні збігатися. Достатньо вказати атрибут «СКА_EC_PARAMS» для одного з ключів.

Деякі токени можуть підтримувати конкретний набір криптографічних параметрів. При неможливості використовувати визначені параметри функція генерування ключів у відповіді поверне помилку «CKR_DOMAIN_PARAMS_INVALID». У таких випадках використовуються тільки ті параметри, що підтримуються. Такі параметри повинні бути відомими заздалегідь або одержуватися з токена через об'єкти типу «СКО_DOMAIN_PARAMETERS», як зазначено в пункті 2 глави 3 розділу II цих Вимог.

Токени можуть підтримувати значення криптографічних параметрів за умовчанням, але при цьому необхідно вказувати значення атрибута «СКА_EC_PARAMS».

Таблиця 9

Атрибути шаблону особистих ключів, які створюються механізмом
«CKM_DSTU4145_KEY_PAIR_GEN»

Атрибут	Значення
СКА_CLASS	Якщо присутній, повинен бути «СКО_PRIVATE_KEY»
СКА_KEY_TYPE	Якщо присутній, повинен бути «СКК_DSTU4145»
СКА_EC_PARAMS	DER-кодоване значення криптографічних параметрів – структури DSTU4145Params (відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа елементи базового поля зберігаються в LSB-форматі)
СКА_DERIVE	TRUE або FALSE (за умовчанням – FALSE)

Таблиця 10

Атрибути шаблону відкритих ключів, які створюються механізмом
«CKM_DSTU4145_KEY_PAIR_GEN»

Атрибут	Значення
СКА_CLASS	Якщо присутній, повинен бути СКО_PUBLIC_KEY
СКА_KEY_TYPE	Якщо присутній, повинен бути СКК_DSTU4145
СКА_EC_PARAMS	DER-кодоване значення криптографічних параметрів –

	структури DSTU4145Params (відповідно до пункту 3.11 розділу III Вимог до формату посиленого сертифіката відкритого ключа елементи базового поля зберігаються в LSB-форматі)
--	---

**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