ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України   
\_\_ \_\_\_\_\_\_\_\_\_\_ 202\_\_ року № \_\_\_\_\_

ТЕХНІЧНІ СПЕЦИФІКАЦІЇ

до RFC 5652

1. Ці технічні специфікації доповнюють рекомендації Комітету із інженерних питань Інтернету RFC 5652 “Cryptographic Message Syntax (CMS)” (далі RFC 5652) в частині формування повідомлення типу “ContentInfo”, що містить дані типу “еnveloped-data” (“захищені дані”), з використанням законодавства у сфері електронних довірчих послуг та вітчизняних криптографічних алгоритмів, визначених національними стандартами:

ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння” (далі – ДСТУ 4145-2002);

ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування” (далі – ДСТУ 7564:2014);

ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення” (далі – ДСТУ 7624:2014);

ДСТУ ГОСТ 28147:2009 “Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования” (далі – ДСТУ ГОСТ 28147:2009);

ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хеширования” (далі – ГОСТ 34.311-95).

2. Доповнення до пункту 6.1 RFC 5652 “EnvelopedData Type”

Номер версії синтаксису, що визначається полем “Version” структури “EnvelopedData”, повинен мати значення “2”.

3. Доповнення до підпунктів 6.2.2 “KeyAgreeRecipientInfo” та [10.1.3](https://tools.ietf.org/html/rfc5652#section-10.1.3) “KeyEncryptionAlgorithmIdentifier”:

1) під час застосування динамічного механізму узгодження ключів у групі точок еліптичної кривої поле “algorithm” поля “originatorKey” для алгоритму цифрового підпису ДСТУ 4145-2002 може мати такі значення:

для поліноміального базису:

Dstu4145WithDstu7564(256)pb OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithDstu7564(6) 256(1) pb(1)};

Dstu4145WithGost34311(pb) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithGost34311(1) pb(1)};

для оптимального нормального базису:

Dstu4145WithDstu7564(256)оnb OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithDstu7564(6) 256(1) оnb(2)};

Dstu4145WithGost34311оnb OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) ua-pki (1) alg(1) asym (3) Dstu4145WithGost34311(1) onb(2)};

2) параметри алгоритму поля “algorithm” в “originatorKey” повинні бути ASN.1 NULL;

3) поле “originatorKey publicKey” повинно містити відкритий ключ відправника (маркер), що має такий формат:

PublicKey:: = OCTET STRING, що інкапсулюється в BIT STRING.

Відкритий ключ ДСТУ 4145-2002 – послідовність байтів, яка є елементом основного поля (пункт 5.3 розділу 5 ДСТУ 4145-2002), який є стиснутим зображенням (пункт 6.9 розділу 6 ДСТУ 4145-2002) точки на еліптичній кривій. Розмір зображення в байтах дорівнює m/8, заокруглений до найближчого цілого у більшу сторону;

4) об’єктні ідентифікатори (OID) протоколу узгодження ключа в групі точок еліптичної кривої (ECDH):

з використанням геш-функції ДСТУ 7564:2014:

алгоритм з кофакторним множенням:

id-dhSinglePass-cofactorDH-Dstu7564kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass-cofactorDH- Dstu7564kdf (7) };

алгоритм без кофакторного множення:

id-dhSinglePass-stdDH- Dstu7564kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass- stdDH- Dstu7564kdf (8) };

з використанням геш-функції ГОСТ 34.311-95:

алгоритм з кофакторним множенням:

id-dhSinglePass-cofactorDH-gost34311kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass-cofactorDH-gost34311kdf (4) };

алгоритм без кофакторного множення:

id-dhSinglePass-stdDH-gost34311kdf-scheme OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) asym (3) dhSinglePass- stdDH-gost34311kdf (5) };

5) параметри протоколу узгодження ключа в групі точок еліптичної кривої повинні бути визначені такою ASN.1 структурою:

EСDHParameters ::= SEQUENCE {  
 q INTEGER,  
 FR INTEGER,  
 а INTEGER,  
 b INTEGER,  
 G ECPoint,  
 n INTEGER,  
 h INTEGER,  
 dke OCTET STRING OPTIONAL},

де q – довжина поля (field size) у бітах, що дорівнює степеню основного поля (m);

FR – індикатор представлення поля або зведений поліном (reduction polynomial);

a та b – два елементи поля, які визначають криву (коефіцієнти рівняння еліптичної кривої);

G – базова точка еліптичної кривої (Base Point) з координатами (xG, yG);

n – порядок базової точки (order of the point) G;

h – кофактор, еквівалентний порядку кривої, поділеному на n (для еліптичних кривих з ДСТУ 4145-2002 h = 2 (якщо параметр еліптичної кривої а=1) або h = 4 (якщо параметр еліптичної кривої а=0));

значенням точки еліптичної кривої ECPoint повинен бути рядок байтів, який є закодованою точкою еліптичної кривої:

ECPoint ::= OCTET STRING;

процедура кодування точки (Point-to-Octet-String Conversion):

вхідними даними є точка еліптичної кривої P = (Xp, Yp), яка не є нульовою;

вихідними даними є рядок байтів РО – зображення у нестисненому форматі (uncompressed form) точки Р як рядка байтів;

байт РС = 0х04 (ознака нестисненого формату);

результуючий рядок байтів РО повинен бути об’єднанням (конкатенацією): PO = PC || Xр || Yp.

Рядком байтів для представлення нульового елемента групи точок еліптичної кривої О = (0, 0) (infinity) повинен бути один нульовий байт: PО = 0х00;

процедура обчислення FR:

поліномом є примітивний многочлен, що наведений у таблиці 1 ДСТУ 4145-2002. Значенням зведеного полінома є ціле число як рядок бітів;

для оптимального нормального базису FR = 0;

обчислення значення FR для поліноміального базису, де: m – ступінь основного поля, ks[len] – масив цілих чисел ks[0]=k3, ks[1]=k2, ks[2]=k1, що є ступенями примітивного многочлена. Поліном має вигляд x^m + x^k3 + x^k2 + x^k1 + 1, де: m > k3 > k2 > k1 >= 1, len – довжина масиву ks, для тричлена (trinomial) len = 1 та для п’ятичлена (pentanomial) len = 3, якщо len = 1, то k2 = k1 = 0;

для визначення FR як рядка бітів необхідно:

встановити FR = 1 (встановити біт 0);

встановити у FR біт m та відповідно біти k1, k2, k3;

6) при визначенні механізму узгодження ключів повинна виконуватися операція порівняння загальносистемних параметрів “ECDHParameters” покомпонентно (еквівалентність параметрів q, FR) або як порівняння масивів байтів DER-кодованої структури “EСDHParameters”. Якщо загальносистемні параметри еквівалентні, застосовується статичний механізм узгодження ключів, в інших випадках – динамічний;

7) формат сертифіката відкритого ключа, призначеного для узгодження симетричного ключа шифрування (далі – сертифікат шифрування), повинен відповідати вимогам законодавства у сфері електронних довірчих послуг.

Сертифікат шифрування повинен мати розширення “використання ключа”, що має об’єктний ідентифікатор id-ce-keyUsage OBJECT IDENTIFIER::= {id-ce 15}із значенням “узгодження ключа” (“keyAgreement”).

4. Доповнення до підпункту 10.1.4 “ContentEncryptionAlgorithmIdentifier” та пункту 12 “Security Considerations”:

1) як алгоритм шифрування даних “contentEncryptionAlgorithm” структури “EncryptedContentInfo” можуть використовуватися алгоритми:

ДСТУ 7624:2014 у режимах “Калина-256/256-OFB” (режим гамування зі зворотним зв’язком за шифротекстом відповідно до розділу 8 ДСТУ 7624:2014) та “Калина-256/256-CFB” (режим гамування зі зворотним зв’язком за шифрограмою відповідно до розділу 11 ДСТУ 7624:2014), які мають такі об’єктні ідентифікатори:

id-Dstu7624ofb(256) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) dstu7624 (3) ofb (6) 256(2)};

id-Dstu7624cfb(256) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) dstu7624 (3) cfb (3) 256(2)};

ДСТУ ГОСТ 28147:2009 в режимах “id-gost28147-ofb” (режим гамування, розділ 3 ДСТУ ГОСТ 28147:2009) та “id-gost28147-cfb” (режим гамування зі зворотним зв’язком, розділ 4 ДСТУ ГОСТ 28147:2009), які мають такі об’єктні ідентифікатори:

id-gost28147-ofb OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki(1) alg(1) sym(1) gost28147(1) ofb(2)};

id-gost28147-cfb OBJECT IDENTIFIER ::= {iso(1)member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki(1) alg(1) sym(1) gost28147(1) cfb(3)};

2) параметри алгоритму ДСТУ ГОСТ 28147:2009:

GOST28147Parameters ::= SEQUENCE {

iv OCTET STRING (SIZE (8)),

dke OCTET STRING (SIZE (64)) },

де “iv” – вектор ініціалізації, що обирається випадково;

“dke” – довгостроковий ключовий елемент (ДКЕ) для ДСТУ ГОСТ 28147:2009, що відповідає вимогам Інструкції № 114;

3) параметри алгоритму ДСТУ 7624:2014:

Dstu7624Parameters::= SEQUENCE {

iv OCTET STRING (SIZE (32))},

де “iv” – вектор ініціалізації, що обирається випадково;

4) для шифрування ключових даних чи інших даних, що підлягають захисту, при формуванні “захищених даних” повинен застосовуватися алгоритм захисту ключа шифрування даних “KeyWrapAlgorithm”;

5) алгоритм захисту ключа шифрування даних “KeyWrapAlgorithm” ґрунтується на стандарті ДСТУ 7624:2014, що позначається як “Dstu7624Wrap”, або ДСТУ ГОСТ 28147:2009, що позначається як “GOST28147Wrap”;

6) алгоритм криптографічного перетворення за ДСТУ 7624:2014 застосовується у режимі “Калина-256/256-CFB-256” (гамування зі зворотним зв’язком за шифртекстом відповідно до розділу 8 ДСТУ 7624:2014);

7) алгоритм криптографічного перетворення за ДСТУ ГОСТ 28147:2009 застосовується у режимі CFB (гамування зі зворотним зв’язком відповідно до розділу 4 ДСТУ ГОСТ 28147:2009);

8) алгоритм “KeyWrapAlgorithm”, що ґрунтується на стандарті ДСТУ 7624:2014, має такий синтаксис:

Dstu7624WrapParameters ::= CHOICE {

NULL, parameters Dstu7624Parameters},

Dstu7624Parameters::= SEQUENCE {

iv OCTET STRING (SIZE (32))},

де “iv” – вектор ініціалізації, що обирається випадково;

9) алгоритм “KeyWrapAlgorithm”, що ґрунтується на стандарті ДСТУ ГОСТ 28147:2009, має такий синтаксис:

GOST28147WrapParameters ::= CHOICE {

NULL, parameters GOST28147Parameters},

GOST28147Parameters ::= SEQUENCE {

iv OCTET STRING (SIZE (8)),

dke OCTET STRING (SIZE (64)) },

де “iv” – вектор ініціалізації, що обирається випадково;

“dke” – довгостроковий ключовий елемент (далі - ДКЕ) відповідно до ДСТУ ГОСТ 28147:2009.

За відсутності ДКЕ в параметрах криптоалгоритму використовується ДКЕ № 1 з переліку ДКЕ, які рекомендуються до застосування у засобах КЗІ, наведеного 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 (далі – Інструкція № 114).

Спосіб представлення ДКЕ № 1 повинен відповідати вимогам до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг, встановлених у нормативно-правових актах Мін’юсту та Адміністрації Держспецзв’язку;

10) під час використання “Dstu7624Wrap” або “GOST28147Wrap” як алгоритму захисту ключа шифрування ключів КШК у структурі “захищені дані” (“EnvelopedData”) параметри алгоритму повинні бути NULL.

Значення ДКЕ для алгоритму “GOST28147Wrap” повинно братися з відкритого ключа одержувача;

11) поле “algorithm” повинно містити об’єктний ідентифікатор:

для алгоритму “Dstu7624Wrap”:

id-dstu7624-wrap OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) dstu7624 (3) wrap(11) };

для алгоритму “GOST28147Wrap”:

id-gost28147-wrap OBJECT IDENTIFIER ::= { iso(1) member-body(2) Ukraine(804) root(2) security(1) cryptography(1) ua-pki (1) alg (1) sym (1) gost28147(1) wrap(5) };

12) процес зашифрування (Key Wrap) алгоритму “GOST28147Wrap”

Вхідними даними процесу зашифрування є:

“dke” – довгостроковий ключовий елемент (ДКЕ);

“KEK” – ключ шифрування ключа (КШК);

“CEK” – ключові дані для зашифрування (в операції формування “захищені дані” – ключ шифрування даних КШД).

Вихідними даними процесу зашифрування є “result” – зашифровані ключові дані.

Процес зашифрування виконується за такими етапами:

виконати ініціалізацію алгоритму вхідними даними “dke” та “КЕК”;

обчислити контрольну суму ключових даних “CEK”. Контрольна сума ключових даних (позначена як “ICV”) призначена для контролю правильності розшифрування зашифрованих ключових даних та обчислюється як імітовставка довжини 32 біти (“МАС32”) згідно з розділом 5 ДСТУ ГОСТ 28147:2009.

Значення “dke” та ключ під час обчислення “KEK” беруться ті, що встановлені під час виконання етапів процесу зашифрування:

ICV = МАС32(CEK, dke, КЕК) [4 байти];

виконати конкатенацію ключових даних з отриманою контрольною сумою:

CEKICV = CEK || ICV;

згенерувати випадкові 8 байтів як вектор ініціалізації (синхропосилка, позначено як “IV”);

виконати зашифрування даних “CEKICV” алгоритмом ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв’язком (GOST28147-CFB), використовуючи “dke” та ключ “KEK”, встановлені на кроці 1, і вектор ініціалізації “IV”, отриманий за результатами виконання позиції 4 цього пункту:

TEMP1 = GOST28147-CFB\_encrypt(CEKICV, IV, dke, КЕК).

Довжина вихідних даних “TEMP1” дорівнює довжині “CEKICV”;

виконати конкатенацію:

TEMP2 = IV || TEMP1;

виконати реверсне перетворення порядку байтів TEMP2 так, що перший байт TEMP2 стає останнім байтом. Результат перетворення позначимо TEMP3;

зашифрувати TEMP3 алгоритмом ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв’язком (GOST28147-CFB), використовуючи “dke” та ключ “KEK”, встановлені під час виконання позиції 1 цього пункту, та вектор ініціалізації “IV1”:

IV1 = 4a dd a2 2c 79 e8 21 05 (4a – молодший байт).

Результатом зашифрування алгоритмом GOST28147Wrap є:

result = GOST28147-CFB\_encrypt(TEMP3, IV1, dke, КЕК);

13) процес розшифрування (Key Unwrap) алгоритму GOST28147Wrap

Вхідними даними процесу розшифрування є:

“result” – зашифровані ключові дані;

“dke” – довгостроковий ключовий елемент (ДКЕ);

“KEK” – ключ шифрування ключа (КШК).

Вихідними даними процесу розшифрування є:

“CEK” – ключові дані (в операції формування “захищені дані” – ключ шифрування даних КШД).

Процес розшифрування виконується за такими етапами:

виконати ініціалізацію алгоритму вхідними даними “dke” та “КЕК”. Особливості ініціалізації щодо “dke” наведено у пункті 8.4 глави 8 розділу VI цих Вимог;

виконати розшифрування “result” на алгоритмі ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв’язком (GOST28147-CFB), використовуючи “dke” та ключ “KEK”, встановлені під час виконання етапу, зазначеного у позиції 1 цього пункту, та вектор ініціалізації “IV1”:

IV1 = 4a dd a2 2c 79 e8 21 05 (4a – молодший байт);

TEMP3 = GOST28147-CFB\_decrypt(result, IV1, dke, КЕК);

виконати реверсне перетворення порядку байтів TEMP3 так, що перший байт TEMP3 стає останнім байтом. Результат перетворення позначимо TEMP2;

відокремити складові у TEMP2 (перші 8 байтів – IV, усі інші – TEMP1):

TEMP2 = IV || TEMP1;

виконати розшифрування TEMP1 алгоритмом ДСТУ ГОСТ 28147:2009 у режимі гамування зі зворотним зв’язком (GOST28147-CFB), використовуючи “dke” та ключ “KEK”, встановлені під час виконання етапу, зазначеного у позиції 1 цього пункту, та вектор ініціалізації “IV”, отриманий за результатами виконання етапу, зазначеного у позиції 3 цього пункту:

CEKICV = GOST28147-CFB\_decrypt(TEMP1, IV, dke, КЕК);

відокремити складові у CEKICV (останні 4 байти – контрольна сума ICV, усі інші перші – ключові дані CEK):

CEKICV = CEK || ICV;

обчислити контрольну суму (“ICV1”) отриманих ключових даних “CEK” як імітовставку довжини 32 біти (“МАС32”) згідно з розділом 5 ДСТУ ГОСТ 28147:2009.

Значення “dke” та ключ під час обчислення “KEK” беруться ті, що встановлені під час виконання етапу, зазначеного у позиції 1 цього пункту:

ICV1 = МАС32(CEK, dke, КЕК) [4 байти];

порівняти контрольну суму “ICV”, отриману за результатами виконання етапу, зазначеного у позиції 6 цього пункту, з контрольною сумою “ICV1”, отриманою за результатами виконання етапу, зазначеного у позиції 7 цього пункту.

У разі нееквівалентності зазначених контрольних сум припинити подальше оброблення з результатом “помилка розшифрування ключа”.

У разі еквівалентності зазначених контрольних сум повернути як результат розшифрування алгоритму “GOST28147Wrap” отримане значення ключового матеріалу “CEK”;

14) під час використання “GOST28147Wrap” як алгоритму захисту ключа шифрування ключів КШК у структурі “захищені дані” (“EnvelopedData”) “dke” (довгостроковий ключовий елемент) визначається з параметрів алгоритму відкритого ключа одержувача;

15) процес зашифрування (Key Wrap) алгоритму Dstu7624Wrap

Умовні позначення:

CMAC(T,K) – функція обчислення імітовставки (контрольної суми) за алгоритмом “Калина-256/256-СМАС-256” (розділ 9 ДСТУ 7624:2014) повідомлення T на основі ключа K;

E(T,K,S) – функція шифрування повідомлення T на основі ключа K та синхропосилки S;

D(T,K,S) – функція розшифрування повідомлення T на основі ключа K та синхропосилки S;

REV(T) – функція реверсного перетворення порядку байтів повідомлення T так, що останній байт стає першим;

X||Y – операція конкатенації блоків X та Y;

L(T,N) – функція отримання молодших N-двійкових розрядів повідомлення T;

R(T,N) – функція отримання старших N-двійкових розрядів повідомлення T;

l(T) – функція отримання довжини повідомлення T.

Вхідні параметри:

KEK – ключ шифрування ключа (КШК), двійковий рядок довжиною 256;

CEK – ключові дані для шифрування (в операції формування “захищені дані” – ключ шифрування даних КШД);

IV – синхропосилка, двійковий рядок довжиною 256, генерація здійснюється перед використанням алгоритму;

IV1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням “6973271D6E611D06616715046C65504C2020004F6D68011F65610C0 C73734714”.

Вихідні параметри:

RES – зашифровані ключові дані.

Алгоритм:

виконати такі обчислення:

ICV = CMAC(CEK,KEK)

CEKICV = CEK||ICV

TEMP1 = E(CEKIV,KEK,IV)

TEMP2 = IV||TEMP1

TEMP3 = REV(TEMP2)

RES = E(TEMP3, KEK,IV1);

16) процес розшифрування (Key Unwrap) алгоритму Dstu7624Wrap

Вхідні параметри:

KEK – ключ шифрування ключа (КШК), двійковий рядок довжиною 256;

RES – зашифровані ключові дані;

IV1 – фіксована синхропосилка, двійковий рядок довжиною 256 із значенням “6973271D6E611D06616715046C65504C2020004F6D68011F65610C0 C73734714”.

Вихідні параметри:

CEK – ключові дані для шифрування (в операції формування “захищені дані” – ключ шифрування даних КШД).

Алгоритм:

виконати такі обчислення:

TEMP3 = E(RES,KEK,IV1)

TEMP2 = REV(TEMP3)

IV=L(TEMP2,256)

TEMP1=R(TEMP2,l(TEMP2)−256)

CEKICV = E(TEMP1,KEK,IV)

CEK = L(CEKICV,l(CEKICV)−256)

ICV = R(CEKICV, 256)

ICV1 = CMAC(CEK,KEK).

Порівняти контрольні суми ICV, ICV1. У разі нееквівалентності зазначених контрольних сум припинити подальше оброблення з результатом “помилка розшифрування ключа”.

У разі еквівалентності зазначених контрольних сум повернути як результат розшифрування алгоритму Dstu7624Wrap отримане значення ключового матеріалу *CEK*.

Т.в.о. директора Департаменту захисту інформації

Адміністрації Державної служби спеціального

зв’язку та захисту інформації України

полковник Ігор СТЕЛЬНИК