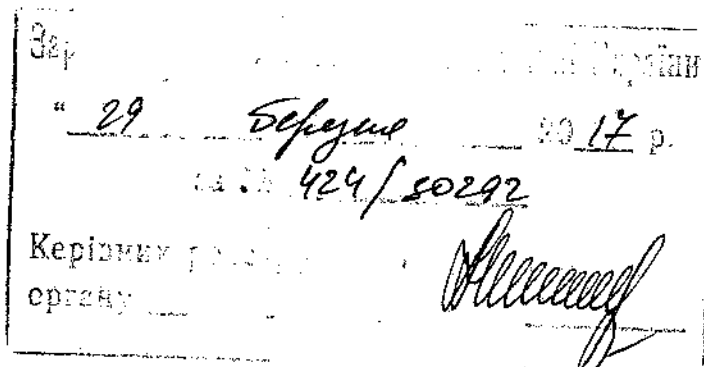


ЗАТВЕРДЖЕНО

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

29 березня 2017 року
№ 1014/15/1206



ЗМІНИ

до Вимог до формату підписаних даних

1. У розділі I:

1) пункт 1.8 викласти в такій редакції:

«1.8. ЕЦП обчислюється за криптографічними алгоритмами, визначеними у ДСТУ 4145-2002 «Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих», затвердженому наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002). Геш-функція обчислюється одним з криптоалгоритмів за:

ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 21 жовтня 1997 року № 640 (далі – ГОСТ 34.311-95);

ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування», затвердженим наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431 (далі – ДСТУ 7564-2014).»;

2) доповнити розділ новим пунктом 1.11 такого змісту:

«1.11. Для визначення алгоритму гешування згідно з ДСТУ 7564-2014 поле «algorithm» типу «AlgorithmIdentifier» може мати такі значення:

Dstu7564(256) OBJECT IDENTIFIER ::= {iso(1) member-body(2)
Ukraine(804) root(2) security(1) cryptography(1) pki(1) alg(1) hash(2)
Dstu7564(2) 1}

Dstu7564(384) OBJECT IDENTIFIER ::= {iso(1) member-body(2)

Ukraine(804) root(2) security(1) cryptography(1) pki(1) alg(1) hash(2)
Dstu7564(2) 2}

Dstu7564(512) OBJECT IDENTIFIER ::= {iso(1) member-body(2)
Ukraine(804) root(2) security(1) cryptography(1) pki(1) alg(1) hash(2)
Dstu7564(2) 3}

Поле «parameters» повинно бути відсутнє.

При використанні функції гешування за ДСТУ 7564-2014 в операціях формування та перевіряння електронного цифрового підпису режим обчислення геш-значення визначається 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.

В усіх інших операціях обчислення значення геш-функції згідно з ДСТУ 7564-2014 рекомендується використовувати режим гешування з формуванням геш-значення завдовжки 256 бітів.».

2. У розділі IV:

1) підпункт 4.2.2 пункту 4.2 викласти в такій редакції:

«4.2.2. Поле «digestAlgorithms» містить алгоритми гешування, що були використані під час формування ЕЦП.

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

Поле «digestAlgorithms» може містити об'єктні ідентифікатори алгоритмів гешування, які визначаються ГОСТ 34.311-95 або ДСТУ 7564-2014.»;

2) підпункт 4.3.5 пункту 4.3 викласти в такій редакції:

«4.3.5. Поле «signatureAlgorithm» містить ідентифікатор алгоритму цифрового підпису.

Поле «algorithm» поля «signatureAlgorithm» для алгоритму цифрового підпису ДСТУ-4145:2002 з геш-функцією за ДСТУ 7564-2014 може мати такі значення:

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

Dstu4145WithDstu7564(384) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) pki(1) alg(1)sym(3)
Dstu4145WithDstu7564(3) 2}

Dstu4145WithDstu7564(512) OBJECT IDENTIFIER ::= {iso(1) member-body(2) Ukraine(804) root (2) security(1) cryptography(1) pki(1) alg(1)sym(3)
Dstu4145WithDstu7564(3) 3}

У цьому випадку поле «parameters» поля «signatureAlgorithm» відсутнє.»;

3) пункт 4.11 викласти в такій редакції:

«4.11. Атрибут «complete-certificate-references» містить посилання на всі сертифікати Центрив, що використовуються для перевірки підпису. Посилання на сертифікат підписувача до зазначеного атрибута не включається. Посилання на сертифікат підписувача включається до атрибута «ESS signing-certificate v2».

Значення атрибута «complete-certificate-references» має тип «CompleteCertificateRefs».

CompleteCertificateRefs ::= SEQUENCE OF OtherCertID

OtherCertID ::= SEQUENCE {

otherCertHashOtherHash,

issuerSerial IssuerSerial OPTIONAL }

OtherHash ::= CHOICE {

otherHashOtherHashAlgAndValue}

OtherHashValue ::= OCTET STRING

OtherHashAlgAndValue ::= SEQUENCE {

hashAlgorithmAlgorithmIdentifier,

hashValueOtherHashValue }

Значення типу OtherHashAlgAndValue обмежується використанням функцій гешування, які визначаються ДСТУ 7564-2014 або ГОСТ 34.311-95.».

3. Пункт 5.3 розділу V доповнити новим підпунктом 5.3.5 такого змісту:

«5.3.5. При обчисленні значення геш-функції згідно з ДСТУ 7564-2014 режим обчислення геш-значення визначається 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, згідно з пунктом 1.11 розділу I цих Вимог.».

**Директор Департаменту
приватного права Міністерства
юстиції України**

 **Олена ФЕРЕНС**

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

 **Андрій ПУШКАРЬОВ**