

ЗАТВЕРДЖЕНО

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

29 березня

2017 року

№ 1014/5/206

Зареєстровано в Міністерстві юстиції України
“ <u>29</u> ” <u>березня</u> <u>2017</u> р.
за № <u>422/30290</u>
Керівнику розділу _____
органу _____

ЗМІНИ

до Вимог до формату посиленого сертифіката відкритого ключа

1. У розділі I:

1) пункт 1.4 викласти у такій редакції:

«1.4. Ці Вимоги засновані на вимогах до змісту сертифіката ключа, встановлених статтею 6 Закону України «Про електронний цифровий підпис», національному стандарті України ДСТУ ISO/IEC 9594-8:2014 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів», затвердженому наказом Міністерства економічного розвитку і торгівлі України від 30 грудня 2014 року № 1493 (далі – ДСТУ ISO/IEC 9594-8:2014), ДСТУ ETSI EN 319 412-1:2016 «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних», затвердженому наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183 (далі – ДСТУ ETSI EN 319 412-1:2016), Європейських стандартах ETSI EN 319 412-2 V2.1.1 (2016-02) «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificate issued to natural persons» (далі – ETSI EN 319 412-2), ETSI EN 319 412-3 V1.1.1 (2016-02) «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificate issued to legal persons» (далі – ETSI EN 319 412-3), ETSI EN 319 412-5 «Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements» (далі – ETSI EN 319 412-5) та на вимогах до застосування міжнародних криптографічних алгоритмів, встановлених національним стандартом України ДСТУ ETSI EN 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти», затвердженим наказом державного

підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 07 вересня 2016 року № 265 (далі – ДСТУ ETSI EN 119 312:2015).»;

2) доповнити розділ новим пунктом 1.5¹ такого змісту:

«1.5¹. Для перевірки електронного цифрового підпису, створеного відповідно до національного стандарту України ДСТУ 4145-2002 «Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих», затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31, повинен застосовуватися сертифікат відкритого ключа, що відповідає вимогам ДСТУ ISO/IEC 9594-8:2014 та цим Вимогам.

Для перевірки електронного цифрового підпису, створеного відповідно до алгоритмів ECDSA, визначеного національним стандартом України ДСТУ ISO/IEC 14888-3:2014 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів», затвердженим наказом Міністерства економічного розвитку і торгівлі України від 30 грудня 2014 року № 1493, або RSA, визначеного рекомендаціями RFC 3447 «Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1», повинен застосовуватися сертифікат відкритого ключа, що відповідає вимогам стандартів ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5.».

2. Назву розділу II викласти в такій редакції:

«II. Подання сертифіката для перевірки електронного цифрового підпису в інформаційно-телекомунікаційних системах з метою електронного документообігу та електронної взаємодії інформаційних систем в межах України».

3. У розділі III:

1) назву розділу викласти в такій редакції:

«III. Основні поля сертифіката для перевірки електронного цифрового підпису в інформаційно-телекомунікаційних системах з метою електронного документообігу, електронної взаємодії інформаційних систем та автентифікації в межах України»;

2) у таблиці 3 пункту 3.8:

позицію третю викласти в такій редакції:

«	commonName	реквізити підписувача	повне (або офіційне скорочене) найменування організації – юридичної особи – підписувача або	+	+
---	------------	-----------------------	---	---	---

		прізвище ім'я та (за наявності) по батькові фізичної особи – підписувача, що відповідають формату «commonName», визначеному у пункті 3.5 цього розділу			»;
--	--	--	--	--	----

позицію п'яту викласти в такій редакції:

«	givenName	ім'я та по батькові	ім'я та (за наявності) по батькові підписувача за паспортними даними id-at-givenName AttributeType ::= {id-at 42} X520givenName ::= DirectoryString (SIZE (64))	+	-	»;
---	-----------	---------------------	--	---	---	----

3) абзац одинадцятий пункту 3.10 виключити.

У зв'язку з цим абзац дванадцятий вважати абзацом одинадцятим;

4) у пункті 3.11:

абзаци другий, третій підпункту 3.11.1.2 підпункту 3.11.1 замінити підпунктами 3.11.1.2.1, 3.11.1.2.2 такого змісту:

«3.11.1.2.1. Для формату Little-Endian (при визначенні параметрів еліптичної кривої у сертифікаті):

поліноміальний базис 1.2.804.2.1.1.1.3.1.1

оптимальний нормальний базис 1.2.804.2.1.1.1.3.1.2.

Для формату Big-Endian:

поліноміальний базис 1.2.804.2.1.1.1.3.1.1.1

оптимальний нормальний базис 1.2.804.2.1.1.1.3.1.2.1.1.

3.11.1.2.2. Використання об'єктних ідентифікаторів, що визначені у пункті 3.11.1.2.1, у полі «subjectPublicKeyInfo» не передбачає будь-яких обмежень щодо використання функції гешування при обчисленні електронного цифрового підпису.»;

підпункт 3.11.2 виключити;

5) у пункті 3.12 слова та цифри «для ГОСТ 34.310-95 – розгорнутий формат» виключити;

6) пункт 3.13 викласти в такій редакції:

«3.13. Порядок використання геш-функцій при обчисленні значення електронного цифрового підпису.

3.13.1. Геш-функція може бути обчислена одним з криптоалгоритмів:

ГОСТ 34.311-95;

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

3.13.2. При використанні функції гешування за ГОСТ 34.311-95 під час обчислення електронного цифрового підпису значення стартового вектора H встановлюється рівним 256 нульовим бітам.

3.13.3. При використанні функції гешування за ДСТУ 7564-2014 під час обчислення електронного цифрового підпису рекомендовано застосовувати режими обчислення геш-значення, що визначаються бітовою довжиною порядку базової точки еліптичної кривої та наведені в таблиці 4. Як стартовий вектор геш-функції використовується нульовий вектор.

Таблица 4

Бітова довжина порядку базової точки	Режим обчислення геш-значення за ДСТУ 7564-2014
163-383	Режим використання функції гешування з формуванням геш-значення завдовжки 256, 384 або 512 бітів
384-511	Режим використання функції гешування з формуванням геш-значення завдовжки 384 або 512 бітів
>512	Режим використання функції гешування з формуванням геш-значення завдовжки 512 бітів

»;

7) У пункті 3.14:

абзац перший викласти в такій редакції:

«3.14. Порядок кодування окремих параметрів криптографічних алгоритмів.

При кодуванні реквізитів криптографічного алгоритму за ДСТУ 4145-2002 застосовуються такі правила:»;

у підпункті 3.14.1 слова та цифри «та ГОСТ 34.310-95» виключити.

4. У розділі IV:

1) назву розділу викласти в такій редакції:

«IV. Розширення сертифіката (extensions) для перевірки електронного цифрового підпису в інформаційно-телекомунікаційних системах з метою електронного документообігу та електронної взаємодії інформаційних систем в межах України»;

2) у пункті 4.2 слово та цифру «Таблиця 4» замінити словом та цифрою «Таблиця 5»;

3) у пункті 4.5:

в абзаці першому слова та цифри «та ГОСТ 34.310-95» виключити;

абзац четвертий викласти в такій редакції:

«Обчислюється значення геш-функції згідно з пунктом 3.13 розділу III цих Вимог.»;

4) пункт 4.12 викласти в такій редакції:

«4.12. Розширення «Персональні дані підписувача» («subjectDirectoryAttributes») має містити додаткові персональні дані підписувача та бути визначено як некритичне. Поле не використовується для зберігання даних про підписувача, що визначені в полі «subject».

Об'єктний ідентифікатор цього розширення має такий вигляд:

id-ce-subjectDirectoryAttributes OBJECTIDENTIFIER ::= {id-ce 9}

SubjectDirectoryAttributes ::= SEQUENCE SIZE (1.. MAX) OF Attribute

Attribute ::= SEQUENCE {

Type

Attributetype,

Values

SET OF AttributeValue}

Кодування національних реквізитів у розширенні «Персональні дані підписувача» («SubjectDirectoryAttributes») виконується за такими правилами:

1) код за Єдиним державним реєстром підприємств та організацій України юридичної особи – резидента (реєстраційний номер облікової картки платника податків – фізичної особи – підприємця) використовується для сертифікатів електронних печаток юридичних осіб – резидентів та для сертифікатів ключів їх посадових осіб. Для сертифікатів ключів посадових осіб у цьому реквізиті вказується код за Єдиним державним реєстром підприємств та організацій України юридичної особи (реєстраційний номер облікової картки платника податків – фізичної особи – підприємця), представником якої (в межах повноважень) є посадова особа.

Для кодування цього реквізиту використовується об'єктний ідентифікатор 1.2.804.2.1.1.1.11.1.4.2.1. Формат реквізиту – «PrintableString», що містить 8, 9 або 10 цифр;

2) реквізит реєстраційного номера облікової картки платника податків – фізичної особи – резидента використовується для сертифікатів ключів, підписувачами у яких є фізичні особи, у тому числі посадові особи. У цьому реквізиті вказується реєстраційний номер облікової картки платника податків – фізичної особи – підписувача.

Для кодування цього реквізиту використовується об'єктний ідентифікатор 1.2.804.2.1.1.1.11.1.4.1.1. Формат реквізиту – «PrintableString», що містить 10 цифр;

3) для фізичних осіб – резидентів, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті, до реквізитів, яким відповідають об'єктні ідентифікатори 1.2.804.2.1.1.1.11.1.4.1.1 та 1.2.804.2.1.1.1.11.1.4.2.1, вносяться серія (за наявності) та номер паспорта громадянина України. Формат реквізиту – «PrintableString», що містить від 2 до 8 літер серії паспорта (за наявності) та 6 або 9 цифр номера паспорта.

Кодування літерної частини реквізиту здійснюється відповідно до таблиці транслітерації українського алфавіту латиницею, затвердженої постановою Кабінету Міністрів України від 27 січня 2010 року № 55;

4) реквізит унікального номера запису в Єдиному державному демографічному реєстрі використовується для сертифікатів, підписувачами у яких є фізичні особи – резиденти, у тому числі посадові особи. У цьому реквізиті вказується унікальний номер запису в Єдиному державному демографічному реєстрі фізичної особи – підписувача. Для кодування цього реквізиту використовується об'єктний ідентифікатор 1.2.804.2.1.1.1.11.1.4.3.1. Формат реквізиту – «PrintableString», що містить послідовність з 8 цифр, символу «-» та 5 цифр.

Кодування реквізитів у розширенні «Персональні дані підписувача» («SubjectDirectoryAttributes») для юридичних осіб – нерезидентів та фізичних осіб – нерезидентів здійснюється за тими самими правилами з урахуванням особливостей форматів ідентифікаційних даних юридичних осіб та фізичних осіб, прийнятих у державі нерезидента, які підтверджено офіційними документами, наданими підписувачем.».

5. Доповнити Вимоги новим розділом V такого змісту:

«V. Подання сертифіката для перевірки електронного цифрового підпису відповідно до міжнародних стандартів

Під час формування сертифікатів відкритих ключів підписувачів повинні використовуватись алгоритми електронного цифрового підпису

ECDSA відповідно до національного стандарту ДСТУ ISO/IEC 14888-3:2014 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів», затвердженого наказом Міністерства економічного розвитку і торгівлі України від 30 грудня 2014 року № 1493, зі ступенем розширення основного поля еліптичної кривої не менше 256 бітів або RSA відповідно до рекомендацій RFC 3447 «Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1».

Для обчислення значення геш-функції під час формування сертифікатів відкритих ключів підписувачів повинен використовуватись алгоритм SHA-256 або SHA-512 відповідно до FIPS PUB 180-4 «Secure Hash Standard».

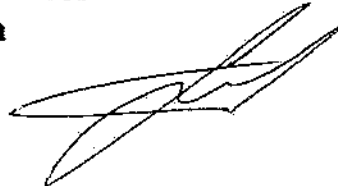
Параметри особистих ключів, які використовуються під час формування сертифікатів відкритих ключів підписувачів, визначаються регламентом роботи центрального засвідчувального органу.».

**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