

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

29 березня 2017 року
№ 1017/5 / 206

Зарплату за 1917 г. за 12 месяцев 1917 г. 120 руб.
" 29 " Березня 2014 р.
425/30293
Керівник :
органу

ЗМІНИ

до Вимог до протоколу фіксування часу

1. У розділі І:

1) пункт 1.8 викласти в такій редакції:

«1.8. Геш-функція обчислюється одним з криптоалгоритмів за:

ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования», затвердженням 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 новими пунктами 1.10, 1.11 такого змісту:

«1.10. Для визначення алгоритму гешування згідно з ДСТУ 7564-2014 поле «algorithm» 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.

1.11. 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. Підпункт 4.1.3 пункту 4.3 розділу IV викласти в такій редакції:

«4.1.3. Поле «reqPolicy» містить об'єктний ідентифікатор політики формування позначок часу:

TSAPolicyId ::= OBJECT IDENTIFIER

Можливі ідентифікатори для «TSAPolicyId» щодо застосування криптографічних алгоритмів підпису у відповіді на запит позначки часу:

ua-pki-TSPpolicyDSTU4145WithGost34311(PB) ::= OBJECT IDENTIFIER

{ua-pki(1.2.804.2.1.1.1) cp(2) TSPpolicy(3) 1} – для формування відповіді з цифровим підписом згідно з ДСТУ 4145-2002 «Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002) (поліноміальний базис), та геш-функцією згідно з ГОСТ 34.311-95;

ua-pki-TSPpolicyDstu4145WithGost34311(ONB) ::= OBJECT IDENTIFIER

{ua-pki(1.2.804.2.1.1.1) cp(2) TSPpolicy(3) 3} – для формування відповіді з цифровим підписом згідно з ДСТУ 4145-2002 (оптимальний нормальний базис) та геш-функцією згідно з ГОСТ 34.311-95;

ua-pki-TSPpolicyDstu4145WithDstu7564(256) ::= OBJECT IDENTIFIER

{ua-pki(1.2.804.2.1.1.1) cp(2) TSPpolicy(3)

TSPpolicyDstu4145WithDstu7564(4) 1} – для формування відповіді з цифровим підписом згідно з ДСТУ 4145-2002 та геш-функцією згідно з ДСТУ 7564-2014 у режимі формування геш-значення завдовжки 256 бітів;

ua-pki-TSPpolicyDstu4145WithDstu7564(256) ::= OBJECT IDENTIFIER

{ua-pki(1.2.804.2.1.1.1) cp(2) TSPpolicy(3)

TSPpolicyDstu4145WithDstu7564(4) 2} – для формування відповіді з цифровим підписом згідно з ДСТУ 4145-2002 та геш-функцією згідно з ДСТУ 7564-2014 у режимі формування геш-значення завдовжки 384 біти;

ua-pki-TSPpolicyDstu4145WithDstu7564(256) ::= OBJECT IDENTIFIER

{ua-pki(1.2.804.2.1.1.1) cp(2) TSPpolicy(3)

TSPpolicyDstu4145WithDstu7564(4) 3} – для формування відповіді з цифровим підписом згідно з ДСТУ 4145-2002 та геш-функцією згідно з ДСТУ 7564-2014 у режимі формування геш-значення завдовжки 512 бітів;

«За умовчанням» використовується політика;

до 31 грудня 2021 року «ua-pki-TSPpolicyDstu4145WithGost34311(PB)»;

з 01 січня 2022 року «TSPpolicyDstu4145WithDstu7564(256)PB», або «TSPpolicyDstu4145WithDstu7564(384)PB», або «TSPpolicyDstu4145WithDstu7564(512)PB» відповідно до вимог Регламенту роботи центрального засвідчувального органу.

При обробці запиту позначки часу Центр визначає можливість застосування вказаного у запиті алгоритму та формує відповідь, якщо зазначений алгоритм (політика) підтримується, або помилку, якщо алгоритм не підтримується.

Якщо у запиті алгоритм не вказано або відсутнє поле «reqPolicy», відповідь формується за алгоритмом, що визначений як алгоритм «за умовчанням».

**Директор Департаменту
приватного права Міністерства
юстиції України**

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



Олена ФЕРЕНС



Андрій ПУШКАРЬОВ