



МІНІСТЕРСТВО
ЕКОНОМІЧНОГО
РОЗВИТКУ І ТОРГІВЛІ
УКРАЇНИ

УКРАЇНА

(19) UA

(11) 120770

(13) U

(51) МПК

H04L 9/14 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2017 08755**

(22) Дата подання заявки: **30.08.2017**

(24) Дата, з якої є чинними
права на корисну
модель: **10.11.2017**

(46) Публікація відомостей
про видачу патенту: **10.11.2017, Бюл.№ 21**

(72) Винахідник(и):

**Янковський Ігор Миколайович (UA),
Цапко Денис Петрович (UA)**

(73) Власник(и):

**ТОВАРИСТВО З ОБМЕЖЕНОЮ
ВІДПОВІДАЛЬНІСТЮ "ІННОВЕЙШН
ДЕВЕЛОПМЕНТ ХАБ",**

пров. Охтирський, 7, корп. 3, м. Київ, 03680
(UA)

(74) Представник:

Матата Юлія Миколаївна

(54) СПОСІБ НАКЛАДАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПISY ЗА ДОПОМОГОЮ МОДУЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

(57) Реферат:

Спосіб накладання електронного цифрового підпису (ЕЦП) за допомогою модуля криптографічних перетворень. Додатково включає етапи, на яких:

- на модуль криптографічних перетворень встановлюють аплет, що імплементують стандарти криптографічного захисту інформації, причому аплет виконаний з можливістю генерації та збереження на модулі криптографічних перетворень приватного та публічного ключа, генерації та збереження на модулі криптографічних перетворень передпідписів, виконання операції накладання ЕЦП та операції перевірки валідності ЕЦП.

За допомогою модуля MSSP-послуг надсилають пакет даних до модуля криптографічних та технологічних перетворень (МКТП), перетворюють цей пакет даних в службове бінарне повідомлення, шифрують службове бінарне повідомлення та надсилають його через сервер оператора зв'язку на аплет.

За допомогою аплету приймають модулем криптографічних перетворень службове бінарне повідомлення, здійснюють його дешифрування та перевіряють особистий пароль користувача для накладання ЕЦП, причому перевірка особистого пароля користувача включає етапи, на яких:

- виводять на екран термінала користувача повідомлення про намір накладання ЕЦП, а також ідентифікуючу інформацію про сайт або ресурс, на якому проходить процес підпису,
- при підтвердженні наміру накладання ЕЦП здійснюють введення особистого пароля, причому кількість спроб вводу особистого пароля є обмеженою,

- при введенні валідного особистого пароля для накладання ЕЦП за допомогою аплету вибирають наступний передпідпис з кеша передпідписів та обчислюють ЕЦП відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015, причому кожен передпідпис генерують базуючись на алгоритмах, що використовуються при накладанні ЕЦП документа відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015, на попередньо згенерованому приватному ключі ЕЦП користувача і передпідписі, що захищено зберігаються в пам'яті модуля криптографічних перетворень та передпідпис використовують лише один раз, при цьому генерацію приватного та публічного ключів здійснюють ізольовано на модулі криптографічних перетворень після відповідного запиту з боку модуля MSSP-послуг,

причому вибір наступного передпідпису здійснюють у фоновому режимі у такій послідовності:

- у фоновому режимі формують список передпідписів у кількості N, де N - натуральне число;

UA 120770 U

- під час здійснення підпису використовують перший перед підпис зі списку передпідписів, відмічають його як використаний та здійснюють підписання документа,
- у разі здійснення наступного підписання документа використовують наступний передпідпис із списку передпідписів.

Після завершення підписів документів у фоновому режимі здійснюють перевірку списку передпідписів і здійснюють повторне генерування всіх передпідписів, що були відмічені як використані.

Генерують службове бінарне повідомлення, до якого включають обчислений ЕЦП, шифрують його та надсилають до МКТП, розшифровують службове бінарне повідомлення, формують пакет даних попередньо визначеної структури, який передають на модуль MSSP-послуг.

Корисна модель належить до галузі криптографічного захисту інформації і може бути використана для накладання електронного цифрового підпису (ЕЦП), верифікації накладення підпису за допомогою модуля криптографічних перетворень, такого як смарт-карта, SIM-карта, що імплементує стандарти криптографічного захисту ДСТУ ISO/IEC 14888-3:2015.

5 Криптографічні алгоритми, що використовуються при накладанні ЕЦП, базуються на використанні попередньо згенерованих приватному та публічному ключах ЕЦП користувача, що захищено зберігаються в пам'яті модуля криптографічних перетворень.

3 рівня техніки відомо спосіб підписання електронних документів аналого-цифровим підписом з додатковою верифікацією (заявка № WO 2014062093, 24.04.2014) за допомогою пристрою для підпису документів електронно-цифровим підписом, який включає пам'ять, мікропроцесор, щонайменше один порт вводу-виводу даних, пристрій вводу біометричних даних. При цьому пам'ять містить секретний ключ і програмне забезпечення, яке реалізує алгоритми обчислення контрольної суми та електронного цифрового підпису. Мікропроцесор пов'язаний з пам'яттю, портом вводу-виводу і пристроєм вводу біометричних даних здійснює обробку даних і виведення обробленої інформації через порт в EOM.

Недоліком відомого рішення є обмежені функціональні можливості, неможливість використання пристрою для підпису документів окремо, а лише у складі засобів криптографічного захисту інформації та електронного цифрового підпису.

Також з рівня техніки відома криптографічна служба у вигляді програмного забезпечення (патент № US 6412069 B1, 25.06.2002), яке розташовується на жорсткому або гнучкому диску та зв'язано зі стандартною операційною системою комп'ютера. Операційна система має простір застосувань та простір ядра. Програмне забезпечення (ПЗ) криптографічних служб виконує криптографічні операції у просторі ядра операційної системи. Це ПЗ включає в себе програмний інтерфейс рівня застосувань простору ядра та модуль криптографічних служб, що має бібліотеку криптографічних алгоритмів.

Недоліком відомої служби є те, що бібліотека криптографічних алгоритмів містить лише міжнародні криптографічні алгоритми, тому не може бути застосована для криптографічних перетворень національних криптографічних алгоритмів, зокрема ДСТУ ISO/IEC 14888-3:2015.

В основу корисної моделі поставлена задача створення способу накладання електронного цифрового підпису за допомогою модуля криптографічних перетворень, який може використовуватись як окремо, так і в складі інших засобів криптографічного захисту інформації (КЗІ) та який би забезпечував реалізацію національного криптографічного алгоритму України ДСТУ ISO/IEC 14888-3:2015.

Технічний результат запропонованого об'єкта корисної моделі полягає у забезпеченні можливості накладання та верифікації ЕЦП за допомогою модуля криптографічних перетворень окремо, що не потребує залучення інших засобів криптографічного захисту інформації, що значно спрощує процедуру накладання ЕЦП, у підвищенні швидкості розрахунку ЕЦП та у забезпеченні реалізації національного криптографічного алгоритму України ДСТУ ISO/IEC 14888-3:2015.

40 Ще одним технічним результатом є те, що завдяки запропонованому способу накладання ЕЦП саме за допомогою модуля криптографічних перетворень, процес накладання ЕЦП може бути здійснений незалежно від місцезнаходження користувача. Користувач лише має знаходитись в зоні покриття мобільного зв'язку, тобто він не обмежений наявністю стаціонарного робочого місця та інших технічних засобів.

45 Поставлена задача вирішується способом накладання електронного цифрового підпису за допомогою модуля криптографічних перетворень, що включає такі дії:

- на модуль криптографічних перетворень встановлюють аплет, що імплементує стандарти криптографічного захисту інформації, причому аплет виконаний з можливістю генерації та збереження на модулі криптографічних перетворень приватного та публічного ключа, генерації та збереження на модулі криптографічних перетворень передпідписів, виконання операції накладання ЕЦП та операції перевірки валідності ЕЦП,

50 - за допомогою модуля MSSP-послуг надсилають пакет даних до модуля криптографічних та технологічних перетворень (МКТП), перетворюють цей пакет даних в службове бінарне повідомлення, шифрують службове бінарне повідомлення та надсилають його через сервер оператора зв'язку на аплет,

55 - за допомогою аплету приймають модулем криптографічних перетворень службове бінарне повідомлення, здійснюють його дешифрування та перевіряють особистий пароль користувача для накладання ЕЦП, причому перевірка особистого пароля користувача включає етапи, па яких:

- виводять на екран термінала користувача повідомлення про намір накладання ЕЦП, а також ідентифікуючу інформацію про сайт або ресурс, на якому проходить процес підпису,
 - при підтвердженні наміру накладання ВЦП здійснюють введення особистого пароля, причому кількість спроб вводу особистого пароля є обмеженою,

5 - при введенні валідного особистого пароля для накладання ЕЦП за допомогою аплету вибирають наступний передпідпис з кеша передпідписів та обчислюють ЕЦП відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015, причому кожен передпідпис генерують базуючись на алгоритмах, що використовуються при накладанні ЕЦП документа відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015, на попередньо згенерованому приватному ключі ЕЦП користувача і передпідписі, що захищено зберігаються в пам'яті модуля криптографічних перетворень та передпідпис використовують лише один раз, при цьому генерацію приватного та публічного ключів здійснюють ізольовано на модулі криптографічних перетворень після відповідного запиту з боку модуля MSSP-послуг,

15 причому вибір наступного передпідпису здійснюють у фоновому режимі у такій послідовності:

- у фоновому режимі формують список передпідписів у кількості N, де N - натуральне число;
 - під час здійснення підпису використовують перший передпідпис зі списку передпідписів, відмічають його як використаний та здійснюють підписання документа,

20 - у разі здійснення наступного підписання документа використовують наступний передпідпис із списку передпідписів,

- після завершення підписів документів у фоновому режимі здійснюють перевірку списку передпідписів і здійснюють повторне генерування всіх передпідписів, що були відмічені як використані,

25 - генерують службове бінарне повідомлення, до якого включають обчислений ЕЦП, шифрують його та надсилають до МКТП, розшифровують службове бінарне повідомлення, формують пакет даних попередньо визначеної структури, який передають на модуль MSSP-послуг.

Як модуль криптографічних перетворень використовується смарт-картка (smart card), що містить інтегральну схему та пам'ять і призначена для ідентифікації, автентифікації, авторизації користувачів, зберігання ключової інформації і проведення криптографічних операцій в довіреному середовищі та інших операцій. В одному з варіантів здійснення способу модулем криптографічних перетворень є SIM-картка, що застосовується в мобільному зв'язку.

На модуль криптографічних перетворень, що являє собою смарт-карту, встановлюють спеціальний компонент (аплет), який може бути реалізований як програмним, так і апаратно-програмним шляхом, причому аплет розробляють з використанням технології JavaCard відповідно до специфікації ISO 7816.

За допомогою аплету здійснюють генерацію та збереження на смарт-карті приватного та публічного ключів, генерацію та збереження на смарт-карті передпідписів, виконання операції накладання ЕЦП та операцію перевірки валідності ЕЦП.

40 За допомогою МКТП здійснюють отримання пакетних даних у вигляді повідомлення від модуля MSSP-послуг, причому пакетні дані можуть включати в себе основні дані попередньо визначеної структури і додаткові ідентифікаційні дані. Крім того, за допомогою МКТП здійснюють перетворення отриманого повідомлення у службове бінарне повідомлення, шифрування службового бінарного повідомлення та отримання у відповідь зашифрованого службового бінарного повідомлення, яке включає обчислений ЕЦП, його розшифрування, формування попередньо визначеної структури даних та їх передачі до модуля MSSP-послуг. В одному з варіантів здійснення способу службовими бінарними повідомленнями є SMS-повідомлення, а сервером є модуль MSSP-послуг та МКТП.

50 Спосіб накладання ЕЦП за допомогою модуля криптографічних перетворень здійснюють таким чином.

За допомогою модуля MSSP-послуг надсилають пакет даних до МКТП, перетворюють цей пакет даних в службове бінарне повідомлення, шифрують службове бінарне повідомлення та надсилають його через сервер оператора зв'язку на аплет.

55 За допомогою аплету приймають модулем криптографічних перетворень службове бінарне повідомлення, здійснюють його дешифрування та перевіряють особистий пароль користувача для накладання ЕЦП, при цьому здійснюють перевірку особистого пароля здійснюють за допомогою використання бібліотеки SIMToolkit.

Перевірку особистого пароля здійснюють в такий спосіб.

60 - На дисплей термінала користувача (мобільного пристрою) виводять повідомлення про намір накладання ЕЦП.

- При підтвердженні дії, виводять повідомлення з проханням ввести особистий пароль, причому пароль вводиться обмежену кількість разів. В одному з варіантів здійснення способу особистий пароль можна вводити не більше 15 разів.

5 - після вводу валідного пароля для накладання ЕЦП за допомогою аплету вибирають наступний передпідпис із кеша передпідписів та проводять необхідні операції по обчисленню ЕЦП відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015.

Після перевірки особистою пароля генерують службове бінарне повідомлення, до якого включають обчислений ЕЦП, шифрують його та надсилають до МКТП, розшифровують службове бінарне повідомлення, формують пакет даних попередньо визначеної структури, який
10 передають на модуль MSSP-послуг.

Для забезпечення підвищення швидкодії, передпідписи ЕЦП попередньо розраховують та захищено зберігають в пам'яті модуля криптографічних перетворень відповідно до п. 11 та п. 12.8 стандарту ДСТУ ISO/IEC 14888-3:2015. При цьому кожен передпідпис генерують базуючись на попередньо згенерованих приватному та публічному ключах ЕЦП користувача, що захищено
15 зберігають в пам'яті смарт-карти та використовують лише один раз. Після використання передпідпис більше ніколи не бере участь у процесі операції накладання ЕЦП.

Також, в одному з варіантів здійснення способів може включати операцію заміни приватного та публічного ключів.

Заміну ключів здійснюють таким чином:

20 - за допомогою модуля MSSP-послуг надсилають запит на генерацію службового бінарного повідомлення із запитом на заміну ключів,

- за допомогою аплету приймають модулем криптографічних перетворень службове бінарне повідомлення із запитом на заміну ключів та відображають на екрані термінала користувача інформацію про поточний запит та запит введення пароля для заміни ключів.

25 - при вдалому введенні пароля користувача здійснюють генерування нових приватного та публічного ключів та зберігають їх у захищеній ділянці пам'яті модуля криптографічних перетворень,

- генерують службове бінарне повідомлення, в якому захищеним каналом передають новий згенерований публічний ключ для формування сертифіката або посиленого сертифіката перевірки ЕЦП.
30

Якщо під час операції заміни приватного та публічного ключів пароль вводять невдало попередньо визначену кількість спроб, то операцію заміни ключів блокують без можливості її відновлення.

35 В одному з варіантів здійснення способів може включати також операцію верифікації згенерованого ЕЦП, яку здійснюють згідно із стандартом ДСТУ ISO/IEC 14888 3:2015.

Також, в одному з варіантів здійснення способу накладання ЕЦП за допомогою модуля криптографічних перетворень на екран термінала користувача (мобільного пристрою) виводять кеш або фрагмент даних, які підписуються ЕЦП.

40 Запропонований спосіб накладання електронного цифрового підпису за допомогою модуля криптографічних перетворень, завдяки запропонованій послідовності дій забезпечує спрощення процедури накладання ЕЦП за рахунок забезпечення можливості накладання та верифікації ЕЦП окремо, що не потребує залучення інших засобів криптографічного захисту інформації, забезпечує підвищення швидкості розрахунку ЕЦП, а також забезпечує реалізацію національного криптографічного алгоритму України ДСТУ ISO/IEC 14888-3:2015. Крім того, за
45 рахунок використання модуля криптографічних перетворень, процес накладання ЕЦП може бути здійснений незалежно від місцезнаходження користувача. Користувач лише має знаходитись в зоні покриття мобільного зв'язку, тобто він не обмежений наявністю стаціонарного робочого місця та інших технічних засобів.

50 ФОРМУЛА КОРИСНОЇ МОДЕЛІ

1. Спосіб накладання електронного цифрового підпису (ЕЦП) за допомогою модуля криптографічних перетворень, який **відрізняється** тим, що включає етапи, на яких:

55 - на модуль криптографічних перетворень встановлюють аплет, що імплементують стандарти криптографічного захисту інформації, причому аплет виконаний з можливістю генерації та збереження на модулі криптографічних перетворень приватного та публічного ключа, генерації та збереження на модулі криптографічних перетворень передпідписів, виконання операції накладання ЕЦП та операції перевірки валідності ЕЦП,

60 - за допомогою модуля MSSP-послуг надсилають пакет даних до модуля криптографічних та технологічних перетворень (МКТП), перетворюють цей пакет даних в службове бінарне

повідомлення, шифрують службове бінарне повідомлення та надсилають його через сервер оператора зв'язку на аплет,

- за допомогою аплету приймають модулем криптографічних перетворень службове бінарне повідомлення, здійснюють його дешифрування та перевіряють особистий пароль користувача для накладання ЕЦП, причому перевірка особистого пароля користувача включає етапи, на яких:

- виводять на екран терміналу користувача повідомлення про намір накладання ЕЦП, а також ідентифікуючу інформацію про сайт або ресурс, на якому проходить процес підпису,

- при підтвердженні наміру накладання ЕЦП здійснюють введення особистого пароля, причому кількість спроб вводу особистого пароля є обмеженою,

- при введенні валідного особистого пароля для накладання ЕЦП за допомогою аплету вибирають наступний передпідпис з кеша передпідписів та обчислюють ЕЦП відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015, причому кожен передпідпис генерують базуючись на алгоритмах, що використовуються при накладанні ЕЦП документа відповідно до стандарту ДСТУ ISO/IEC 14888-3:2015, на попередньо згенерованому приватному ключі ЕЦП користувача і передпідписі, що захищено зберігається в пам'яті модуля криптографічних перетворень та передпідпис використовують лише один раз, при цьому генерацію приватного та публічного ключів здійснюють ізольовано на модулі криптографічних перетворень після відповідного запиту з боку модуля MSSP-послуг,

причому вибір наступного передпідпису здійснюють у фоновому режимі у такій послідовності:

- у фоновому режимі формують список передпідписів у кількості N, де N - натуральне число;

- під час здійснення підпису використовують перший передпідпис зі списку передпідписів, відмічають його як використаний та здійснюють підписання документа,

- у разі здійснення наступного підписання документа використовують наступний передпідпис із списку перед підписів,

- після завершення підписів документів у фоновому режимі здійснюють перевірку списку передпідписів і здійснюють повторне генерування всіх передпідписів, що були відмічені як використані,

- генерують службове бінарне повідомлення, до якого включають обчислений ЕЦП, шифрують його та надсилають до МКТП, розшифровують службове бінарне повідомлення, формують пакет даних попередньо визначеної структури, який передають на модуль MSSP-послуг.

2. Спосіб за п. 1, який **відрізняється** тим, що модулем криптографічних перетворень є SIM-карта або SMART-карта.

3. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що аплет виконано з використанням технології JavaCard.

4. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що службовими бінарними повідомленнями є SMS повідомлення, а сервером є модуль MSSP-послуг та МКТП.

5. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що особистий пароль можна водити не більше 15 разів.

6. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що передпідписи ЕЦП попередньо розраховують та захищено зберігають в пам'яті модуля криптографічних перетворень відповідно до п. 11 та п. 12.8 стандарту ДСТУ ISO/IEC 14888-3:2015.

7. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що додатково включає операцію заміни приватного та публічного ключів, який містить етапи, на яких:

- за допомогою модуля MSSP-послуг надсилають запит на генерацію службового бінарного повідомлення із запитом на заміну ключів,

- за допомогою аплету приймають модулем криптографічних перетворень службове бінарне повідомлення із запитом на заміну ключів та відображають на екрані терміналу користувача інформацію про поточний запит та запит введення пароля для заміни ключів,

- при вдалому введенні пароля користувача здійснюють генерування нових приватного та публічного ключів та зберігають їх у захищеній ділянці пам'яті модуля криптографічних перетворень,

- генерують службове бінарне повідомлення, в якому захищеним каналом передають новий згенерований публічний ключ для формування сертифіката або посиленого сертифіката перевірки ЕЦП.

8. Спосіб за п. 7, який **відрізняється** тим, що операцію заміни приватного та публічного ключа блокують без можливості відновлення після попередньо визначеної кількості невдалих спроб вводу пароля.

9. Спосіб за будь-яким з пунктів 7-8, який **відрізняється** тим, що додатково здійснюють операцію верифікації згенерованого ЕЦП згідно із стандартом ДСТУ ISO/IEC 14888-3:2015.

10. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що пакетом даних, який надсилають за допомогою модуля MSSP-послуг, є REST або пакет PKCS//7.
11. Спосіб за будь-яким з попередніх пунктів, який **відрізняється** тим, що додатково виводять на екран термінала користувача кеш або фрагмент даних, які підписують ЕЦП.

5

Комп'ютерна верстка Г. Паяльніков

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601