УКРАЇНА

(19) UA (11) 122325 (13) U

(51) МПК
H04L 9/14 (2006.01)

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2017 10093**

(22) Дата подання заявки: **18.10.2017**

(24) Дата, з якої є чинними права на корисну модель: **26.12.2017**

(46) Публікація відомостей про видачу патенту: **26.12.2017, Бюл.№ 24**

(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) АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ МОБІЛЬНОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

(57) Реферат:

Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису містить: модуль криптографічних перетворень (МКП), модуль MSSP-послуг, модуль криптографічних та технологічних перетворень (МКТП),
модуль протоколювання, модуль адміністрування. Модуль MSSP-послуг, МКТП, модуль протоколювання, модуль адміністрування поєднані за допомогою відокремленої мережі з окремою точкою доступу в мережі інтернет з модулем інтеграції, з МКП за допомогою службових повідомлень у захищеному каналі, створеним на обладнанні GSM-мережі оператора стільникового зв'язку.

UA 122325 U

Корисна модель належить до галузі криптографічного захисту інформації (КЗІ) і може бути використана у складі засобів КЗІ (у тому числі електронного цифрового підпису (ЕЦП)) для КЗІ з обмеженим доступом (крім службової інформації та інформації, яка становить державну таємницю), та відкритої інформації, вимога щодо захисту якої встановлена законом.

Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису призначений для забезпечення конфіденційності, цілісності та авторства інформації, яка передається та зберігається в автоматизованих системах класу 2 та 3. Комплекс включає апаратно-програмні та програмні засоби шифрування, ЕЦП та управління ключами.

Задачею корисної моделі є створення апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису, що призначений для забезпечення конфіденційності, цілісності та авторства інформації, яка передається та зберігається в автоматизованих системах класу 2 та 3 та КЗІ з обмеженим доступом (крім службової інформації та інформації, яка становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом, згідно з ДСТУ 4145-2002, ДСТУ ГОСТ 28147-2009, ГОСТ 34.311-95, ДСТУ ISO/IEC 14888-3:2015, ДСТУ ETSI EN 119 312:2015, ДСТУ ISO/IEC 18033-3:2015 та FIPS PUB 180-4 "Secure Hash Standard".

Технічний результат запропонованої корисної моделі полягає у створенні апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису, який забезпечує конфіденційність, цілісність та авторство інформації, яка передається та зберігається в автоматизованих системах класу 2 та 3 та КЗІ з обмеженим доступом (крім службової інформації та інформації, яка становить державну таємницю) та забезпечує реалізацію національних криптографічних алгоритмів України ДСТУ 4145-2002. ДСТУ ГОСТ 28147-2009. ГОСТ 34.311-95 та національних і міждержавних криптографічних алгоритмів ДСТУ ISO/IEC 14888-3:2015. ДСТУ ETSI EN 119 312:2015, ДСТУ ISO/IEC 18033-3:2015 та FIPS PUB 180-4 "Secure Hash Standard".

Поставлена задача вирішується за рахунок того, що в апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису введено

- модуль криптографічних перетворень (МКП), виконаний з можливістю забезпечення генерації особистого та відкритого ключа, зберігання ключів в захищеній ділянці пам'яті, взаємодії з сервером оператора мобільного зв'язку, отримання/відправлення службових повідомлень, а також реалізації функцій криптографічних перетворень, можливість проведення криптографічних перетворень у фоновому режимі,
- модуль MSSP-послуг, виконаний з можливістю здійснення криптографічних перетворень, взаємодії з іншими складовими апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису, причому модуль MSSP-послуг спеціально пристосований для використання інтерфейсів підключення до серверів оператора стільникового зв'язку та взаємодії з зовнішнім АЦСК або ЦСК,
- модуль криптографічних та технологічних перетворень (МКТП), виконаний з можливістю:
- отримання пакетних даних у вигляді повідомлення від модуля MSSP-послуг, причому пакетні дані включають в себе основні дані попередньо визначеної структури і додаткові ідентифікаційні дані;
- перетворення отриманого повідомлення у службове бінарне повідомлення;
- шифрування службового бінарного повідомлення;
- пересилання службового бінарного повідомлення на SMPP-сервер оператора стільникового зв'язку для його подальшого пересилання до модуля МКП для здійснення операції з обчислення електронного цифрового підпису (ЕЦП), верифікації ЕЦП або шифрування;
- отримання у відповідь зашифрованого службового бінарного повідомлення, яке включає обчислений ЕЦП, його розшифровування, формування попередньо визначеної структури даних та їх передачі до модуля MSSP-послуг,
- модуль протоколювання, виконаний з можливістю реєстрації подій від модуля MSSP-послуг, криптографічного захисту інформації, причому модуль виконаний з можливістю:
- збереження протягом попередньо визначеного строку даних, асоційованих з усіма операціями користувачів за всіма видами послуг за весь час;
- формування звітів за заданими критеріями;
- проставлення ЕЦП на сформованих звітах автентифікованими особами,
- модуль інтеграції, виконаний з можливістю:

- проставлення та перевірки ЕЦП, шифрування/дешифрування та надання інтерфейсів для здійснення цих операцій;

- надання інтерфейсів для підключення зовнішніх додатків/веб-сайтів до послуг, що надаються модулем MSSP-послуг,

- побудови захищеного каналу зв'язку між підключеними зовнішніми сервісами, з якими взаємодіє апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису, та його серверами

- модуль адміністрування, виконаний з можливістю контролю підключення та роботи зовнішніх додатків та сервісів, регулювання ролевої моделі управління та доступу до апаратно-програмного комплексу електронної ідентифікації, регулювання розмежування наданих послуг, а також надання сервісів для зовнішніх додатків, для АЦСК та ЦСК, мобільних операторів та регуляторів встановлених згідно з діючим законодавством,

при цьому модуль MSSP-послуг. МКТП, модуль протоколювання, модуль адміністрування поєднані за допомогою відокремленої мережі з окремою точкою доступу в мережі інтернет з модулем інтеграції, з МКП за допомогою службових повідомлень у захищеному каналі, створеним на обладнанні GSM-мережі оператора стільникового зв'язку.

Заявлена корисна модель пояснюється фігурою 1, на якій показано загальну схему апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису.

Захист інформації здійснюється шляхом застосування криптографічних алгоритмів згідно з ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ДСТУ ГОСТ 34.311-95, ДСТУ ISO/IEC 14888-3:2015, ДСТУ ETSIEN 119 312:2015, ДСТУ ISO/IEC 18033-3:2015 та FIPS PUB 180-4 "Secure Hash Standard", а також погоджених з Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку) методик генерації, розподілу та зберігання ключів, інструкцій із забезпечення безпеки інформації та генерації ключових даних тощо.

Комплекс спеціально пристосований для застосування пристрою функцій криптографічних перетворень, який функціонує під керуванням таких операційних систем (ОС):

- 32, 64-розрядних сімейства Windows: 7, 8, 8.1, 101, Server 2008 R2, Server 2012 R2, Server 2016+;

- 64-розрядних сімейства Linux з ядром 3.13 +;

- Ubuntu 14.04+;

- віртуальна Java-машина.

Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису забезпечує підписання, шифрування, розшифрування та перевірку підпису інформації, отриманої від джерела інформації, ведення журналів роботи, забезпечує захист від НСД до ключів та до інформації, що захищається.

Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису забезпечує роботу з контактними SIM-картами згідно із стандартом ISO/IEC 7816.

Модуль криптографічних перетворень (МКП) 1.

Як МКП 1, який виконує функцію захисту від НСД, використовується смарт-карта на базі SIM-карти стандарту SWP з криптоконтролером серії SLE 97CNFX1M50PE ı, виробництва Infineon.

МКП 1 є апаратно-програмним засобом КЗІ, у складі якого застосовується пристрій функцій криптографічних перетворень, який власне здійснює криптографічні перетворення.

МКП 1 забезпечує:

- генерацію особистого та відкритого ключа згідно зі стандартами ДСТУ 4145 та ДСТУ ISO/IEC 14888-3:2014, ДСТУ ETSI EN 119 312:2015;

- генерацію сеансових ключів згідно зі стандартом ДСТУ ISO/IEC 18033-3:2015 та ДСТУ ГОСТ 28147:2009

- зберігання ключів в захищеній ділянці пам'яті;

- взаємодію з сервером оператора мобільного зв'язку 8, отримання/відправлення службових повідомлень.

Модуль MSSP-послуг 2

Модуль MSSP-послуг 2 виконаний з можливістю здійснення криптографічних перетворень, керування серверами апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису, а також забезпечення взаємодії з іншими складовими та зовнішніми системами.

Модуль криптографічних та технологічних перетворень (МКТП) 3.

МКТП 3 виконаний з можливістю:

- отримання пакетних даних у вигляді повідомлення від модуля MSSP-послуг 2, причому пакетні дані включають в себе основні дані попередньо визначеної структури і додаткові ідентифікаційні дані;

- перетворення отриманого повідомлення у службове бінарне повідомлення;

- шифрування службового бінарного повідомлення;

- пересилання службового бінарного повідомлення на SMPP-сервер оператора стільникового зв'язку для його подальшого пересилання до МКП 1 для здійснення операції з обчислення ЕЦП або шифрування;

- отримання у відповідь зашифрованого службового бінарного повідомлення, яке включає обчислений ЕЦП, його розшифровування, формування попередньо визначеної структури даних та їх передачі до модуля MSSP-послуг 2.

Модуль протоколювання 4 забезпечує:

- протоколювання роботи послуг (збереження протягом визначеного строку даних щодо всіх операцій користувачів за всіма видами послуг за весь час);

- формування звітів за заданими критеріями;

- проставлення ЕЦП на сформованих звітах уповноваженими особами,

Модуль інтеграції 5 забезпечує:

- проставлення та перевірки ЕЦП, шифрування/дешифрування та надання інтерфейсів для здійснення цих операцій;

- надання інтерфейсів для підключення зовнішніх додатків/веб-сайтів до послуг, що надаються модулем MSSP-послуг 2;

- побудова захищеного каналу між підключеним зовнішнім ресурсом та серверами платформи.

Модуль адміністрування 6 забезпечує:

- адміністрування системи адміністраторами апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису", згідно з ролевою моделлю;

- адміністрування системи представниками оператора мобільного зв'язку 8, згідно з ролевою моделлю;

- адміністрування системи представниками АЦСК та ЦСК 7, згідно з ролевою моделлю;

- адміністрування системи представниками зовнішніх сервісів, згідно з ролевою моделлю;

- адміністрування системи представниками регулюючого органу, згідно з ролевою моделлю;

Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису реалізує такі механізми захисту:

- механізми контролю цілісності криптографічних перетворень та захисту ключових даних (для програмних засобів КЗІ контролю цілісності ПЗ);

- механізми надійного тестування засобу на правильність функціонування та блокування роботи в разі виявлення порушень;

- механізми захисту від порушення конфіденційності інформації внаслідок помилкових дій оператора або в разі відхилень у роботі складових елементів засобу КЗІ;

- механізми розмежування доступу до функцій засобу КЗІ, криптографічної схеми та ключових даних;

- механізми реалізації довіреного каналу для отримання інформації, що підлягає захисту;

- механізми знищення ключових даних після закінчення терміну їх дії;

- механізми захисту ключових даних на їх носіях від несанкціонованого зчитування;

- механізм захисту приватного ключа, що робить неможливим його отримання з захищеного носія інформації;

- механізми захисту засобу КЗІ від здійснення порушником навмисного зовнішнього впливу;

- механізми захисту від порушення конфіденційності та цілісності ключових даних на ключових документах.

Застосування ЕЦП реалізовано відповідно до ДСТУ 4145-2002, ДСТУ ETSI EN 119 312:2015 та ДСТУ ISO/IEC 14888-3:2014(2015).

Шифрування даних реалізовано за криптографічним алгоритмом відповідно до ДСТУ ГОСТ 28147:2009 у режимі гамування та ДСТУ ISO/IEC 18033-3:2015.

Генерацію сеансового ключа (256 біт) алгоритму шифрування, визначеного ДСТУ ГОСТ 28147:2009, реалізовано пристроєм функцій криптографічних перетворень за алгоритмом генерації псевдовипадкових послідовностей відповідно до вимог Додатку А ДСТУ 4145-2002 та методики, погодженої Держспецзв'язку встановленим порядком.

Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису використовує такі ключові дані:

- ключові дані генератора псевдовипадкових чисел ДСТУ ГОСТ 4145-2002;
- довгострокові ключові елементи для алгоритму ДСТУ ГОСТ 28147:2009;
- пари секретний/відкритий ключ (сертифікат відкритого ключа) алгоритму ДСТУ 4145-2002;
- пари секретний/відкритий ключ (сертифікат відкритого ключа) алгоритму ДСТУ ISO/IEC 14888-3:2014;
- пари секретний/відкритий ключ (сертифікат відкритого ключа) алгоритму ДСТУ ETSIEN 119 312:2015.

Секретні ключі зберігаються у спеціальних інформаційних об'єктах захищених ключових контейнерах під маскою, яка є індивідуальною для кожної криптографічної складової окремо.

Розподіл та використання ДКЕ для алгоритму ДСТУ ГОСТ 28147:2009 використовуються відповідно до вимог Інструкції про порядок постачання і використання ключів для засобів КЗІ, затвердженої наказом Адміністрації Держспецзв'язку від 12.06.07 №114. Термін дії довгострокових ключів 2 роки, ключових даних датчика псевдовипадкових чисел 2 роки.

Запропонований апаратно-програмний комплекс криптографічного захисту інформації забезпечує конфіденційність, цілісність та авторство інформації, яка передається та зберігається в автоматизованих системах класу 2 та 3 та криптографічного захисту інформації з обмеженим доступом, реалізацію національних криптографічних алгоритмів України ДСТУ 4145-2002, ДСТУ ГОСТ 28147-2009, ГОСТ 34.311-95 та національних і міждержавних криптографічних алгоритмів ДСТУ ISO/IEC 14888-3:2015. ДСТУ ETS1 EN 119 312:2015, ДСТУ ISO/IEC 18033-3:201 та FIPS PUB 180-4 "Secure Hash Standard" забезпечує використання пристрою функцій криптографічних перетворень та підтримку різних операційних систем, таких як 32, 64-розрядних сімейства Windows: 7, 8, 8.1, 10 +. Server 2008 R2, Server 2012 R2, Server 20161, 64-розрядних сімейства Linux з ядром 3.13 +, Ubuntu 14.04 і. віртуальна Java-машина.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

1. Апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису, який **відрізняється** тим, що містить:
- модуль криптографічних перетворень (МКП), виконаний з можливістю забезпечення генерації особистого та відкритого ключа, зберігання ключів в захищеній ділянці пам'яті, взаємодії з сервером оператора мобільного зв'язку, отримання/відправлення службових повідомлень, а також реалізації функцій криптографічних перетворень, можливість проведення криптографічних перетворень у фоновому режимі,
- модуль MSSP-послуг, виконаний з можливістю здійснення криптографічних перетворень, взаємодії з іншими складовими апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису, причому модуль MSSP-послуг спеціально пристосований для використання інтерфейсів підключення до серверів оператора стільникового зв'язку та взаємодії з зовнішнім АЦСК або ЦСК,
- модуль криптографічних та технологічних перетворень (МКТП), виконаний з можливістю:
- отримання пакетних даних у вигляді повідомлення від модуля MSSP-послуг, причому пакетні дані включають в себе основні дані попередньо визначеної структури і додаткові ідентифікаційні дані;
- перетворення отриманого повідомлення у службове бінарне повідомлення:
- шифрування службового бінарного повідомлення;
- пересилання службового бінарного повідомлення на SMPP-сервер оператора стільникового зв'язку для його подальшого пересилання до модуля МКП для здійснення операції з обчислення електронного цифрового підпису (ЕЦП), верифікації ЕЦП або шифрування;
- отримання у відповідь зашифрованого службового бінарного повідомлення, яке включає обчислений ЕЦП, його розшифровування, формування попередньо визначеної структури даних та їх передачі до модуля MSSP-послуг,
- модуль протоколювання, виконаний з можливістю реєстрації подій від модуля MSSP-послуг, криптографічного захисту інформації, причому модуль виконаний з можливістю:
- збереження протягом попередньо визначеного строку даних, асоційованих з усіма операціями користувачів за всіма видами послуг за весь час;
- формування звітів за заданими критеріями;
- проставлення ЕЦП на сформованих звітах автентифікованими особами, модуль інтеграції, виконаний з можливістю:
- проставлення та перевірки ЕЦП, шифрування/дешифрування та надання інтерфейсів для здійснення цих операцій;

- надання інтерфейсів для підключення зовнішніх додатків/веб-сайтів до послуг, що надаються модулем MSSP-послуг,
- побудови захищеного каналу зв'язку між підключеними зовнішніми сервісами, з якими взаємодіє апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису, та його серверами
- модуль адміністрування, виконаний з можливістю контролю підключення та роботи зовнішніх додатків та сервісів, регулювання ролевої моделі управління та доступу до апаратно-програмного комплексу електронної ідентифікації, регулювання розмежування наданих послуг, а також надання сервісів для зовнішніх додатків, для АЦСК та ЦСК, мобільних операторів та регуляторів, встановлених згідно з діючим законодавством,

при цьому модуль MSSP-послуг, МКТП, модуль протоколювання, модуль адміністрування поєднані за допомогою відокремленої мережі з окремою точкою доступу в мережі інтернет з модулем інтеграції, з МКП за допомогою службових повідомлень у захищеному каналі, створеним на обладнанні GSM-мережі оператора стільникового зв'язку.

2. Комплекс за п. 1, який **відрізняється** тим, що апаратно-програмний комплекс електронної ідентифікації з використанням мобільного електронного цифрового підпису додатково включає пристрій функцій криптографічних перетворень.

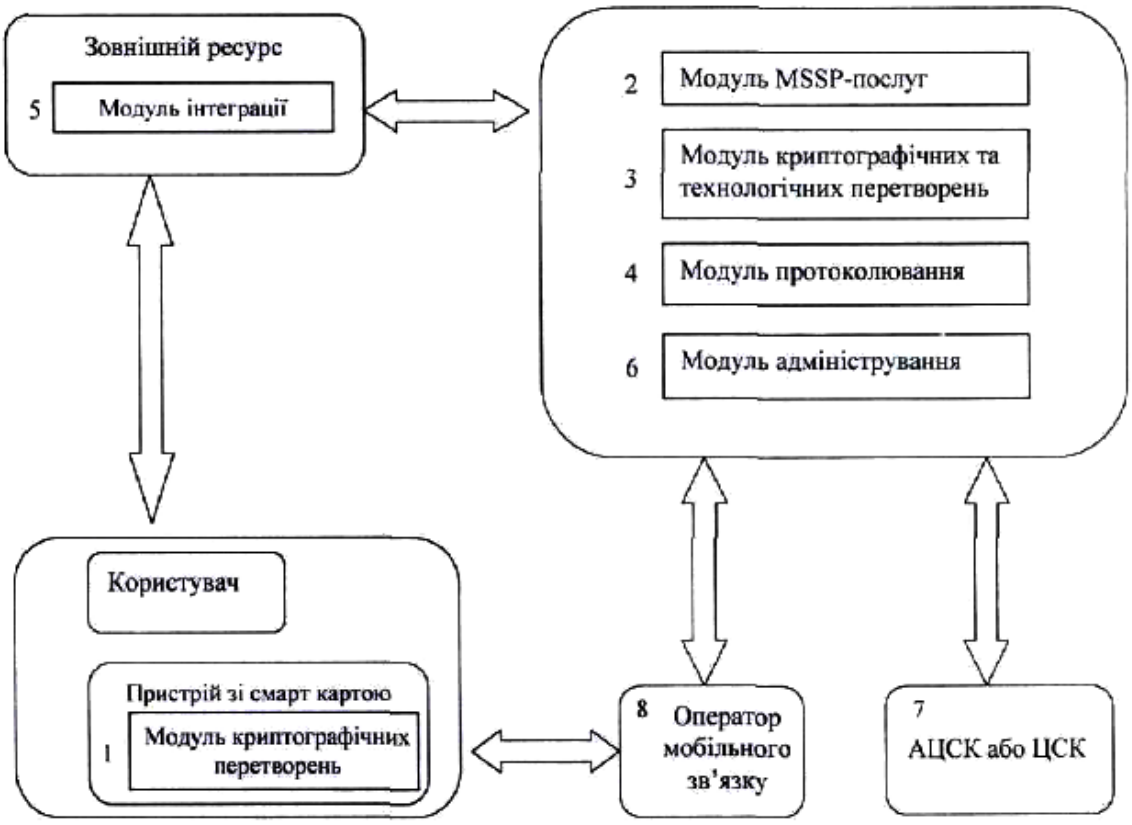
3. Комплекс за п. 2, який **відрізняється** тим, що пристрій функцій криптографічних перетворень реалізує генерацію сеансового ключа (256 біт) алгоритму шифрування, визначеного ДСТУ ГОСТ 28147:2009 відповідно до алгоритму генерації псевдовипадкових послідовностей згідно з ДСТУ 4145-2002.

4. Комплекс за будь-яким з попередніх пунктів, який **відрізняється** тим, що він додатково містить інтерфейс взаємодії з іншими складовими апаратно-програмного комплексу електронної ідентифікації з використанням мобільного електронного цифрового підпису.

5. Комплекс за будь-яким з попередніх пунктів, який **відрізняється** тим, що МКП є смарт-картою стандарту SWP з криптоконтролером серії SLE 97CNFX1M50PEI виробництва Infineon або аналогічних.

6. Комплекс за будь-яким з попередніх пунктів, який **відрізняється** тим, що він додатково виконаний з можливістю роботи з контактними SIM-картами згідно із стандартом ISO/IEC 7816.

7. Комплекс за будь-яким з попередніх пунктів, який **відрізняється** тим, що він додатково виконаний з можливістю застосування національних криптографічних алгоритмів України ДСТУ 4145-2002, ДСТУ ГОСТ 28147-2009, ГОСТ 34.311-95 та національних і міждержавних криптографічних алгоритмів ДСТУ ISO/IEC 14888-3:2015, ДСТУ ETSI EN 119 312:2015, ДСТУ ISO/IEC 18033-3:2015 та FIPS PUB 180-4 "Secure Hash Standard".



Фіг. 1

Комп'ютерна верстка Л. Ціхановська

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

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