**Тема 3. Електронний цифровий підпис**

1. Визначення терміну електронного цифрового підпису

2. Валідація цифрового підпису

3. Хеш-функція та принципи її роботи

4. Різниця цифрового та електронний підписів

**1. Визначення терміну електронного цифрового підпису**

Електронний цифровий підпис (або скорочено – ЕЦП) за правовим статусом прирівняний до власноручного підпису або печатки.

ЕЦП – це дані в електронній формі, отримані за результатами криптографічного перетворення, які додаються до інших даних або документів і забезпечують їх цілісність та ідентифікацію автора.

Надійний засіб електронного цифрового підпису — засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Одним із елементів обов'язкового реквізиту є електронний підпис, який використовується для аутентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Оригіналом електронного документа вважається електронний примірник з електронним цифровим підписом автора.

За допомогою послуг ЕЦП можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо. Документи, підписані за допомогою ЕЦП, мають таку саму юридичну силу, як і звичайні.

Станом на середину 2018 року близько 9 мільйонів фізичних осіб та представників юридичних осіб та вже мають ЕЦП, серед них третина – фізичні особи, фізичні особи-підприємці та самозайняті особи.

Отримати послуги ЕЦП фізична або юридична особа може в одному з Акредитованих центрів сертифікації ключів (АЦСК)

***Кваліфіковані надавачі електронних довірчих послуг***

|  |  |  |
| --- | --- | --- |
|  | Назва юридичної особи | Назва кваліфікованого надавача електронних довірчих послуг |
|  | [АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"](https://czo.gov.ua/ca-registry-details?type=0&id=93) | [Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ "ПРИВАТБАНК"](https://czo.gov.ua/ca-registry-details?type=0&id=93) |
|  | [Військова частина 2428](https://czo.gov.ua/ca-registry-details?type=0&id=119) | [Кваліфікований надавач електронних довірчих послуг "Військова частина 2428" Державної прикордонної служби України](https://czo.gov.ua/ca-registry-details?type=0&id=119) |
|  | [Генеральний штаб Збройних Сил України](https://czo.gov.ua/ca-registry-details?type=0&id=117) | [Кваліфікований надавач електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"](https://czo.gov.ua/ca-registry-details?type=0&id=117) |
|  | [Офіс Генерального прокурора](https://czo.gov.ua/ca-registry-details?type=0&id=125) | [Кваліфікований надавач електронних довірчих послуг органів прокуратури України](https://czo.gov.ua/ca-registry-details?type=0&id=125) |
|  | [Державна казначейська служба України](https://czo.gov.ua/ca-registry-details?type=0&id=100) | [Кваліфікований надавач електронних довірчих послуг Державної казначейської служби України](https://czo.gov.ua/ca-registry-details?type=0&id=100) |
|  | [Акціонерне товариство "Оператор ринку"](https://czo.gov.ua/ca-registry-details?type=0&id=118) | [Кваліфікований надавач електронних довірчих послуг "АЦСК ринку електричної енергії"](https://czo.gov.ua/ca-registry-details?type=0&id=118) |
|  | [Державне підприємство "ДІЯ"](https://czo.gov.ua/ca-registry-details?type=0&id=116) | [Кваліфікований надавач електронних довірчих послуг "ДІЯ"](https://czo.gov.ua/ca-registry-details?type=0&id=116) |
|  | [Державне підприємство "Українські спеціальні системи"](https://czo.gov.ua/ca-registry-details?type=0&id=112) | [Кваліфікований надавач електронних довірчих послуг Державного підприємства "Українські спеціальні системи"](https://czo.gov.ua/ca-registry-details?type=0&id=112) |
|  | [Інформаційно-довідковий департамент ДПС](https://czo.gov.ua/ca-registry-details?type=0&id=97) | [Кваліфікований надавач електронних довірчих послуг Інформаційно-довідкового департаменту ДПС](https://czo.gov.ua/ca-registry-details?type=0&id=97) |
|  | [Міністерство внутрішніх справ України](https://czo.gov.ua/ca-registry-details?type=0&id=122) | [Кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів МВС України](https://czo.gov.ua/ca-registry-details?type=0&id=122) |
|  | [Національний банк України](https://czo.gov.ua/ca-registry-details?type=0&id=124) | [Кваліфікований надавач електронних довірчих послуг "Акредитований центр сертифікації ключів Національного банку України"](https://czo.gov.ua/ca-registry-details?type=0&id=124) |
|  | [Акціонерне товариство "Державний ощадний банк України"](https://czo.gov.ua/ca-registry-details?type=0&id=123) | [Кваліфікований надавач електронних довірчих послуг - центр сертифікації ключів акціонерного товариства «Державний ощадний банк України»](https://czo.gov.ua/ca-registry-details?type=0&id=123) |
|  | [Товариство з обмеженою відповідальністю "Арт-мастер"](https://czo.gov.ua/ca-registry-details?type=0&id=85) | [Кваліфікований надавач електронних довірчих послуг "MASTERKEY"](https://czo.gov.ua/ca-registry-details?type=0&id=85) |
|  | [Товариство з обмеженою відповідальністю "Центр сертифікації ключів "Україна"](https://czo.gov.ua/ca-registry-details?type=0&id=96) | [Кваліфікований надавач електронних довірчих послуг ТОВ "Центр сертифікації ключів "Україна"](https://czo.gov.ua/ca-registry-details?type=0&id=96) |
|  | [Філія "Головний інформаційно-обчислювальний центр" акціонерного товариства "Українська залізниця"](https://czo.gov.ua/ca-registry-details?type=0&id=89) | [Кваліфікований надавач електронних довірчих послуг ЦСК АТ "УКРЗАЛІЗНИЦЯ"](https://czo.gov.ua/ca-registry-details?type=0&id=89) |

**2. Валідація цифрового підпису**

Процедера перевірки ЕД полягає у перевірці наявності всіх його обовязкових реквізитів та його цілісності шляхом перевірки та підтвердження КЕП та/або печатки.

**Валідація** – процес верифікації та підтвердження того, що підпис валідний (дійсний).

**Політика валідації підпису** – набір правил, що застосовуються до одного або кількох цифрових підписів, який визначає технічні та процедурні вимоги для їх валідації, з метою задоволення конкретної бізнес-потреби та під яким цифрові підписи можуть бути визнані як валідні.

**Обмеження підпису** – абстрактне формулювання правил, значень, діапазонів і результатів обчислень згідно з якими цифровий підпис може пройти валідацію. Обмеження бувають:

- *Криптографічні* – накладання обмежень по конфіденційності, цілісності і автентичності інформації за допомогою математичних методи забезпечення;

- *Обмеження на валідацію* – непідтвердження законності підпису;

- *Обмеження елементів підпису*;

- *Інші обмеження*.

Криптографічний захист (шифрування) інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Методи криптографії поділяють на дві групи – підставлення (заміни) і переставлення. Підстановний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза – ключ. У загальному випадку у криптографії ключ – це послідовність бітів, що використовуються для шифрування та розшифрування даних.

Подібний шифр дуже швидко можна розкрити, вивчивши повторюваність символів та короткі слова «і», «або», «за» і т. ін. У разі використання перестановного алгоритму змінюються не символи, а порядок їх розміщення в повідомленні.

**Залежно від доступності ключів розрізняють:**

*- симетричне шифрування* – для шифрування і розшифрування використовується один ключ. Такі системи із закритим ключем реалізовані, наприклад, в архіваторах даних. Це зручно для шифрування приватної інформації, але під час передавання повідомлення по каналах зв’язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування. У принципі, якщо можна таємно передати ключ, то можна передати і таємну інформацію, тоді відпадає необхідність у шифруванні, а якщо такої можливості немає, шифрування даремне;

- *асиметричне* – для шифрування використовується один, відкритий (публічний, загальнодоступний) ключ, а для дешифрування – інший, закритий (секретний, приватний). Це робить непотрібним таємне передавання ключів між кореспондентами. Відкритий ключ безплідний для дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи – ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати. Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA, названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970—х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

**Стани повної валідації:**

- TOTAL PASED – криптографічні перевірки підпису а також віс перевірки передбачен політикою конфіденційностівалідації підпису пройшли успішно.

- TOTAL FAILED – криптографічні перевірки підпису не вдалися або доведено, що генерація підпису відбувалася після анулювання сертифіката підписання або тому що підпис не відповідає одному з базових стандартів у тій мірі, в якій складова частина криптографічної верифікації не може обробити його.

- INDETERMINATE:

- результати проведених перевірок не дозволяють встановити, що підпис TOTAL PASED або TOTAL FAILED;

- якщо докладна інформація вказує, що результат може змінитися при повторному виконанні алгоритму перевірки, то можна повторити валідацію на основі додаткової інформації або пізніше у часі.

**3. Хеш-функція та принципи її роботи**

***Хеш-функція*** -це спеціальна програма, яка перетворює будь-яку пропущену через неї інформацію в хеш або дайджест - унікальну комбінацію букв і цифр заданої довжини. Будь-яка зміна початкових даних призведе до формування зовсім іншого хеша. Саме тому більшість систем на основі блокчейн активно використовує цей метод шифрування даних.

**Принципи роботи**

*1. Хешування даних*. Вкрай важливий момент при роботі з блокчейном (**blockchain** - розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків), що постійно довшає). Незважаючи на те, що для верифікації даних досить підписування свого імені на основі приватного ключа, цей підпис завжди пропускають через власні хеш-алгоритми. Просто для того, щоб отримати дайджест заданої довжини і формату, з яким куди простіше працювати системі.

*2. Підпис.* Існує ряд односпрямованих алгоритмів, які формують цифровий підпис на основі приватного ключа. І інших алгоритмів, що дозволяють підтвердити справжність отриманого результату на основі публічного ключа. Крім того, варто враховувати, що даний спосіб підтвердження формується не тільки на основі приватного ключа, а й з урахуванням вмісту повідомлення. Тому в кожному конкретному випадку він буде унікальним. Що робить неможливою «сліпу підстановку» одного цифрового підпису для підтвердження іншого вмісту.

*3. Перевірка.* Приватний ключ завжди один, тоді як публічних може бути безліч. І кожен власник публічного може за допомогою спеціальних алгоритмів переконатися в тому, що прийняте повідомлення підписано саме приватним ключем, але без розуміння його вмісту. Тому основне завдання будь-якого шахрая - за всяку ціну заволодіти приватним ключем. На щастя, класичні методи соціальної інженерії тут не підходять - тільки пряме перехоплення повідомлень що вводяться.

*Що дає цей спосіб підтвердження:*

- *Цілісність даних* - кожний власник публічного ключа може упевнитися в достовірності інформації, зашифрованої приватним , без розшифровки її змісту.

- *Аутентифікація - к*ожний власник публічного ключа може переконатися, що має справу з володарем приватного.

- *Незмінність -* дані, зашифровані приватним ключем, однозначно належать його власнику. І угоди, здійснені на таких умовах, не мають зворотної сили.

**Можливі недоліки при роботі із хеш-функцією:**

-*Проблеми алгоритму* - якщо хеш-функція недостатньо складна, стає набагато простіше розшифрувати зміст цифрового підпису.

- *Проблеми реалізації* - навіть повністю робочий цифровий підпис не допоможе, якщо кінцева програма її не сприймає.

- *Проблема власності* - втрата приватного ключа - найстрашніше, що може трапитися з власником криптовалютных активів. Це все одно, що особисто відкрити двері перед грабіжниками і детально їм розповісти, де лежать цінності в будинку.

**4. Різниця цифрового та електронний підписів**

Якщо коротко, то кожний цифровий підпис - електронна. А ось зворотне правило працює далеко не завжди. Цифровими є лише ті підписи, які використовують при своєму створенні криптографію з відкритим ключем, хеш-функції і різноманітні методи шифрування.

**Варіанти використання:**

- Інформаційні технології. За допомогою цієї технології можна домогтися куди більшої безпеки інтернет-комунікації.

- Фінанси. Аудит, кредити, звіти про витрати та інші документи, скріплені підписом, підробити і змінити заднім числом практично нереально.

- Юриспруденція. Ділові угоди і контракти, в тому числі і самого високого (урядового) рівня.

- Охорона здоров'я. Незмінні рецепти і медичні дані.

- Блокчейн. Достовірність переданої інформації. Підтвердження криптовалютних транзакцій.

Отже, використання цифрових підписів, а також унікальних алгоритмів кодування і шифрування, привело до створення унікальних електронних даних. Це та сама основа, на якій збудована сучасна система криптовалюти.

Цифрові підписи - головне підтвердження достовірності криптовалютних транзакцій, які свідчать про те, що монети витрачає людина, яка реально ними володіє.

Однак тільки однією криптоекономікою застосування даного способу захисту інформації не обмежується. Практично будь-яка галузь людської діяльності, в якій йде мова про унікальну електронну інформацію, може бути адаптована під використання даного способу підтвердження.