ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

1. Урядовий портал

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.

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), повний перелік яких наведено в Електронному реєстрі суб'єктів, які надають послуги, пов'язані з ЕЦП

Основні відомості

Перші активні спроби використання електронних документів у комерційних інформаційних системах, перш за все банківських, почалися ще наприкінці 60-х років. Вони привели до появи нової технології оформлення документа в електронному вигляді та так званого "цифрового або електронного підпису" (ЕЦП).

Для чого потрібен ЕЦП

Електронно-цифровий підпис (ЕЦП) ставиться під електронним документом з тією ж метою, як і звичайний ручний підпис під паперовим документом:

- ✓ Для перевірки, що електронний документ створено саме особою, яка поставила під ним свій ЕЦП
- ✓ Для гарантії того, що електронний документ не змінювався після його підписання

При цьому цифровий підпис має таку ж юридичну силу, як і звичайний.

Основні визначення

Закритий ключ – рядок символів, згенерований для конкретного користувача (унікальний рядок). Зберігається у користувача.

Відкритий ключ – рядок символів, згенерований для конкретної людини (унікальний рядок), і пов'язаний із закритим ключем математичною залежністю. Зберігається в базі даних. Відкритий ключ працює тільки в парі із закритим ключем. На відкритий ключ видається сертифікат, який автоматично передається разом із листом, підписаним ЕЦП. Потрібно забезпечити наявність свого відкритого ключа у всіх, з ким Ви маєте намір обмінюватися підписаними документами. Дублікат відкритого ключа надсилається в Посвідчувальний центр, де зберігається бібліотека відкритих ключів ЕЦП. У бібліотеці посвідчувального центру забезпечується реєстрація та надійне зберігання відкритих ключів, щоб уникнути спроб підробки або внесення спотворень.

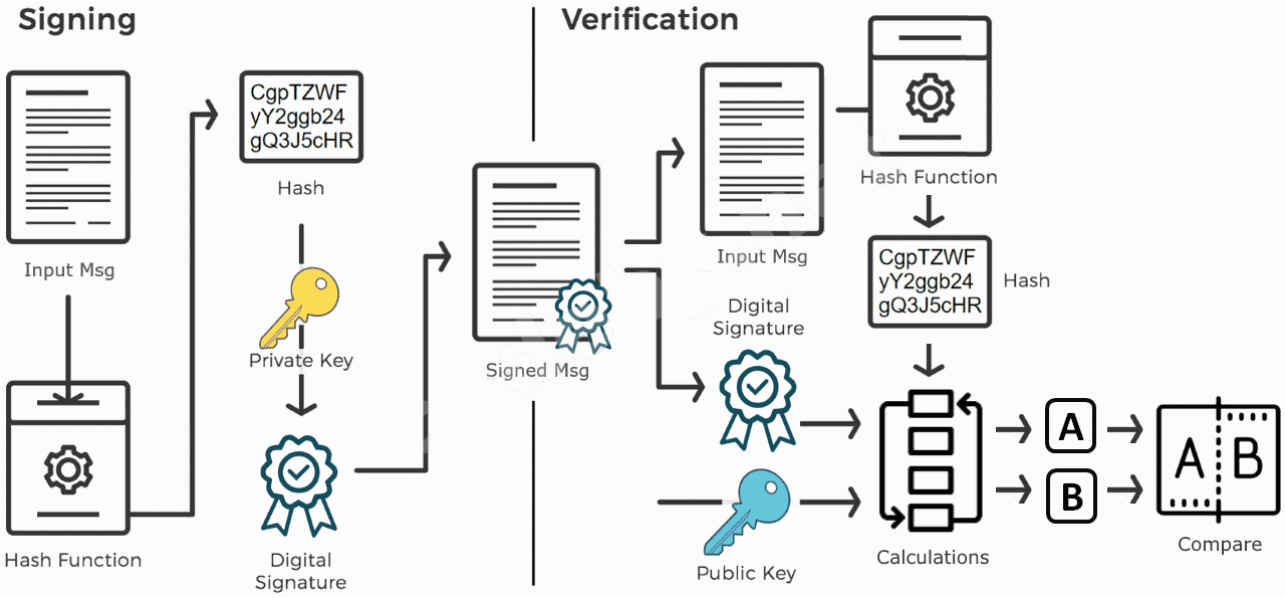
Результат перевірки підпису – твердження **ТАК / НІ**, отримане в результаті криптоперетворення з файлу з ЕЦП та відкритого ключа.

Принцип створення ЕЦП

У роботі ЕЦП використовуються два ключі секретний і відкритий, що належать автору.

Електронний документ підписується автором із використанням свого **секретного ключа**. В результаті виходить підписаний електронний документ, тобто пара – (Документ, ЕЦП автора до цього документа).

Секретний ключ зберігається на комп'ютері автора у зашифрованому вигляді. Як зрозуміло з назви, свій секретний ключ автор не повинен нікому повідомляти. При будь-якій підозрі про втрату секретності ключа (його компрометації) автор повинен негайно замінити свій комплект ключів. Відкритий ключ автора передається одержувачам і використовується ними для перевірки справжності ЕЦП.



АЛГОРИТМ ПОБУДОВИ ЕЦП НА ОСНОВІ АСИМЕТРИЧНОГО ШИФРУВАННЯ

1. Генерація ключів
2. Створення підпису
3. Перевірка (верифікація) підпису

Для того, щоб відправник зміг передати одержувачу документ разом з цифровим підписом, а одержувач переконатися в тому, що він отримав справжній документ, необхідно виконати наступні дії:

Генерація ключів

Ключі надаються ПІДПИСУВАЧУ (автору документа) кваліфікованим надавачом електронних довірчих послуг – **акредитованим Центром сертифікації ключів** (див. https://czo.gov.ua/ca-registry)

Створення ЕЦП

ВІДПРАВНИК (автор документа):

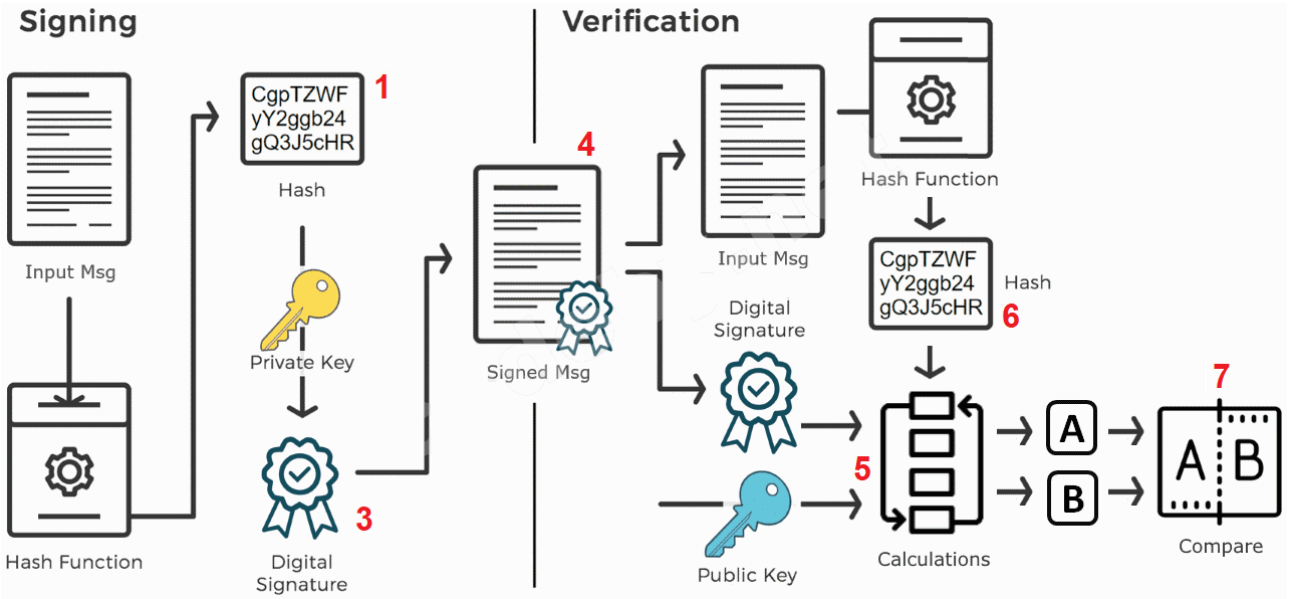
1. Обчислює хеш-код документа.
2. З хеш-коду та інших метаданих (дата підписання, ім'я підписанта та ін.) формує відкритий текст M.
3. Шифрує текст M закритим ключем (private key) і одержує підпис.
4. Передає одержувачу відкритий ключ, документ та підпис:

RSA: (e, n) $\boldsymbol{(M, S(h(M))}$

Перевірка ЕЦП

ОДЕРЖУВАЧ:

5. Розшифровує підпис публічним ключем (public key) відправника та отримує відкритий текст M — хеш-код та метадані.
6. Обчислює хеш-код документа.
7. Порівнює хеш-коди з пунктів 5 і 6. **Якщо вони рівні, то підпис вірний**.
8. Перевіряє метадані.



Результат верифікації підпису **ТАК** підтверджує 2 факти:

- даний документ був підписаний власником секретного ключа;
- у документі відсутні зміни.

Якщо звірка дала негативний результат, то або документ був підписаний не автором, або зміст документа було змінено після його підписання. В обох випадках такому документу вірити не можна.

Підписати документ від імені автора з використанням відкритого ключа неможливо. Тому свій відкритий ключ автор може повідомляти будь-якій особі, з якою він збирається обмінюватися електронними документами. Додатковий захист від підробки підпису забезпечується Центром сертифікації ключів.