УДК 621.39

ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ І СЕРТИФІКАТІВ ДЛЯ БЕЗПЕКИ ТРАНЗАКЦІЙ І ПІДТВЕРДЖЕННЯ СПРАВЖНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Григоренко О.Г., Реута Г.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, glebreuta14@gmail.com

DIGITAL SIGNATURES AND CERTIFICATES USING FOR SECURE TRANSACTIONS AND CONFIRMATION OF THE ELECTRONIC DOCUMENTS AUTHENTICITY

Analyzed features of digital signatures and certificates and the advantages of their use in various areas of modern life, which allows safe transactions on the Internet and confirm the authenticity of electronic documents.

Проаналізовані особливості цифрових підписів та сертифікатів та переваги їх використання в різних сферах сучасного життя, що дозволяє безпечно проводити транзакції в мережі Інтернет та підтверджувати справжність електронних документів.

Цифрові підписи та сертифікати використовуються у різних сферах нашого життя. «Зелене світло» для широкого застосування електронних документів та цифрового підпису в Україні дали Закон “Про електронні документи та електронний документообіг” та Закон “Про ЕЦП” [1,2]. В Україні використання цих технологій є надзвичайно актуальним через війну, а раніше локдаун.

Цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача [2,4,5]. Електронний цифровий підпис (ЕЦП) накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Ілюстрація цифрового підпису показана на рис.1.

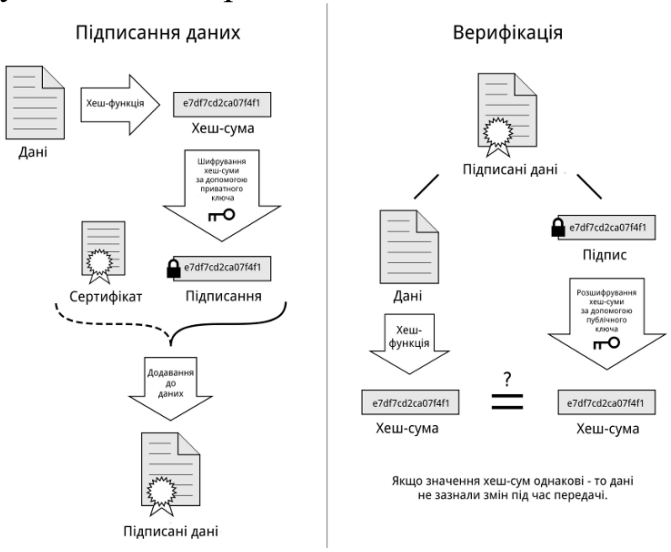

Рис.1. Ілюстрація цифрового підпису даних [7].

Цифровий підпис складається з двох частин:

перша — відкрита для тих сторін, що обслуговують програмне забезпечення, яке використовує та допомагає складати електронні документи, відправляє та отримує електронні документи, — ця частина дозволяє таким сторонам ідентифікувати особу;

друга — секретна частина створюється лише власником підпису, це є пароль власника, яким він користується, щоб створити електронний цифровий підпис та потім підписувати ним електронні документи.

Гарантії цифрового підпису забезпечуються його особливостями [3]:

- **Автентичність.** Підтверджується особа, яка підписала документ.
- **Цілісність.** Вміст не змінено або не підроблено після того, як на ньому поставлено цифровий підпис.
- **Неможливість відмови.** Підтверджує для всіх сторін походження підписаного вмісту. Відмова – це заперечення автором підпису своєї причетності до підписаного вмісту.
- **Нотаріальне засвідчення.** Підписи у файлах, наприклад, Microsoft Word, Microsoft Excel або Microsoft PowerPoint із позначкою часу від надійного сервера позначок часу за певних умов прирівнюються до нотаріального засвідчення.

Сертифікат — це цифровий документ, який використовується для підтвердження справжності цифрового підпису. Він видається Центром сертифікації і містить інформацію про власника підпису та ключ, до якого він був створений. Сертифікат може бути використаний для перевірки справжності та цілісності даних, які були створені за допомогою відповідного цифрового підпису.

Цифрові сертифікати використовуються для перевірки організації або окремого користувача, а також для аутентифікації веб-сайту постачальника і встановлення зашифрованого з'єднання для обміну конфіденційними даними. Якщо цифровий сертифікат відповідає стандартній структурі, то його може прочитати та зрозуміти будь-яка система незалежно від того, ким він був виданий. X.509 є стандартом для інфраструктури відкритих ключів (PKI - public key infrastructure) для керування цифровими сертифікатами.

Найпоширеніші приклади використання цифрових підписів та сертифікатів (ЦПС) у різних галузях включають: електронну комерцію (для безпечної аутентифікації електронних платежів та забезпечення конфіденційності та цілісності електронних транзакцій між різними сторонами), банківський сектор, державну та муніципальну сфери, медичну сферу (для підписання та обміну медичними документами та рецептами), корпоративну сферу, Інтернет-безпеку (для перевірки справжності та цілісності веб-сайтів та захисту користувачів від фішингу та інших типів шахрайства), інтелектуальну власність (для захисту авторських прав і патентів).

На онлайн-платформі державних послуг ДІЯ за допомогою ЕЦП можна отримати послуги щодо отримання грантів для розвитку малого та середнього бізнесу, електронний кабінет пенсійного фонду, електронний кабінет водія тощо [6].

Найбільш поширеними є три алгоритми цифрового підпису - Digital

Signature Algorithm (**DSA)**, Rivest-Shamir-Adleman (**RSA**) і Elliptic Curve Digital Signature Algorithm (**ECDSA**). Всі три алгоритми містять механізми створення та перевірки цифрових підписів і функціонують **на основі асиметричного шифрування** з використанням відкритих ключів. Операції генерації ключа та перевірки вимагають шифрування і дешифрування ключів.Також була представлена розширена криптосистема цифрового підпису Меркле (XMSS), яка має пряму секретність та стійкість до криптоаналізу із використанням квантових комп'ютерів [7].

Алгоритм DSA базується на складності обчислень дискретних логарифмів. Можливості алгоритму DSA обмежуються формуванням та перевіркою цифрового підпису. RSA є найбільш поширеним алгоритмом і може використовуватися не тільки для роботи з цифровими підписами, а також для шифрування повідомлення. DSA працює швидше, ніж RSA, в якості підпису для цифрового документа. Алгоритм RSA краще підходить для ситуацій, коли крім вимог підпису і перевірки електронних документів необхідне ще й шифрування повідомлень. Алгоритм RSA базується на двох математичних компонентах: модульній арифметиці і задачі факторизації великих цілих чисел. ECDSA поступово замінює RSA тому, що ECDSA може використовувати набагато менші розміри ключа при такому ж рівні безпеки і вимагає значно менших об'ємів обчислень, ніж RSA.

Надзвичайно важливим є використання позначок часу при застосуванні ЕЦП, бо їх відсутність призводить до критичної вразливості і дозволяє реалізувати атаки на ЕЦП [7]. Це пов'язано з особливостями застосування ЕЦП, щодо документів, термін дії яких перевищує термін дії ЕЦП. Валідність таких документів перевіряється тільки на момент підпису. Прикладом таких документів є подача електронної звітності.

Перераховані вище особливості електронного цифрового підпису є ефективним інструментом забезпечення інформаційної безпеки на всіх рівнях інфраструктури суспільства та держави. Окрім цього перехід до електронного документообігу дозволяє зберігати ліси, зменшувати кількість підприємств з виробництва паперу, що призводить до енергозбереження та захисту довкілля в результаті.

Література

1. Закон України від 22.05.2003 р. №851-IV «Про електронні документи та електронний документообіг».
2. Закон України від 22.05.2003 р. №852-IV «Про електронний цифровий підпис».
3. https://support.microsoft.com/uk-ua/office/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96-%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81%D0%B8-%D1%82%D0%B0-%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%B8-8186cd15-e7ac-4a16-8597-22bd163e8e96
4. https://online.dtkt.ua/2012/20/50377
5. Цифровий електронний підпис // Юридична енциклопедія : [у 6 т.] / ред. кол.: Ю. С. Шемшученко (відп. ред.) [та ін.]. — К. : Українська енциклопедія ім. М. П. Бажана, 2004. — Т. 6 : Т — Я. — 768 с. — ISBN 966-7492-06-0.
6. https://pravokator.club/news/elektronnyj-tsyfrovyj-pidpys-osoblyvosti-vykorystannya/
7. https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81