Дослідження електронного підпису як елемента цифрової ідентичності

Study of the Electronic Signature as an Element of Digital Identity

Іванна Хомич [A]
Corresponding author: студентка кафедри захисту інформації, e-mail: ivanna.khomych.kb.2021@lpnu.ua, ORCID: 0009-0005-3307-6276

Анастасія Швець [A]
студентка кафедри захисту інформації, e-mail: anastasiia.shvets.kb.2021@lpnu.ua, ORCID: 0009-0008-5148-761X

Соломія Сорока [A]
студентка кафедри " захисту інформації, e-mail: solomiia.soroka.kb.2021@lpnu.ua, ORCID: 0009-0001-8124-647X

Роман Кутень [A]
Ph.D, e-mail: roman.b.kuten@lpnu.ua, ORCID: 0000-0002-5688-2976

[A] Національний університет "Львівська політехніка", м. Львів, Україна

Ivanna Khomych [A]
Corresponding author: Cybersecurity Department Student, e-mail: ivanna.khomych.kb.2021@lpnu.ua, ORCID: 0009-0005-3307-6276

Anastasiia Shvets [A]
Cybersecurity Department Student, e-mail: anastasiia.shvets.kb.2021@lpnu.ua, ORCID: 0009-0008-5148-761X

Solomiia Soroka [A]
Cybersecurity Department Student, e-mail: solomiia.soroka.kb.2021@lpnu.ua, ORCID: 0009-0001-8124-647X

Roman Kuten [A]
Ph.D, e-mail: roman.b.kuten@lpnu.ua, ORCID: 0000-0002-5688-2976

[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: May 16, 2025 | Revised: June 22, 2025 | Accepted: June 30, 2025

DOI: 10.33445/sds.2025.15.3.17

Мета роботи: виявлення основних технічних та правових механізмів, що забезпечують надійність електронного підпису як складової цифрової ідентичності, зокрема його здатність гарантувати автентифікацію користувача, цілісність електронних документів і юридичну силу підписів.

Метод дослідження: порівняльний аналізі правових і технічних підходів.

Результати дослідження: Дослідження виявило суттєві відмінності між підходами до електронного підпису в США та ЄС: у США юридична сила базується на намірі підписанта, а в ЄС — на високих стандартах безпеки та кваліфікованих підписах (QES), прирівняних до власноручних. Україна інтегрувала європейську модель, запровадивши КЕП, що відповідає eIDAS і гарантує юридичну силу цифрової ідентичності. Кваліфіковані надавачі довірчих послуг забезпечують ідентифікацію, захист ключів і відкликання сертифікатів, мінімізуючи ризики. Виявлено, що КЕП ефективний у боротьбі з дезінформацією завдяки автентичності, цілісності та невідмовності. Впровадження ШІ та міжнародна інтероперабельність є ключовими для розвитку цифрової ідентичності.

Теоретична цінність дослідження: У роботі узагальнено визначення цифрової ідентичності та електронного підпису в межах стандартів NIST, eIDAS та українського законодавства, що дозволяє сформувати єдиний підхід до розуміння цих понять.

Практична цінність дослідження: Електронні підписи є ефективними інструментами для автентифікації користувача, перевірки цілісності документів і протидії дезінформації шляхом верифікації джерела контенту.

Перспективи подальших досліджень: До перспективних напрямів належать інтеграція біометрії, використання ШІ для верифікації підписів та забезпечення інтероперабельності між юрисдикціями.

Тип статті: теоретична.

Ключові слова: електронний підпис; цифрова ідентичність; кваліфікований електронний підпис; автентифікація; достовірність контенту.

Purpose: to identify the key technical and legal mechanisms that ensure the reliability of electronic signatures as a component of digital identity, particularly their ability to guarantee user authentication, document integrity, and the legal validity of signatures. Special attention is given to the role of qualified trust service providers, the protection of private keys, and the potential use of electronic signatures to combat misinformation.

Method: comparative analysis of legal and technical frameworks.

Findings: The study revealed significant differences between electronic signature approaches in the USA and the EU: in the USA, legal validity is based on the signer's intent, while in the EU it relies on high security standards and qualified electronic signatures (QES) equivalent to handwritten ones. Ukraine has integrated the European model by adopting the qualified electronic signature (QES), compliant with eIDAS, ensuring the legal validity of digital identity. Qualified trust service providers ensure user identification, key protection, and certificate revocation, minimizing risks. It was found that QES is effective in combating disinformation by guaranteeing authenticity, integrity, and non-repudiation. The implementation of AI and international interoperability are key to advancing digital identity development.

Theoretical implications: The study consolidates digital identity and e-signature definitions across NIST, eIDAS, and Ukrainian frameworks, bridging technical standards with legal interpretations into a unified perspective.

Practical implications: Electronic signatures are effective tools for user authentication, verifying document integrity, and combating misinformation by authenticating the source of content.

Value: The study highlights the dual significance of the Qualified Electronic Signature (QES) as both a legal instrument and a cybersecurity tool and reveals its role in ensuring the authenticity of digital content.

Future research: Future work should explore biometric integration, AI-driven signature verification, and cross-jurisdictional interoperability of e-signature systems.

Papertype: theoretical.

Key words: electronic signature, digital identity, qualified electronic signature, authentication, content provenance.

Вступ

У сучасну епоху стрімкого розвитку цифрових технологій дедалі більше процесів переходять в онлайн-середовище. Віддалена робота та електронні послуги стирають географічні межі між постачальниками і споживачами, дозволяючи ефективну співпрацю незалежно від місця перебування. В умовах такого глобального цифрового середовища електронний підпис набуває особливого значення, виконуючи роль інструмента, що забезпечує достовірність та юридичну силу взаємодії сторін на відстані. Завдяки використанню електронного підпису стало можливим підписувати і засвідчувати документи між учасниками, які знаходяться у різних частинах світу, без потреби фізичної присутності чи обміну паперовими копіями. Це значно зменшує бюрократичне навантаження та спрощує доступ до адміністративних, фінансових та комерційних послуг онлайн. Ба більше, електронний підпис сьогодні є не лише технічним засобом, а й ключовим елементом цифрової ідентичності – способом підтвердження особи в електронному просторі.

Актуальність теми полягає в тому, що цифрова ідентичність стала фундаментом довіри в кіберпросторі, а електронний підпис – одним з головних механізмів її реалізації. Метою дослідження є аналіз ролі електронного підпису як складової цифрової ідентичності, з особливою увагою до його безпекових характеристик та правового регулювання в сучасному цифровому середовищі. В рамках цього дослідження акцентовано проблематику захисту приватного ключа, довірчих відносин між користувачем і постачальником послуг, а також нормативні вимоги, що визначають правовий статус електронного підпису в Україні та Європейському Союзі. Вступ окреслює загальну проблематику та значущість електронного підпису для забезпечення довіри в цифрових взаємодіях; далі розглянемо теоретичні основи поняття цифрової ідентичності й електронного підпису, визначимо дослідницьке питання, методологію, а також представимо результати й обговорення отриманих висновків.

Теоретичні основи дослідження

У сфері електронного врядування, онлайн-банкінгу та інших цифрових сервісів поняття *цифрової ідентичності* набуває ключового значення, оскільки вона дозволяє однозначно пов’язати конкретну людину (або організацію) з її діями в інформаційному просторі. Згідно з рекомендаціями NIST SP 800-63-3, цифрова ідентичність визначається як унікальне представлення суб’єкта, залученого до цифрової транзакції, що є унікальним в межах певної системи, але не обов’язково розкриває особу поза цією системою [1]. Інакше кажучи, користувач може мати дійсну цифрову ідентичність у конкретному сервісі без розкриття свого реального імені чи особистих даних [1]. Відповідно до українського законодавства, хоча сам термін *“цифрова ідентичність”* прямо не визначено, у Законі України “Про електронну ідентифікацію та електронні довірчі послуги” фактично закладено це поняття через визначення процесу електронної ідентифікації – як використання сукупності електронних даних для унікального встановлення фізичної або юридичної особи в електронному середовищі [3]. Електронна ідентифікаційна інформація трактується як набір електронних даних, що дозволяють здійснити таку ідентифікацію, що підтверджує наявність концепції цифрової ідентичності на практиці, навіть якщо сам термін відсутній у нормативній лексиці. Таким чином, цифрова ідентичність є багатовимірним поняттям, яке охоплює як технічні способи перевірки особи (ідентифікації та автентифікації), так і правові механізми визнання цих процесів у різних юрисдикціях.

Цікаво, що поняття цифрової ідентичності поступово інтегрується й у публічний дискурс в Україні. Зокрема, на державній платформі “Дія.Освіта” розроблено окремий освітній модуль, присвячений цифровій ідентичності, де вона описується як спосіб підтвердження особи в інтернеті за допомогою таких інструментів, як електронний підпис, BankID, Mobile ID та

біометричні рішення [4]. Це свідчить про поступову гармонізацію українського підходу з міжнародними стандартами, особливо у сфері електронних послуг і електронного урядування. У світлі цього, електронний підпис можна розглядати як один із ключових інструментів реалізації цифрової ідентичності, що поєднує в собі технічну складову (криптографічну автентифікацію) з юридично значущою дією (підписанням документа).

Електронний підпис (ЕП) у найзагальнішому вигляді – це технологія, що дозволяє встановити зв'язок між певною особою та електронним документом (або транзакцією) шляхом криптографічного підтвердження. Різні нормативні та стандартизуючі документи надають власні визначення електронного підпису, акцентуючи увагу на різних аспектах. Згідно із законодавством України, електронний підпис визначається як "електронні дані, що додаються до інших електронних даних або логічно з ними пов'язані і використовуються підписувачем як підпис" [3]. Це визначення підкреслює технічну сутність ЕП як спеціальних даних (коду, зашифрованого хешу тощо), що додаються до документа і виконують функцію, аналогічну власноручному підпису, але в цифровому форматі. Дуже близьке за змістом визначення міститься і в європейському законодавстві: Регламент (ЄС) № 910/2014 (відомий як eIDAS) описує електронний підпис практично тими самими словами – як "дані в електронній формі, що прикріплені або логічно пов'язані з іншими електронними даними та використовуються підписувачем для підписання" [2]. Спільним у цих підходах (українському та європейському) є те, що електронний підпис розглядається не як окремий фізичний об'єкт, а як невід'ємна частина електронного документу чи транзакції, яка гарантує автентичність підписанта і його волевиявлення.

Водночас американський підхід, закріплений у федеральному законі США "Electronic Signatures in Global and National Commerce Act" (ESIGN Act), має більш широку інтерпретацію. Там електронний підпис визначено як "електронний звук, символ або процес, прикріплений чи логічно пов'язаний з контрактом або іншим записом і виконаний або прийнятий особою з наміром підписати цей запис" [5]. У цьому визначенні акцент зроблено на сам факт вираження згоди чи наміру особи (тобто на волевиявленні), а не на конкретний криптографічний метод. Таким чином, американське право допускає будь-яку електронну позначку, яка демонструє намір підписати, тоді як європейські та українські підходи більшою мірою наголошують на використанні саме криптографічних механізмів для гарантування безпеки підпису.

Інститут стандартів і технологій США (NIST) у своїх настановах також трактує електронний підпис через призму криптографічної безпеки. NIST визначає електронний підпис як використання криптографічного механізму з метою підтвердження автентичності та цілісності повідомлення або документа [1]. Тобто, за NIST електронний підпис – це, по суті, результат криптографічної операції (наприклад, шифрування геш-функції документа приватним ключем підписувача), що дозволяє перевірити, чи не змінювався документ після підписання та чи дійсно він підписаний заявленою особою. Цей технічний погляд доповнює юридичні визначення: якщо законодавчі акти фокусуються на тому, що ЕП є даними, пов'язаними з іншими даними, або актом, здійсненим з наміром, то технічний стандарт наголошує на функціональному призначенні ЕП – забезпечити достовірність (автентичність підписанта) та незмінність (цілісність) підписаного електронного документа.

Підсумовуючи, у базових дефініціях електронного підпису можна виокремити два основних підходи: технічний (криптографічний) і юридичний. Перший підхід (як у визначенні NIST [1]) розглядає ЕП як інструмент забезпечення інформаційної безпеки, який гарантує, що дані не були змінені та походять від відомого джерела. Другий підхід (закріплений у законодавстві [2, 3, 5]) сприймає ЕП як юридично значущу дію, еквівалентну власноручному підпису, що фіксує намір особи. Попри відмінності, обидва ці підходи сходяться на тому, що головна суть електронного підпису – це встановлення і підтвердження особи в цифровому середовищі та надання її діям юридичної сили. Іншими словами, електронний підпис виконує

функцію елемента цифрової ідентичності, надаючи підписувачу довірений статус у цифрових транзакціях.

У міжнародній практиці електронні підписи поділяються на різні типи залежно від рівня довіри і застосовуваних засобів захисту. Європейський регламент eIDAS встановлює три рівні електронного підпису [2]:

- *Простий електронний підпис* (Simple Electronic Signature, SES) – будь-які електронні дані (наприклад, зображення підпису, позначка або навіть натискання кнопки «Я згоден»), що додаються до документа з метою його підписання. SES засвідчує намір особи, але не гарантує автентичність підписувача чи цілісність документа.

- *Удосконалений електронний підпис* (Advanced Electronic Signature, AdES) – підпис, що відповідає підвищеним вимогам безпеки. AdES однозначно пов'язаний з підписувачем, створений під його повним контролем (наприклад, за допомогою особистого ключа, який нікому більше не доступний) і здатен виявити будь-які зміни даних після підписання. Таким чином, AdES забезпечує значно вищий рівень довіри, ніж SES.

- *Кваліфікований електронний підпис* (Qualified Electronic Signature, QES) – найвищий рівень електронного підпису. QES фактично є різновидом удосконаленого підпису, додатково посиленим вимогами щодо засобів та суб'єктів його створення. Він створюється за допомогою *кваліфікованого засобу* (наприклад, захищеного апаратного токена або смарт-карти) та базується на кваліфікованому сертифікаті, виданому *кваліфікованим надавачем довірчих послуг*. Кваліфікований електронний підпис у країнах ЄС має той самий юридичний статус, що й власноручний підпис на папері [2]; тобто документ, підписаний QES, визнається офіційними органами так само, як і підписаний від руки.

В Україні законодавство імплементує подібну градацію, хоча формально не використовує термінів SES, AdES, QES. Згідно із Законом України "Про електронні довірчі послуги", електронний підпис визначено аналогічно до європейського SES [3]. Цей же закон вводить поняття кваліфікованого електронного підпису (КЕП), який фактично відповідає європейському QES. КЕП визначається як удосконалений електронний підпис, створений з використанням *кваліфікованого засобу електронного підпису* і на основі *кваліфікованого сертифіката відкритого ключа* [3]. Законодавство встановлює, що документ, підписаний КЕП, має ту саму юридичну силу, що й паперовий документ з власноручним підписом (ст.18 Закону №2155-VIII) [3]. Таким чином, на найвищому рівні довіри українська модель електронного підпису повністю узгоджується з європейською: КЕП виконує функції, тотожні QES, і виступає найнадійнішим засобом цифрової ідентифікації особи. Сертифікат КЕП містить персональні атрибути підписувача (ПІБ, ідентифікаційний код, приналежність до організації тощо), що дозволяє точно ідентифікувати його без додаткових перевірок.

Отже, теоретичний огляд демонструє, що цифрова ідентичність забезпечується через поєднання технологічних рішень і правових норм. Електронний підпис постає як один з ключових компонентів цієї системи: він забезпечує автентифікацію (встановлення особи), цілісність даних (гарантію незмінності документа) та невідмовність (неможливість заперечити своє авторство). Далі сформулюємо дослідницьке питання, яке випливає з цього огляду, і окреслимо методичний підхід до його вирішення.

Постановка проблеми

З огляду на викладені теоретичні засади, постає головне дослідницьке питання: *яким чином електронний підпис слугує ключовим елементом цифрової ідентичності в сучасному цифровому середовищі та які безпекові характеристики й нормативні механізми*

забезпечують його надійність і юридичну значимість у онлайн-взаємодіях? Іншими словами, дослідження сфокусовано на тому, як електронний підпис поєднує в собі технічні та правові властивості для гарантування достовірної автентифікації користувача і забезпечення довіри до електронних транзакцій. Це питання охоплює декілька аспектів: визначення електронного підпису у різних системах та стандартах; аналіз рівнів довіри (кваліфікованого підпису) та інфраструктури довірчих послуг; виявлення механізмів, що забезпечують безпеку ЕП (захист ключів, процедури відкликання сертифікатів); а також роль електронного підпису у ширшому контексті цифрової безпеки та протидії таким викликам, як дезінформація. Відповідь на це дослідницьке питання дозволить оцінити, наскільки ефективно сучасні моделі електронного підпису виконують роль "цифрового паспорта" особи і чи відповідає українська практика найкращим міжнародним стандартам у цій сфері.

Методологія

Для досягнення поставленої мети було застосовано якісний дослідницький підхід із акцентом на аналіз нормативно-правових та стандартних документів, а також вивчення міжнародного досвіду. Зокрема, проведено нормативно-правовий аналіз ключових джерел, що визначають поняття цифрової ідентичності та електронного підпису: рекомендацій NIST SP 800-63-3 (США) [1], Регламенту (ЄС) № 910/2014 (eIDAS) [2], Закону України "Про електронну ідентифікацію та електронні довірчі послуги" [3] та суміжних підзаконних актів. Одночасно здійснено аналіз технічних стандартів і специфікацій, зокрема європейського стандарту ETSI EN 319 411-1, що встановлює вимоги до політик і безпеки для надавачів довірчих послуг [6], та ініціатив Cloud Signature Consortium [8], які регламентують сучасні підходи до реалізації хмарних підписів.

Дослідження включало порівняльний аналіз визначень та підходів у різних юрисдикціях: було зіставлено американський підхід (як у ESIGN Act [5] та рекомендаціях OECD [7]) з європейським (eIDAS [2], стандарти ETSI [6]) і українським [3, 4]. Для ширшого контексту розглянуто також аналітичні та оглядові матеріали, зокрема звіт Організації економічного співробітництва та розвитку щодо управління цифровою ідентичністю в інтернет-економіці [7], а також сучасні ініціативи, спрямовані на забезпечення автентичності цифрового контенту (наприклад, Content Authenticity Initiative) [9].

Отримані дані (визначення, принципи, вимоги) були систематизовані за тематичними блоками: концепція цифрової ідентичності; правові дефініції електронного підпису; класифікація рівнів довіри та роль кваліфікованого підпису; механізми забезпечення безпеки (ключова інфраструктура, надавачі довірчих послуг, процедури відкликання); виклики та перспективи. Це дозволило провести аналітичну інтерпретацію – виявити спільні риси та відмінності між різними підходами, оцінити відповідність української моделі європейським вимогам, а також окреслити проблеми і потенціал подальшого розвитку системи електронного підпису. Методологія дослідження, таким чином, поєднала огляд нормативної бази з порівняльним аналізом і синтезом практик, що забезпечує надійну основу для формування висновків.

Результати

Проведений аналіз підтвердив, що електронні підписи відіграють роль безпечних цифрових ідентифікаторів, які пов'язують особу з її діями в електронному просторі. В усіх розглянутих нормативних системах електронний підпис слугує засобом підтвердження, що саме певна уповноважена особа здійснила ту чи іншу дію (підписала документ, подала запит, дала згоду тощо) онлайн. Таким чином, ЕП забезпечує довіру до електронних транзакцій, виконуючи функцію "цифрового паспорта" користувача. Зокрема, завдяки використанню криптографічних методів електронний підпис гарантує автентичність (можливість перевірити особу підписанта) та цілісність електронних документів (контроль незмінності даних після

підписання) [1]. Крім того, на найвищому рівні він забезпечує невідмовність: підписант не може заперечити факт підписання документа, оскільки кваліфікований підпис юридично прирівняний до власноручного [2, 3]. Ці властивості роблять електронний підпис одним із ключових інструментів кібербезпеки в цифровій ідентифікації.

Аналіз нормативних документів ЄС та України показав, що найвищий рівень довіри надається саме *кваліфікованому електронному підпису*. У європейському правовому полі QES (Qualified Electronic Signature) може створюватися лише з використанням сертифікованих засобів і після перевірки особи довіреним постачальником, що забезпечує його максимальну надійність [2]. Такий підпис юридично визнається еквівалентним власноручному підпису у всіх державах-членах ЄС. В Україні запроваджено аналогічну концепцію у вигляді КЕП, який відповідає усім критеріям QES і також має повну юридичну силу власноручного підпису [3]. Документ, підписаний КЕП, обов'язково визнається дійсним та не може бути відхилений лише через його електронну форму. Таким чином, однією з головних знахідок дослідження є підтвердження того, що українська модель електронного підпису синхронізована з європейською в частині рівнів довіри: кваліфікований підпис забезпечує найвищий рівень впевненості в особі підписувача та цілісності документів.

Кваліфікований електронний підпис тісно пов'язаний з поняттям *кваліфікованого надавача електронних довірчих послуг* (КНЕДП) – організації, яка має право видавати кваліфіковані сертифікати та обслуговувати підписи. Результати аналізу показують, що роль таких постачальників є критичною для функціонування інфраструктури довіри. По-перше, КНЕДП здійснює ідентифікацію підписувача перед видачею сертифіката: закон вимагає, щоб особа пройшла перевірку документів або електронну ідентифікацію (через BankID, Mobile ID тощо) [3]. По-друге, надавач відповідає за надійне зберігання сертифікатів і пов'язаних даних, ведення реєстрів чинних і відкликаних сертифікатів, а також за оперативне відкликання та внесення змін до статусу сертифікатів у разі потреби [3, 6]. Відповідно до стандартів ETSI та вимог законодавства, кваліфіковані постачальники зобов'язані дотримуватися суворих політик безпеки – захищати свою інфраструктуру, застосовувати надійні криптографічні алгоритми, забезпечувати фізичну охорону апаратних засобів та проходити регулярні аудити на відповідність вимогам [6]. Таким чином, надійність електронного підпису великою мірою залежить від надійності роботи КНЕДП: тільки за умови сумлінної діяльності постачальника можна гарантувати, що видані ним підписи будуть довіреними. Наші результати підкреслюють: вибір кваліфікованого постачальника – стратегічно важливе рішення для користувача, адже саме якість послуг (в тому числі здатність швидко реагувати на інциденти, забезпечувати безперебійний доступ до сервісів OCSP/CRL тощо) визначає стабільність цифрової ідентичності підписувача.

Важливим аспектом забезпечення довіри до електронного підпису є захист особистого криптографічного ключа підписувача. Встановлено, що найбільш поширеним методом зберігання особистих ключів у рамках КЕП є використання фізичних захищених носіїв – апаратних токенів чи смарт-карт, які ізолюють ключ від несанкціонованого доступу. Для організацій з підвищеними вимогами безпеки застосовуються апаратні криптомодулі HSM (Hardware Security Module), які забезпечують генерацію та зберігання ключів у захищеному середовищі. Наразі також набирає популярності модель *хмарного підпису*, за якої особистий ключ зберігається не у користувача, а у захищеному хмарному сховищі, що належить довірчому постачальнику, і доступ до нього здійснюється через багатофакторну автентифікацію користувача. Наш аналіз показав, що такі інноваційні моделі узгоджуються з сучасними рекомендаціями Cloud Signature Consortium та відповідають стандартам безпеки, визначеним європейськими нормами (ETSI) [6, 8]. Тобто, відбувається перехід до архітектур, де безпека ключа гарантується не лише самим користувачем, а й професійним провайдером, що додає рівень захисту (наприклад, унеможливлює втрату ключа через компрометацію

пристрою користувача). В результаті дослідження підтверджено: захист приватного ключа – фундамент безпеки електронного підпису, і поєднання технічних рішень (токени, HSM, хмарні сховища) з організаційними (регламентовані процедури видачі/зберігання, аудити постачальників) суттєво підвищує рівень довіри до системи електронної ідентичності.

Окремим важливим результатом є висновки щодо процедури відкликання сертифікатів електронного підпису та її значення для підтримання довіри. Життєвий цикл кваліфікованого сертифіката включає етапи генерації ключів, їх використання, закінчення строку дії і, за необхідності, відкликання (скасування) сертифіката. На кожному з цих етапів були ідентифіковані потенційні загрози: зокрема, компрометація особистого ключа під час генерації або зберігання, втрата чи крадіжка носія з ключем, уразливості програмного забезпечення для накладання підпису тощо. Якщо особистий ключ потрапляє до рук зловмисників, останні можуть підписувати документи від імені користувача, фактично підміняючи його цифрову особу. Тому законодавством чітко регламентовано обов'язки сторін: підписувач у разі підозри на компрометацію ключа повинен *негайно* повідомити про це свого КНЕДП і подати заявку на відкликання сертифіката [3]. Кваліфікований постачальник, зі свого боку, зобов'язаний забезпечити цілодобову доступність сервісів перевірки статусу сертифікатів (OCSP – Online Certificate Status Protocol, або списки відкликаних сертифікатів, CRL) і якнайшвидше обробляти запити на відкликання [3]. Від часу, що мине між скомпрометуванням ключа та фактичним відкликанням сертифіката, залежить масштаб потенційних зловживань: доки сертифікат формально діє, усі підписи, зроблені зловмисником, матимуть юридичну силу. Тому оперативність відкликання є критичною. Наші результати підкреслюють, що добре налагоджена система відкликання – запорука безперервності довіри: навіть якщо інцидент стався, швидке відкликання мінімізує ризики. Таким чином, безпека цифрової ідентичності забезпечується не лише на етапі створення підпису, а й протягом усього його життєвого циклу, включно з можливістю своєчасно анулювати довірені повноваження при виникненні загроз.

Синтезуючи результати, можна зробити висновок, що електронний підпис виступає одним з базових будівельних блоків системи цифрової ідентичності. Він надає користувачу *юридично значущу присутність* у цифровому світі, дозволяючи здійснювати дії онлайн з тим самим рівнем довіри, що й офлайн. Виявлено, що у сферах електронного урядування, бізнесу, фінансів, охорони здоров'я тощо, впровадження електронних підписів дозволило перенести багато критично важливих процесів у цифровий формат без втрати легітимності. Фактично, електронний підпис став основою для розвитку таких сервісів, як подання податкових декларацій та заяв в електронному уряді, укладення договорів онлайн, отримання електронних рецептів і довідок, голосування чи участь у електронних аукціонах тощо. Усі ці застосування можливі лише тому, що є засіб достовірно підтвердити особу та її волю – тобто, працює інститут цифрового підпису. Додатково, результати дослідження продемонстрували, що можливості електронного підпису виходять за межі суто юридичних транзакцій: завдяки властивостям підтвердження автентичності та цілісності, кваліфіковані підписи можуть бути використані для боротьби з дезінформацією та забезпечення достовірності цифрового контенту (про що детальніше йдеться в обговоренні) [9]. Таким чином, електронний підпис нині – це не просто технологія для підписання документів, а багатофункціональний інструмент встановлення довіри у цифровому суспільстві.

Обговорення

Отримані результати підтверджують двоєдину природу електронного підпису: він одночасно є технічним засобом криптографічного захисту і юридичним інструментом, визнаним законом. Така комбінація робить його надзвичайно ефективним елементом цифрової ідентичності. Кваліфікований електронний підпис (КЕП) виконує роль "цифрового печатки" особи,

забезпечуючи високий рівень довіри до будь-яких електронних дій цієї особи. В обговоренні варто підкреслити кілька ключових моментів. По-перше, українська модель електронного підпису загалом відповідає європейським стандартам. Законодавче визначення ЕП та КЕП [3] майже ідентичне європейському [2], запроваджено інфраструктуру кваліфікованих постачальників, сертифікатів і довірчих списків, що дуже схоже на систему eIDAS. Це означає, що Україна фактично інтегрувалася у загальноєвропейський простір довірчих послуг, принаймні на рівні вимог і технічної реалізації. Практична вигода цього – взаємне визнання підписів і довірчих сертифікатів, що є потенційним підґрунтям для транскордонних цифрових транзакцій.

По-друге, дослідження виявило цікавий контраст із підходом США: у той час, як в ЄС та Україні основний акцент зроблено на технологічній довіреності (криптографія, сертифікати, регульовані провайдери), у США законодавство (ESIGN Act) надає юридичну чинність будь-якому електронному підпису, якщо є доведений намір особи [5]. Цей підхід більш гнучкий технологічно, але менше акцентує увагу на стандартизованих рівнях безпеки. У дискусіях фахівців часто зазначається, що європейська модель забезпечує вищий формальний рівень довіри (через акредитацію постачальників, обов'язкові апаратні засоби тощо), тоді як американська – вищу зручність і доступність. Українська система, перебуваючи під впливом європейського регулювання, прийняла модель високих гарантій (КЕП), що є виправданим кроком для розвитку e-government і захисту критичних даних, хоча можливо дещо підвищує бар'єр входу для масового використання (потреба отримувати сертифікати, токени тощо). Ця відмінність свідчить про альтернативні підходи до забезпечення довіри: або через ринкову гнучкість і постфактум юридичну відповідальність (США), або через попереднє регулювання і стандартизацію (ЄС).

В ході дослідження були окреслені основні загрози, що виникають на різних етапах використання електронного підпису. В обговоренні важливо оцінити, наскільки наявні механізми протидіють цим загрозам. Як показано в результатах, найвразливішим місцем є особистий ключ підписувача: його компрометація фактично означає крах цифрової ідентичності, адже зловмисник може видавати себе за іншу особу. Сучасні засоби захисту (апаратні носії, HSM, хмарні підписи з MFA) значно знижують ризики несанкціонованого доступу [6, 8]. Однак жодна технологія не виключає повністю людського фактора: користувач може ненавмисно розкрити пароль до ключа або запізнитися з повідомленням про компрометацію. Тому критичною є оперативна взаємодія між користувачем і постачальником: готовність останнього швидко відкликати сертифікат і поінформувати зацікавлені сторони. Українське законодавство [3] досить чітко це регулює, проте на практиці швидкість реакції може варіювати. В обговоренні варто підкреслити потребу у підвищенні обізнаності користувачів щодо правил безпеки (зберігання ключів, негайне звернення при загрозах) та вдосконаленні інфраструктури постачальників (наприклад, автоматизовані системи моніторингу аномальної активності, щоб своєчасно виявляти можливу компрометацію).

Як вже зазначалося, на нормативному рівні відповідність майже повна: Україна запровадила класифікацію підписів та роль КНЕДП, аналогічні eIDAS. У практичній площині інтеграція триває. Зокрема, Україна підтримує власний *довірчий список* (реєстр кваліфікованих постачальників) і працює над взаємним визнанням сертифікатів з ЄС. Одним із показників відповідності є те, що українські КЕП активно використовуються у взаємодії з європейськими партнерами (наприклад, при поданні заяв на отримання послуг в європейських установах). Проте, критично аналізуючи, слід зазначити і виклики: швидка еволюція стандартів (наприклад, поява нового регламенту eIDAS 2.0, концепція Європейської цифрової ідентичності та електронних гаманців) вимагатиме від України оперативного оновлення законодавства, щоб зберегти сумісність. Загалом можна констатувати, що українська модель електронного підпису наразі відповідає актуальним європейським вимогам, але потребує

подальшого розвитку у напрямку міжнародної інтероперабельності та підтримки нових технологічних рішень.

Одним з інноваційних аспектів, висвітлених у дослідженні, є використання електронного підпису для верифікації цифрового контенту з метою боротьби з дезінформацією. У цифровому просторі сьогодення дезінформація (свідоме поширення неправдивої або маніпулятивної інформації) становить серйозну загрозу як для суспільства, так і для національної безпеки [7]. Фальсифіковані електронні документи, підроблені новини, глибокі фейки (deepfakes) – усе це підриває довіру до інформації. В цьому контексті електронні підписи, особливо кваліфіковані, можуть стати частиною рішення. Наше дослідження показало, що КЕП має низку властивостей, корисних у протидії дезінформації:

- Автентичність джерела: Документ чи повідомлення, підписане кваліфікованим підписом, дає змогу точно встановити особу або організацію, від імені якої його було створено. А оскільки кваліфікований сертифікат видається лише після перевірки особи, можливість анонімно поширювати фейковий “офіційний” документ практично виключається [3].

- Цілісність контенту: Якщо після накладання електронного підпису у документі буде хоч найменша зміна, підпис стане недійсним. Це дозволяє відразу виявити факти підроблення чи несанкціонованого редагування офіційного цифрового контенту [1, 6].

- Невідмовність і підзвітність: Кваліфікований підпис фіксує відповідальну особу – підписант не може заперечити свою причетність. Це важливо, коли йдеться про публікацію неправдивих даних: якщо документ підписано конкретним посадовцем або установою, вони не зможуть потім заявити, що не причетні, що підвищує підзвітність та дисциплінує поширювачів інформації [5].

Окрім того, електронний підпис сприяє відстеженню походження інформації. Використовуючи підпис, можна визначити першоджерело – хто саме (яка установа, орган чи особа) вперше оприлюднив певний документ чи заяву. Це особливо корисно при роботі з прес-релізами, офіційними повідомленнями, аналітичними звітами, де важливо переконатися, що вони справді виходять від автентичного джерела [4, 8]. На міжнародному рівні ця концепція набуває розвитку через такі ініціативи, як Content Authenticity Initiative (CAI). В рамках CAI розробляються стандарти (зокрема, зусиллями коаліції C2PA – Coalition for Content Provenance and Authenticity) для впровадження у цифрові платформи технічних засобів фіксації походження та історії змін цифрових медіа [9]. Планується, що до фотографій, відео та інших файлів буде прикріплюватися своєрідний «сертифікат походження», який підтверджує, де і ким цей контент створено і чи змінювався він. Електронні підписи можуть органічно увійти до цього механізму глобальної верифікації: наприклад, офіційні фотографії чи документи, підписані КЕП, матимуть позначку достовірності в інформаційних системах. Таким чином, у перспективі електронний підпис може стати частиною ширшої екосистеми забезпечення довіри до цифрового контенту у всьому світі [9].

Для України практичним кроком у цьому напрямі могло б стати запровадження вимоги обов’язкового використання КЕП для певних видів публічної інформації: офіційних документів органів влади, публікацій на державних веб-сайтах, новин від урядових прес-служб тощо. Також варто заохочувати засоби масової інформації інтегрувати електронні підписи у свої редакційні процеси – це підвищить прозорість і довіру до оприлюднюваних матеріалів, унеможливить непомічене внесення змін після публікації. Звичайно, електронний підпис не є панацеєю від дезінформації, але у поєднанні з іншими заходами (правовими, освітніми, технологічними) він суттєво зміцнює позиції суспільства у боротьбі за цифрову достовірність.

Таблиця 1 – Порівняння підходів до електронного підпису в ЄС, США та Україні

Критерій	ЄС (eIDAS)	США (ESIGN Act)	Україна (Закон №2155-VIII)
Типи підписів	SES, AdES, QES	Без класифікації, загальне визначення “електронний підпис”	ЕП, удосконалений ЕП, кваліфікований ЕП (КЕП)
Юридична сила	QES = власноручному підпису	Будь-який ЕП = власноручному (якщо є намір)	КЕП = власноручному підпису
Рівень довіри	QES – найвищий, має міждержавне визнання	Юридична сила базується на намірі, а не на рівні безпеки	КЕП забезпечує найвищий рівень, юридично обов’язковий
Вимоги до постачальників	Кваліфіковані надавачі довірчих послуг (QTSP)	Відсутні суворі вимоги до постачальників	Кваліфіковані надавачі довірчих послуг (КНЕДП)
Захист ключів	Обов’язкові засоби: токени, смарт-карти, HSM	Визначається провайдером, відсутня регуляція	Захищені носії, можливість використання хмарних КЕП
Визнання між юрисдикціями	Автоматичне між країнами ЄС	Обмежене (немає автоматичного міжнародного визнання)	Орієнтоване на відповідність eIDAS, часткове визнання в ЄС
Підхід до автентифікації	Технічна ідентифікація, сертифікати, регістри	Будь-яке волевиявлення, зокрема клік або звук	Ідентифікація за ID/паспортом, BankID, Mobile ID, реєстри сертифікатів
Наголос	Безпека, міждержавна сумісність	Гнучкість, доступність	Безпека, державне регулювання, наближення до eIDAS

Розвиток технологій і нормативного поля відкриває нові можливості для вдосконалення системи електронного підпису як складової цифрової ідентичності. Одним з перспективних напрямів є інтеграція біометричних даних у процес підписання. Наприклад, додаткове підтвердження операції підпису за відбитком пальця або розпізнаванням обличчя забезпечило б ще вищий рівень впевненості, що саме законний власник ключа здійснює підпис (особливо актуально для хмарних підписів, де доступ віддалений). Інший напрям – використання штучного інтелекту (ШІ) для верифікації підписів. Уже зараз ШІ застосовується для аналізу рукописних підписів; у цифровій сфері він міг би, наприклад, моніторити аномалії у використанні електронного підпису (нетиповий час, місце, обсяг підписаних документів) і сигналізувати про потенційні зловживання.

Ще одна перспектива – міжюрисдикційна інтероперабельність. Хоча ЄС досяг значного прогресу у взаємному визнанні електронних підписів (усі країни-члени визнають QES одна одної), на глобальному рівні є багато розрізнених стандартів. Узгодження підходів між різними країнами (наприклад, між ЄС і США, де підходи зараз істотно різняться) могло б спростити міжнародні цифрові транзакції. Деякі кроки в цьому напрямі вже робляться – міжнародні організації працюють над стандартами й рекомендаціями, спільними проектами

(як-от згадана ініціатива C2PA з акторами з різних країн). Для України потенціал інтеграції полягає у приєднанні до глобальних ініціатив та активній участі у формуванні нових стандартів: маючи сучасну нормативну базу, Україна може позиціювати себе як надійного партнера у світовому цифровому просторі.

Звичайно, з новими можливостями з'являються й нові виклики. Зокрема, поява квантових обчислень у майбутньому може поставити під загрозу сучасні криптографічні алгоритми, тож спільноті доведеться переходити на пост-квантові алгоритми електронного підпису. Також слід враховувати аспект захисту приватності: розширення цифрової ідентичності (включно з біометрією) не повинно призводити до надмірного контролю або витоку персональних даних. Таким чином, інтеграція – це балансування між зручністю, безпекою і правами користувачів.

Підсумовуючи обговорення, варто зазначити: результати дослідження підтвердили фундаментальну роль електронного підпису в сучасній цифровій екосистемі, а також окреслили шляхи, як цей інструмент може еволюціонувати. Українська практика рухається в руслі світових тенденцій, і надалі важливо підтримувати цей курс, приділяючи увагу як поточним загрозам, так і майбутнім технологічним можливостям.

Висновки

Електронний підпис відіграє ключову роль у цифровому середовищі як засіб автентифікації особи та надання юридичної сили електронним діям. Проведене дослідження дозволило глибше зрозуміти природу електронного підпису як елемента цифрової ідентичності та зробити низку ключових висновків:

- Поєднання технічного та правового аспектів: Електронний підпис є одночасно технічним механізмом захисту даних і юридично визнаним інструментом волевиявлення. Завдяки цьому він забезпечує унікальну можливість – гарантовано встановити особу та її намір в електронній взаємодії, що робить його фундаментом довіри в цифровому суспільстві.

- Найвищий рівень довіри – кваліфікований підпис: В ЄС та Україні створено багаторівневу модель електронних підписів, де найвищим рівнем є кваліфікований електронний підпис (QES/КЕП) [2][3]. КЕП прирівняний за силою до власноручного підпису і забезпечує автентичність, цілісність та невідмовність на рівні, необхідному для критично важливих електронних транзакцій. Українська нормативна база узгоджена з європейською, що підтверджує готовність країни до інтеграції у міжнародний цифровий простір довіри.

- Інфраструктура довірчих послуг є вирішальною: Ефективність та надійність електронного підпису залежать від інфраструктури, яка його підтримує – передусім, від роботи кваліфікованих надавачів довірчих послуг (КНЕДП). Встановлені вимоги до постачальників та процедур (перевірка особи, захист ключів, відкликання сертифікатів, аудити) [3][6] є критично важливими для збереження цілісності цифрової ідентичності. Надійна робота КНЕДП, своєчасне реагування на інциденти та дотримання стандартів безпеки визначають успішність функціонування всієї системи.

- Забезпечення безпеки протягом життєвого циклу: Захист електронного підпису повинен бути комплексним – від генерації ключів до можливого відкликання сертифіката. Дослідження показало, що лише при умові належного зберігання особистих ключів (апаратні засоби, HSM, хмарні рішення з MFA) [6, 8], постійного моніторингу загроз та наявності чітких процедур відкликання [3] можна гарантувати

довгострокову довіру до цифрової ідентичності користувача. Будь-який збій у цьому ланцюжку (компрометація ключа, затримка з відкликанням) становить ризик, тому вкладення ресурсів у безпеку виправдане і необхідне.

- Практична цінність і розширення застосувань: Електронний підпис уже довів свою практичну користь – він дає змогу громадянам і бізнесу взаємодіяти з державою та між собою онлайн, економлячи час і ресурси. Він є невід'ємною складовою електронного урядування, електронної комерції, фінансових послуг, охорони здоров'я і багатьох інших сфер. Крім того, його значення виходить за межі суто юридичних операцій: завдяки властивостям підтвердження авторства та цілісності контенту електронний підпис стає потужним інструментом у боротьбі з дезінформацією та забезпеченні достовірності даних [9]. Таким чином, впровадження електронних підписів підвищує загальний рівень довіри до цифрових процесів і інформації.

- Науковий внесок та перспективи подальших досліджень: Дане дослідження узагальнило і систематизувало знання про електронний підпис у контексті цифрової ідентичності, об'єднавши технічні стандарти і правові норми в єдину аналітичну перспективу. Новизна роботи полягає у висвітленні *подвійної ролі* кваліфікованого підпису – як юридичного аналога власноручного підпису і водночас інструмента кібербезпеки, що забезпечує достовірність цифрового контенту. Практична цінність отриманих результатів полягає у рекомендаціях щодо зміцнення системи електронної ідентифікації (посилення захисту ключів, вдосконалення процедур відкликання, інтеграції підписів у медіасередовище).

Перспективи подальших досліджень включають глибше вивчення біометричної аутентифікації в поєднанні з електронним підписом, застосування штучного інтелекту для моніторингу та верифікації підписів, а також питання взаємодії різних систем цифрової ідентичності у глобальному масштабі (розробка стандартів інтероперабельності між юрисдикціями, включно з імплементацією нових ініціатив на кшталт цифрових гаманців і децентралізованих ідентифікацій). Крім того, важливим напрямом є дослідження стійкості електронних підписів до майбутніх викликів, таких як квантові обчислення, та перехід на криптографічні алгоритми нового покоління.

На завершення, можна впевнено ствердити, що електронний підпис сьогодні – це не лише технологія для автентифікації, але й основа довіри цифрового суспільства. Від його надійності та повсюдного впровадження залежить успіх цифрової трансформації, тому постійна увага до розвитку і вдосконалення механізмів електронного підпису є запорукою побудови безпечного і відкритого інформаційного середовища.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. NIST. Digital Identity Guidelines: NIST Special Publication 800-63-3 [Електронний ресурс]. – URL : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
2. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

(eIDAS) [Електронний ресурс]. – URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910
3. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII [Електронний ресурс]. – URL : https://zakon.rada.gov.ua/laws/show/2155-19#Text
4. Цифрова ідентичність / Освітній модуль на порталі «Дія.Освіта» [Електронний ресурс]. – URL : https://it-osvita.diia.gov.ua/educational-unit/1.1_cifrova_identichnist
5. U.S. Electronic Signatures in Global and National Commerce Act (ESIGN Act), 2000 [Електронний ресурс] // Federal Deposit Insurance Corporation (FDIC). – URL : https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf
6. ETSI EN 319 411-1 V1.2.2 (2016-02). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [Електронний ресурс]. – URL : https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.02.02_60/en_31941101v010202p.pdf
7. OECD. The Role of Digital Identity Management in the Internet Economy [Електронний ресурс]. – Paris: OECD, 2009. – URL : https://www.oecd.org/sti/ieconomy/42753181.pdf
8. Cloud Signature Consortium. Technical Committee [Електронний ресурс]. – URL : https://cloudsignatureconsortium.org/about-us/technical-comittee/
9. Content Authenticity Initiative [Електронний ресурс]. – URL : https://contentauthenticity.org
10. Вчасно. Що таке електронний підпис? [Електронний ресурс]. – URL : https://vchasno.ua/en/shcho-take-elektronnyi-pidpys/
11. MDPI. Various Factors Affecting the Implementation of Digital Signature Technology in Organizations [Електронний ресурс] // *Sustainability*. – 2023. – Vol. 15(6), Article 5008. – URL : https://www.mdpi.com/2071-1050/15/6/5008
12. Про електронний цифровий підпис: Закон України від 22.05.2003 № 851-IV [Електронний ресурс]. – URL : https://zakon.rada.gov.ua/laws/show/851-15#Text
13. Cybersecurity and Infrastructure Security Agency (CISA). Understanding Digital Signatures [Електронний ресурс]. – URL : https://www.cisa.gov/news-events/news/understanding-digital-signatures
14. XtraTrust. Various Types of Digital Signatures and Its Uses [Електронний ресурс]. – URL : https://xtratrust.com/index.php/blog/digital-signature/various-types-of-digital-signatures-and-its-uses
15. SSH Communications Security. How Digital Signatures Work [Електронний ресурс]. – URL : https://www.ssh.com/academy/secure-information-sharing/how-digital-signatures-work

References

1. National Institute of Standards and Technology. (2017). *Digital identity guidelines (NIST Special Publication 800-63-3)*. Available from : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
2. European Parliament and Council of the European Union. (2014). *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*. Available from : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910
3. On electronic identification and electronic trust services: Law of Ukraine dated 05.10.2017 No. 2155-VIII [Electronic resource]. Available from : https://zakon.rada.gov.ua/laws/show/2155-19#Text

4. Digital identity / Educational module on the portal “Diya.Osvita” [Electronic resource]. Available from : https://it-osvita.diia.gov.ua/educational-unit/1.1_cifrova_identichnist
5. United States Congress. (2000). *Electronic Signatures in Global and National Commerce Act (ESIGN Act)*. Federal Deposit Insurance Corporation (FDIC). Available from : https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf
6. European Telecommunications Standards Institute. (2016). *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (ETSI EN 319 411-1 V1.2.2)*. Available from : https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.02.02_60/en_31941101v010202p.pdf
7. Organisation for Economic Co-operation and Development. (2009). *The role of digital identity management in the internet economy*. Available from : https://www.oecd.org/sti/ieconomy/42753181.pdf
8. Cloud Signature Consortium. (n.d.). *Technical Committee*. Available from : https://cloudsignatureconsortium.org/about-us/technical-comittee/
9. Content Authenticity Initiative. (n.d.). *Content Authenticity Initiative*. https://contentauthenticity.org
10. On time. (n.d.). What is an electronic signature? Available from : https://vchasno.ua/en/shcho-take-elektronnyi-pidpys/
11. Nguyen, T. H., Do, T. T., & Nguyen, N. T. (2023). Various factors affecting the implementation of digital signature technology in organizations. *Sustainability, 15*(6), Article 5008. Available from : https://www.mdpi.com/2071-1050/15/6/5008
12. On electronic digital signature: Law of Ukraine dated 22.05.2003 No. 851-IV [Electronic resource]. Available from : https://zakon.rada.gov.ua/laws/show/851-15#Text
13. Cybersecurity and Infrastructure Security Agency. (n.d.). *Understanding digital signatures*. Available from : https://www.cisa.gov/news-events/news/understanding-digital-signatures
14. XtraTrust. (n.d.). *Various types of digital signatures and its uses*. Available from : https://xtratrust.com/index.php/blog/digital-signature/various-types-of-digital-signatures-and-its-uses
15. SSH Communications Security. (n.d.). *How digital signatures work*. Available from : https://www.ssh.com/academy/secure-information-sharing/how-digital-signatures-work