ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ В ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня магістра

зі спеціальності _____125_____

Кібербезпека_____

(код, найменування спеціальності)

освітньо-професійної програми_Інформаційна та кібернетична безпека____

(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____БОНДАРЄВ Ілля

Виконав: здобувач вищої освіти групи БСДМ-61

БОНДАРЄВ Ілля

(ПРІЗВИЩЕ, ім'я)

Керівник
д.т.н, проф. КОЖУХІВСЬКИЙ Андрій

(ПРІЗВИЩЕ, ім'я)

Рецензент
к.т.н, доцент _____

(ПРІЗВИЩЕ, ім'я)

КИЇВ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____Гайдур Г.І
«___»_____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бондарєву Іллі Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: «Технологія використання електронних цифрових підписів в організації»

керівник кваліфікаційної роботи Кожухівський А.Д., д.т.н, проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи

1) Алгоритми та стандарти електронних цифрових підписів;
2) Платформи та рішення для створення цифрових підписів;
3) Наукова та технічна література. Стандарти. Рекомендації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Аналіз правових аспектів функціонування цифрових підписів в Україні та світі;
2) Дослідження алгоритмів та стандартів створення електронних цифрових підписів;
3) Дослідження механізмів та засобів безпечної інтеграції електронних цифрових підписів у документообігу організації.

5. Перелік ілюстративного матеріалу:

1) Мета, об'єкт та предмет дослідження;

2) Послідовність реалізації цифрового підпису;

3) Дослідження алгоритмів та стандартів створення електронних цифрових підписів;

4) Порівняння показників безпеки використання цифрових підписів;

5) Отримання кваліфікованого електронного підпису (КЕП);

6) Алгоритм генерації ключів в АЦСК «центр сертифікації ключів україни»;

7) Використання мобільного додатку eSign для генерації цифрового підпису;

8) Перевірка сертифікатів в реєстрі документів довільних форматів;

9) Висновки.

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз науково-технічної літератури	02.11.2023 р.	виконано
2.	Аналіз правових аспектів функціонування цифрових підписів в Україні та світі	14.11.2023 р.	виконано
3.	Дослідження особливостей реалізації традиційних схем електронного підпису	19.11.2023 р.	виконано
4.	Дослідження алгоритмів та стандартів створення електронних цифрових підписів	22.11.2023 р.	виконано
5.	Дослідження механізмів та засобів безпечної інтеграції електронних цифрових підписів у документообігу організації	26.11.2023 р.	виконано
7.	Реферат, вступ, висновки	07.12.2023 р.	виконано
8.	Підготовка презентації	11.12.2023 р.	виконано

Здобувач вищої освіти _____ Ілля БОНДАРЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Андрій КОЖУХІВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 80 сторінок, 43 рисунка, 2 таблиці, 39 джерел.

Об'єкт дослідження – процес безпечного застосування електронних цифрових підписів в організаційних операціях.

Предмет дослідження – механізми та засоби безпечної інтеграції електронних цифрових підписів у документообіг організації.

Мета роботи – підвищення рівня інформаційної безпеки в організації шляхом впровадженню електронних цифрових підписів в документообіг.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки.

В роботі проаналізовано поняття цифрового підпису та досліджено вітчизняне та міжнародне законодавство, що регламентує особливості функціонування електронних цифрових підписів. Зазначено вимоги щодо цифрових підписів, особливості та їх класифікації та досліджено алгоритми та стандарти створення електронних цифрових підписів.

Виокремлено особливості реалізації традиційних схем електронного підпису та проведено аналіз алгоритмів хешування. Досліджено механізми та засоби безпечної інтеграції електронних цифрових підписів у документообігу організації.

Досліджено платформи для створення цифрового підпису.

Розроблено алгоритм генерації ключів в АЦСК «Центр сертифікації ключів України» та алгоритм використання мобільного додатку eSign для генерації цифрового підпису.

Галузь використання – кібербезпека.

ЦИФРОВИЙ ПІДПИС, PUBLIC KEY, NIST, ISO, PDF, RSA, X.509, СЕРТИФІКАТ, ДІЯ, BANKID, MICROSOFT, БЕЗПЕКА, ОРГАНІЗАЦІЯ, ДОКУМЕНТООБІГ, АУТЕНТИФІКАЦІЯ.

ABSTRACT

Qualification's thesis: 80 pages, 43 figures, 2 tables, 39 sources.

The object of research – the process of secure application of electronic digital signatures in organizational operations.

The subject of research – is the mechanisms and means of secure integration of electronic digital signatures into the document flow of an organization.

The aim of research is to increase the level of information security in the organization by implementing electronic digital signatures in document circulation.

Research methods – information theory, international and national standards in the field of cybersecurity, security policies.

The work analyzes the concept of a digital signature and investigates domestic and international legislation that regulates the specifics of the functioning of electronic digital signatures. The requirements for digital signatures, their features and classifications are indicated, and algorithms and standards for creating electronic digital signatures are investigated.

The peculiarities of implementing traditional electronic signature schemes are distinguished, and hashing algorithms are analyzed. Mechanisms and means of secure integration of electronic digital signatures into the document circulation of an organization are investigated.

Platforms for creating a digital signature are studied.

An algorithm for key generation in the ACCS «Key Certification Center of Ukraine» and an algorithm for using the eSign mobile application to generate a digital signature have been developed.

Field of use – cybersecurity.

DIGITAL SIGNATURE, PUBLIC KEY, NIST, ISO, PDF, RSA, X.509, CERTIFICATE, ACTION, BANKID, MICROSOFT, SECURITY, ORGANIZATION, DOCUMENTATION, AUTHENTICATION.

ЗМІСТ

ВСТУП

Актуальність дослідження. Електронний підпис - це метод, який дозволяє особі авторизувати вміст електронного повідомлення або документа. Він може існувати у різних форматах, таких як введене ім'я, електронна адреса, скановане зображення підпису, чи автоматичний підпис електронної пошти. Ця політика регулює використання електронних підписів у компанії, забезпечуючи, що вони виконують ті ж функції, що й письмові підписи, та відповідають необхідним стандартам автентичності та безпеки.

Працівники повинні дотримуватися визначеної політики, не використовуючи електронні підписи, які не належать їм, без дозволу. Порушення цієї політики може призвести до різних негативних наслідків. Політики регулярно переглядаються, щоб вони відповідали актуальним законодавчим вимогам та потребам організації.

Цифровий підпис є різновидом електронного підпису, який забезпечує вищий рівень безпеки порівняно зі стандартними електронними підписами. Під час підписання документа цифровим підписом, підпис асоціюється з унікальним «відбитком» документа, що відноситься до підписувача. Ця інформація стає невід'ємною частиною документа, забезпечуючи засіб виявлення будь-яких спроб змін або підробки після підписання. Завдяки тому, що інформація про підпис вбудована безпосередньо в документ, не існує необхідності звертатися до постачальника послуг для перевірки його безпеки, на відміну від ситуацій з використанням стандартного електронного підпису.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технології використання електронних цифрових підписів в організації.

Об’єкт дослідження – процес безпечного застосування електронних цифрових підписів в організаційних операціях.

Предмет дослідження – механізми та засоби безпечної інтеграції електронних цифрових підписів у документообіг організації.

Мета роботи – підвищення рівня інформаційної безпеки в організації шляхом впровадженню електронних цифрових підписів в документообіг.

Наукові завдання:

- проаналізувати правові аспекти функціонування цифрових підписів в Україні та світі;
- дослідити алгоритми та стандарти створення електронних цифрових підписів;
- дослідити механізми та засоби безпечної інтеграції електронних цифрових підписів у документообігу організації;
- дослідити платформи для створення цифрових підписів в Україні.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки.

Практичне значення одержаних результатів полягає в розробці алгоритмів підвищення рівня інформаційної безпеки шляхом впровадження електронних цифрових підписів в документообігу організації.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРАВОВОГО РЕГУЛЮВАННЯ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ В УКРАЇНІ ТА СВІТІ

1.1 Призначення електронного цифрового підпису та його властивості

Цифровий підпис — це електронний підпис, який використовується для автентифікації повідомлень або документів і гарантує, що передані дані не були змінені чи модифіковані.

Цифровий підпис вважається більш корисним, ніж електронний підпис у сфері функціонування уряду, банку чи бізнесу, через вищий рівень безпеки. Електронним підписом може бути будь-який тип електронного методу затвердження, наприклад електронний символ або процес. Прикладом реалізації можна розглядати програму, інстальовану на комп'ютері, де для встановлення програмного забезпечення вимагаються умови угоди. Звичайний користувач повинен прийняти ці умови, натиснувши кнопку прийняти, це є фактичним підписом користувача про схвалення умов угоди. Зазначений приклад електронного підпису не забезпечує автентифікацію, цілісність або безпеку, тому юридична цінність не є значно високою порівняно з правовими аспектами цифрового підпису [1].

Залежно від тлумачення законодавства, цифровий підпис можна вважати еквівалентним фізичному підпису. Однак цифровий підпис є більш ефективним за часом і може забезпечувати більший захист. Цифровий підпис гарантує походження та цілісність повідомлення (рис.1.1).

Основні характеристики та переваги цифрових підписів включають:

- Автентифікація – процес підтвердження особи відправника, оскільки лише особа з приватним ключем може створити правильний підпис;

- Цілісність - гарантує, що документ або дані не були підроблені під час передачі;

- Невідмовність - відправник не може заперечувати, що підписав документ, оскільки підпис математично прив’язаний до його закритого ключа;

- Ефективність - цифрові підписи є ефективними та можуть використовуватися для електронного підпису документів швидко та без необхідності фізичної присутності.

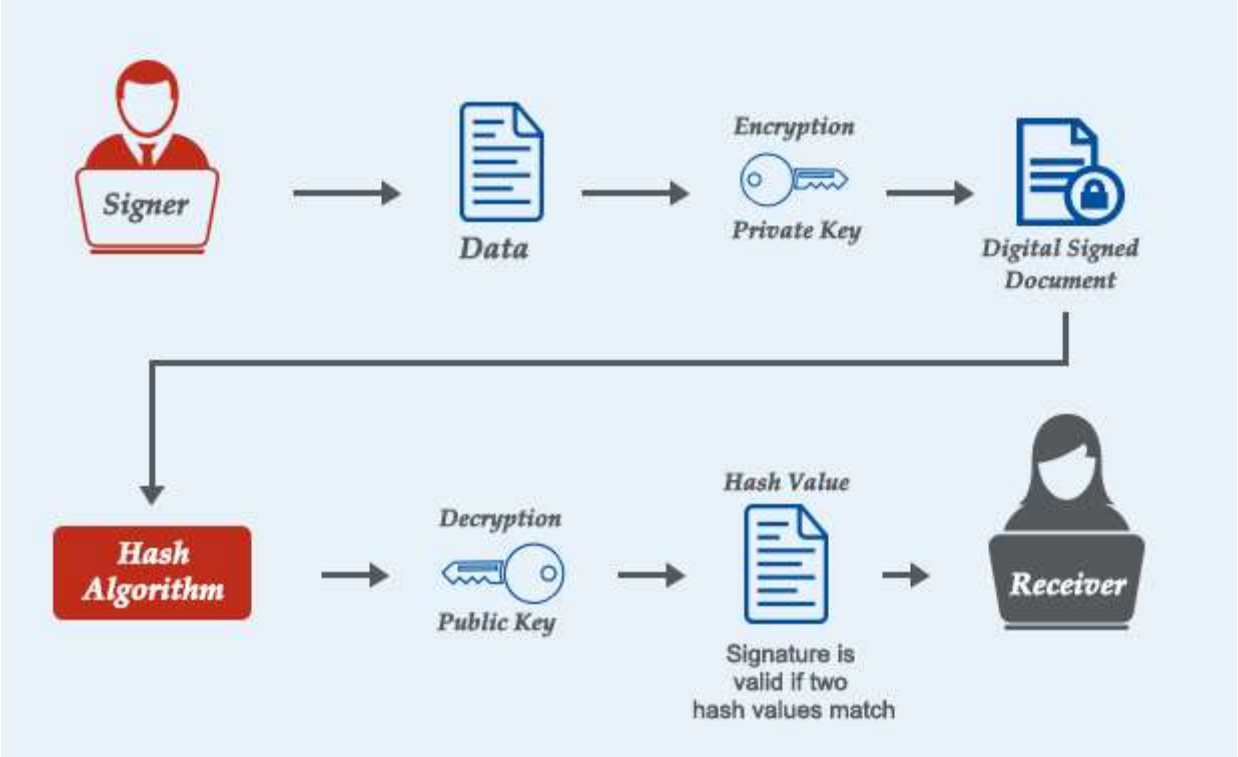

Рис.1.1. Послідовність реалізації цифрового підпису

Цифрові підписи використовуються в різних програмах і галузях для покращення рівня безпеки, перевірки автентичності та забезпечення цілісності цифрових документів і операції. Декілька поширених випадків використання цифрових підписів:

1. Безпека електронної пошти. Цифрові підписи використовуються в електронному зв’язку для перевірки автентичність електронних повідомлень. Коли електронний лист має цифровий підпис, одержувач може бути впевненим, що його надіслав заявлений відправник і що вміст повідомлення не змінювався під час пересилання;

2. Підпис документів. У діловому світі цифрові підписи широко використовуються для підписання договорів, документів та інших правових

паперів в електронному вигляді. Це усуває потребу в фізичних підписах і паперових документах, роблячи процес швидким та ефективним;

3. Розповсюдження програмного забезпечення. Розробники програмного забезпечення часто використовують цифрові підписи для підтвердження пакетів програмного забезпечення або оновлення. Це дозволяє користувачам перевірити, чи програмне забезпечення не було змінено або скомпрометовано під час завантаження та встановлення;

4. Відповідність державним і нормативним вимогам. Багато державних установ і галузей промисловості мають правила, які вимагають використання цифрових підписів для забезпечення безпека та автентичності цифрових записів і транзакцій;

5. Фінансові операції. Цифрові підписи використовуються в онлайн-банкінгу та при фінансових операціях для підтвердження особи користувача і безпечної авторизації фінансових транзакцій;

6. Автентифікація. Цифрові підписи використовуються для автентифікації користувачів у різних онлайн-сервісах та платформах. Наприклад, можна використовувати цифровий підпис для перевірки користувача, який підключається до захищеної системи;

7. Логістика. В управлінні ланцюгом постачання цифрові підписи можуть використовувати для перевірки автентичності товаросупровідних документів, рахунків-фактур, що знижує ризик шахрайства та помилок;

8. Захист інтелектуальної власності. Художники, письменники та митці можуть використовувати цифрові підписи для встановлення автентичності та прав власності на їхні цифрові роботи, наприклад як цифрове мистецтво, електронні книги та музика;

9. Нотаріальні послуги. Деякі нотаріальні онлайн-послуги використовують цифрові підписи для нотаріального засвідчення документів, додаючи до нотаріального засвідчення додатковий рівень автентифікації та безпеки.

10. Уряд і голосування. Цифрові підписи досліджено на предмет безпеки системи онлайн-голосування, що дозволяє виборцям голосувати в електронному вигляді забезпечуючи прозорість та чесність виборчого процесу.

Для всіх зазначених випадків, основною метою використання цифрових підписів є: забезпечення безпечного і надійного методу перевірки ідентичності відправника, що забезпечує цілісність даних і гарантує неспростовність, де відправник не може заперечити, що підписав документ або повідомлення. Цифрові підписи відіграють вирішальну роль у цифровій трансформації різних галузей шляхом заміни традиційних паперових підписів з безпечними та ефективними електронними альтернативами [2].

1.2. Аналіз правових аспектів функціонування цифрових підписів в Україні та світі

Попри глобальне поширення та складність в реалізації у світі, не всі взаємовідносини між учасниками процесу електронного документообігу чітко врегульовані. Загострюється це питання через відсутність специфічного законодавства та відповідних юридичних норм.

Розвиток електронного документообігу, який включає як технологічні, так і правові аспекти, вимагає інтеграції професійних знань із різних, традиційно не пов'язаних між собою, областей.

В розвинених державах електронний документообіг перетворився на важливий елемент юридичних стосунків у внутрішній та міжнародній торгівлі, що призвело до ряду значущих правових змін:

- Виникла нова правова категорія, що включає такі поняття, як електронні угоди, електронні підписи, електронні платежі та електронні гроші;
- Електронне спілкування та обмін даними, які використовуються для заключення та виконання угод, замінили традиційну паперову документацію в комерційних операціях. Це породило необхідність розробки стандартів та вимог до електронних угод;

- Суть угоди залишилася незмінною, але змінився спосіб її заключення та виконання.
- У діловому обороті зміцнився основний правовий принцип електронного документообігу, згідно з яким сторони не можуть заперечувати законність та дійсність угоди лише через її електронний формат.

Проте, в деяких випадках, дотримання цього принципу натрапляють на труднощі, що призводить до юридичних комплікацій. Існує ризик, що не всі положення електронної угоди будуть мати однакову юридичну вагу при судовому розгляді.

У сучасному світі, де економіка має глобальні масштаби і складну структуру, жоден уряд чи державний орган не може ефективно регулювати її в режимі реального часу. Отже, необхідно звести законодавство до необхідного мінімуму, забезпечити його міжнародний характер, прозорість і консистентність, а також чіткість у визначенні основних цілей.

Закони, міжнародні та вітчизняні, повинні створювати довіру, забезпечувати ефективність і узгодженість у нормах поведінки. Важливо також закріпити основні процедури для визнання легітимності електронних угод та визначити, як судові органи повинні розглядати справи, що стосуються застосування електронного цифрового підпису та інших подібних питань.

Регулююче Законодавстов в Україні. Державна регуляція у сфері реалізується через два ключові органи: Національний банк України, який встановлює технологічні стандарти, в тому числі безпеку платежів, та Департамент спеціальних телекомунікаційних систем та захисту інформації при Службі безпеки України, відповідальний за вимоги щодо захисту інформації. З розвитком сучасних інформаційних технологій, концепція, що більшість документів буде переведена в електронний формат і матиме таку саму юридичну вагу, як традиційні паперові документи, стає все більш прийнятною та реалістичною.

Відповідно до статті 6, Закону України «Про електронні документи та електронний документообіг», визначається що «Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для

ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу»

Відповідно до статті 5 Закону України «Про електронні документи та електронний документообіг» термін електронний документ - це «документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.»

Відповідно до статті 1 Закону України «Про електронні документи та електронний документообіг» визначається окремо ряд термінів, а саме:

- засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;
- особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;
- відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;
- засвідчення чинності відкритого ключа - процедура формування сертифіката відкритого ключа;
- сертифікат відкритого ключа (далі - сертифікат ключа) - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;
- посилений сертифікат відкритого ключа (далі - посилений сертифікат

ключа) - сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

- акредитація - процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;
- компрометація особистого ключа - будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;
- блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;
- підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;
- послуги електронного цифрового підпису - надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;
- 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.

Відповідно до статті 4 Закону України «Про електронні документи та електронний документообіг», визначається призначення електронного цифрового підпису [3].

Електронний цифровий підпис створено для підтримки діяльності індивідуальних та корпоративних суб'єктів, які ведуть свої операції за допомогою електронних документів.

Стандарт X.509, розроблений міжнародним технічним комітетом ITU-T, є важливим у цій сфері і дотримується в більшості країн, що розвивають національні та міжнародні системи електронного документообігу із застосуванням цифрових підписів.

Електронний цифровий підпис застосовується учасниками електронного документообігу, як фізичними, так і юридичними особами, для ідентифікації особи, що підписує, та забезпечення незмінності інформації в електронному вигляді.

Застосування електронного цифрового підпису не вносить змін у встановлений законодавством порядок підписання договорів та інших документів у письмовій формі.

Резюмуючи розвиток правового середовища в Україні, що стосується електронного документообігу, слід підкреслити значні покращення і досягнення, які були здійснені в цій області останнім часом. Це, ймовірно, пов'язано з активним входженням України в сферу електронної торгівлі та електронних послуг, які займають важливу частину світового ринку.

Інновації в технологіях, нарешті, почали відображатися у вітчизняному законодавстві. Такі нововведення, ефективно імплементовані в судовій практиці, нададуть українським компаніям захист як на внутрішньому, так і на зовнішньому ринках, не поступаючись у конкурентній боротьбі на широкому сегменті ринку, що включає електронний документообіг[4].

Регулююче Законодавстов в Сполучених Штатах Америки. Федеральний закон США про електронні підписи у глобальній і національній торгівлі розширює застосування електронних підписів, контрактів та інших записів у сфері торгівлі. Цей закон спрощує використання електронних записів і підписів у міжштатній та міжнародній торгівлі. Хоча на рівні штатів є багато законів про електронні підписи, у сфері міжштатної та міжнародної торгівлі переважно застосовуються федеральні законодавчі акти. Таким чином, цей закон охоплює значну частку американської торгівлі [5].

Основні положення цього закону включають:

- Відсутність відмови в юридичній силі, дійсності чи виконанні підпису,

контракту чи іншого запису, що стосується транзакції, лише через їхнє електронне втілення;

- Заборона позбавлення контракту, пов’язаного з транзакцією, юридичної сили, дійсності або позовної сили лише через використання електронного підпису або електронного запису під час його формування;
- Акт не обмежує, змінює або впливає на будь-які інші вимоги, встановлені законом, нормативним актом чи правилом, що стосується прав і обов’язків осіб, крім вимог щодо оформлення контрактів чи інших документів у неелектронній формі;
- Акт не вимагає від будь-якої особи згоди на використання або прийняття електронних записів чи електронних підписів, за винятком урядових установ, щодо записів, у яких вони є стороною, крім контрактів.

Електронні методи не можуть бути відкинуті як недійсні або позбавлені юридичної сили тільки через їх електронну форму. Приватні особи не зобов'язані приймати або використовувати електронні підписи, однак для державних установ це все ще може бути допустимим способом діяльності.

У разі надання споживачем згоди на використання електронних записів неурядовими організаціями, такі підписи можуть вважатися достатніми для виконання будь-яких вимог щодо письмової форми інформації. Проте, якщо споживач не погодився на електронні підписи, він має право використовувати традиційні паперові документи.

Таким чином, законодавство забезпечує споживачам право вибору між електронними та фізичними методами документації [6].

Регулююче Законодавстов в Європейському Союзі. Європейський Союз активно розробляє законодавство, що стосується електронних підписів.

Директива 1999/93/ЕС була ініціативою ЄС у цій області, метою якої було забезпечення сумісності продуктів електронного підпису та усунення можливих бар'єрів для електронних комунікацій і торгівлі, які могли виникати через відмінності у правилах внутрішнього ринку ЄС[7].

Стаття 5 зазначеної директиви визначає юридичні наслідки електронних підписів, зазначаючи, що розширені електронні підписи, засновані на кваліфікованому сертифікаті та створені з використанням захищеного пристрою для створення підпису, мають відповідати юридичним вимогам, які ставляться до звичайних підписів у паперовій формі, і повинні бути допустимими як докази в судових розглядах.

Згідно з текстом директиви: «Держави-члени забезпечують, що такі розширені електронні підписи: відповідають юридичним вимогам, які ставляться до власноручного підпису на папері та можуть використовуватися як доказ у судових розглядах. Держави-члени гарантують, що електронний підпис не втрачає юридичної сили та прийнятності як доказу в суді лише через те, що він: електронний, не заснований на кваліфікованому сертифікаті, не заснований на кваліфікованому сертифікаті, виданому акредитованим сертифікаційним центром, не створений за допомогою захищеного пристрою для створення підпису».

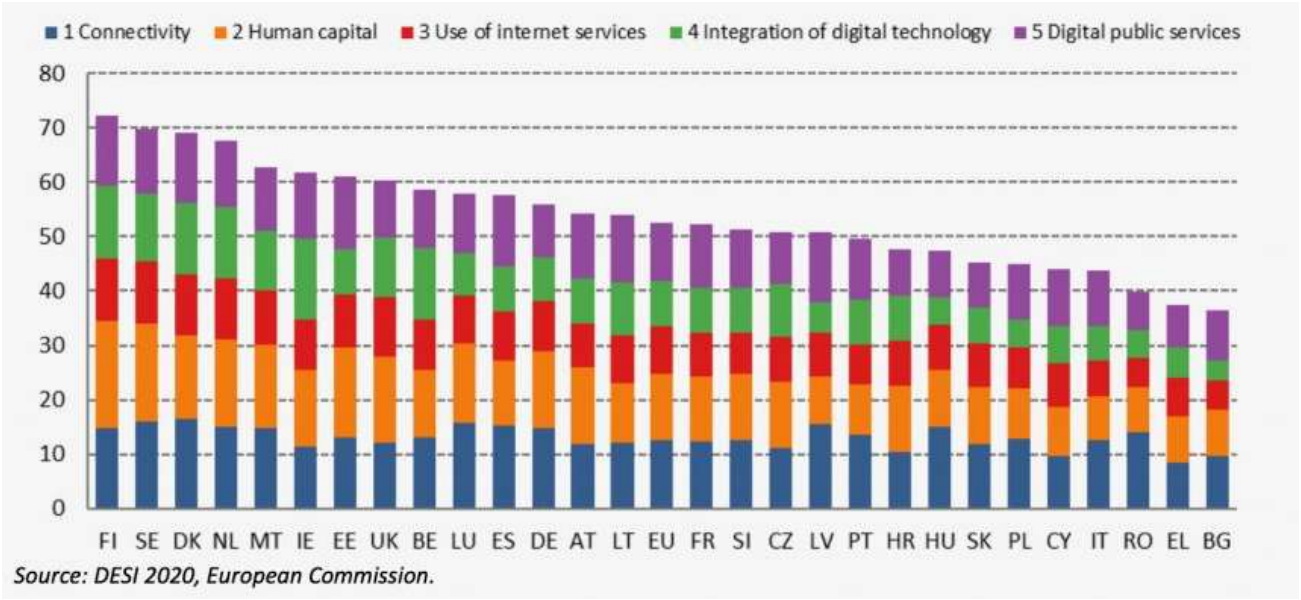

Рис.1.2. Інтеграція технології цифрового підпису в країни ЄС

З часом, Директива ЄС про електронні підписи виявилася недостатньою. Відгуки зазначали, що вона не забезпечила уніфіковану і перетинну структуру для безпечних і простих у використанні електронних транзакцій на рівні транскордонної і міжсекторної взаємодії. Громадяни ЄС зіткнулися з проблемами

у використанні електронної ідентифікації у різних державах-членах. У відповідь на це, Директива була замінена регламентом eIDAS.

eIDAS встановлює правила для електронної ідентифікації та супутніх довірчих послуг, необхідних для забезпечення безпеки електронної комерції в ЄС. Регламент включає такі ключові визначення:

Ідентифікаційні дані особи, які дозволяють чітко ідентифікувати особу для електронної ідентифікації.

Електронні підписи і розширені електронні підписи, які є більш безпечними та мають такі характеристики:

- Створені з використанням даних, що перебувають під одноосібним контролем підписувача;
- Пов’язані з даними, які підписуються, таким чином, що будь-які зміни виявляються.

Кваліфіковані електронні підписи, які створені за допомогою спеціалізованого пристрою та засновані на кваліфікованому сертифікаті. Пристрої для створення кваліфікованого електронного підпису, які складаються з безпечних апаратно-програмних компонентів. Кваліфіковані сертифікати для електронних підписів, що пов'язують криптографічні ключі з особами чи організаціями, видаються кваліфікованими постачальниками довірчих послуг. Проєктування систем для забезпечення безпечного ведення бізнесу в Інтернеті, як для приватного, так і для державного сектору[8].

1.3. Вимоги до електронного підпису

Електронні та цифрові підписи стають ключовими інструментами у цифровому епосі для забезпечення безпеки та юридичної валідності різноманітних онлайн-транзакцій, документацій та державних послуг. Ці технології забезпечують надійний та визнаний спосіб електронного підпису документів.

Стаття 26 Регламенту ЄС 910/2014 про електронну ідентифікацію та довірчі послуги на внутрішньому ринку визначає критерії для просунутого електронного

підпису (AES), який є важливим елементом в сучасних цифрових транзакціях. Відповідно до регламенту, AES повинен відповідати наступним вимогам:

- Унікальне пов'язування з підписантом. AES повинен бути безпосередньо асоційований з особою, яка його створює. Це забезпечує відповідальність та неможливість заперечення авторства підпису;
- Ідентифікація підписанта. Система повинна забезпечувати надійне визначення особи підписанта, використовуючи унікальні характеристики або дані, що дозволяють точно ідентифікувати особу;
- Контроль даних для створення підпису. AES має бути створений за допомогою даних (наприклад, закритого ключа шифрування), які перебувають під одноосібним контролем підписувача, що забезпечує безпеку та цілісність процесу підписання.
- Виявлення змін у підписаних даних. AES повинен бути пов'язаний із підписаними даними таким чином, що будь-які зміни після підписання можна виявити. Це гарантує, що документ не був змінений після підписання.

Регламентом також визначено декілька різновидів електронних підписів, а саме:

- Звичайний електронний підпис. Цей тип підпису включає будь-які дані в електронній формі, які використовуються підписувачем для підписання. Приклади включають рукописний підпис, зроблений за допомогою стилуса або миші, або підпис, генерований комп'ютером. Важливо, що цей тип підпису не вимагає залучення незалежної третьої сторони для верифікації особи підписувача (рис.1.3).

Дані про застосування та ефективність електронних підписів у сучасному світі свідчать про їх вирішальну роль у цифровій трансформації бізнес-процесів та управлінні документообігом. Завдяки цим технологіям забезпечується вищий рівень безпеки, прозорості та ефективності у сфері цифрової комерції та обміну документацією.

Рис.1.3. Приклад звичайного цифрового підпису

- Розширений електронний підпис (AES). Більш складний та безпечний вид електронного підпису, створений за допомогою криптографії з відкритим ключем (PKI). AES вбудовується безпосередньо в код електронного документа, забезпечуючи вищий рівень безпеки та ідентифікації підписанта (рис.1.4). Вимоги до AES визначені в статті 26 Регламенту.

Регламент є технологічно нейтральним і не вказує конкретні технічні способи реалізації цих вимог. Форум європейських наглядових органів для електронних підписів надає додаткові рекомендації та вказівки, зокрема, в документі, опублікованому у жовтні 2004 року, вказуючи на те, що AES зазвичай досягається за допомогою технології PKI.

Використання електронних підписів у транзакціях включає вибір між різними видами підписів в залежності від потреб безпеки та автентичності. Підприємства повинні враховувати варіанти використання стандартних, розширених або кваліфікованих електронних підписів залежно від вимог їхніх операцій та юридичних вимог.

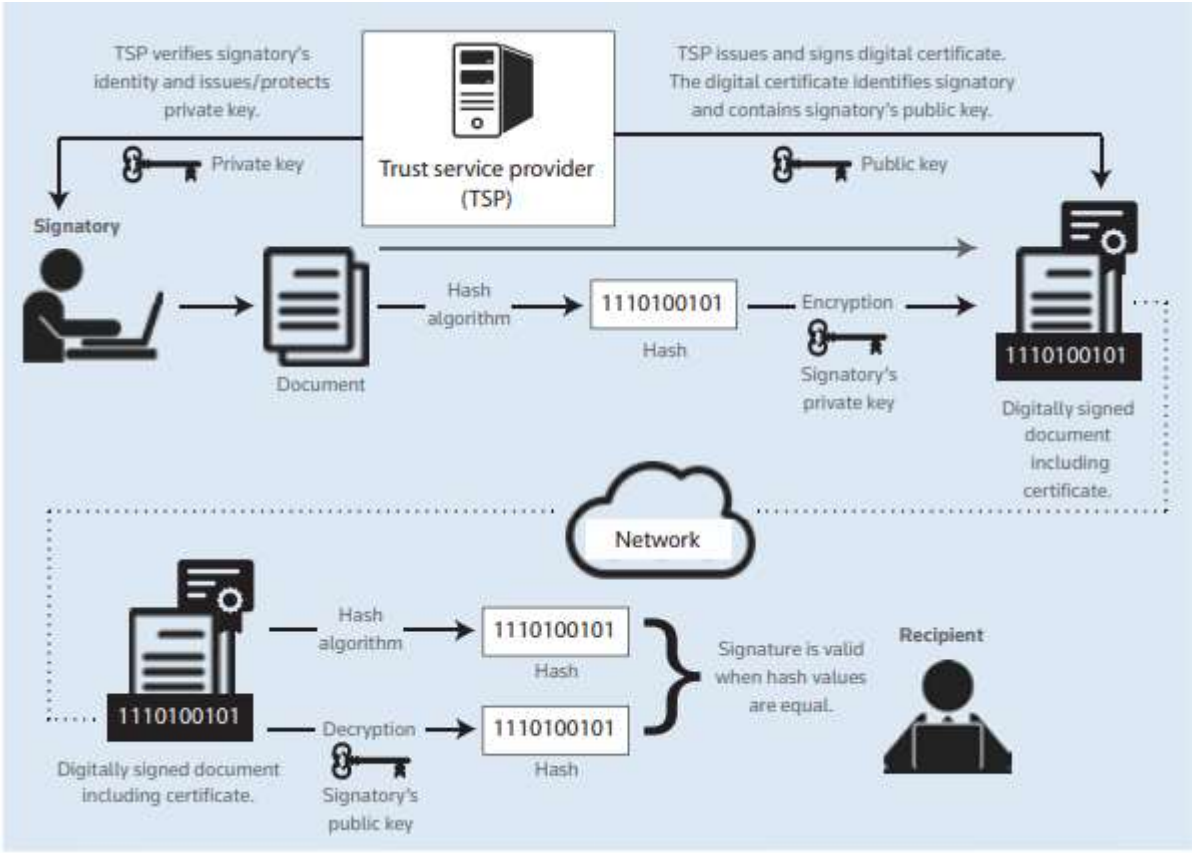

Рис.1.4. Приклад розширеного електронного підпису

Для створення цифрового підпису, як AES, постачальник платформи використовує криптографічний алгоритм для генерації публічного та приватного ключів, що разом утворюють пару ключів. Підписант використовує свій приватний ключ для шифрування хешу електронного документа.

Хеш — це унікальний відбиток документа, створений за допомогою хеш-функції, який забезпечує його унікальність. Зашифрований хеш є цифровим підписом, який надсилається разом з електронним документом одержувачу.

Одержувач використовує публічний ключ підписанта для розшифровки цифрового підпису і перевірки його справжності. Одержувач також генерує свій власний хеш документа і порівнює його з розшифрованим цифровим підписом. Якщо вони співпадають, це підтверджує, що цифровий підпис є дійсним і документ не був змінений[9].

Пари ключів можуть бути схильні до ризиків, таких як підробка, крадіжка або створення з використанням фіктивної особи. Щоб управляти цим ризиком,

використовується цифрова сертифікація. Цифровий сертифікат, який видається постачальником платформи або третьою довіреною стороною (постачальником довірчих послуг), перевіряє і підтверджує особу підписанта, наприклад, за допомогою перевірки паспорта, і містить публічний ключ підписанта.

Цифровий сертифікат криптографічно прив'язаний до електронного документа, що містить цифровий підпис. Одержувач, маючи цифровий сертифікат, може бути впевнений у тому, що підписант є тим, ким він себе видає, та використовує публічний ключ підписанта для підтвердження дійсності цифрового підпису. Це створює надійну систему, що дозволяє перевірити автентичність та цілісність електронного документа.

1.4. Аналіз вимог щодо провайдерів платформ електронного підпису

Щодо угод з постачальниками платформ електронного підпису, існує кілька ключових питань, які повинні бути враховані. Часто ці платформи пропонуються як хмарні сервіси (SaaS) з можливістю доступу через веб-браузер на основі підписки, яка може тривати від одного до трьох років. Це означає, що програмне забезпечення та клієнтські дані розміщуються на спільній IT-інфраструктурі. Інколи провайдери надають можливість розгортання на локальній платформі або в приватній хмарі, але частіше вони пропонують публічну хмарну службу.

При виборі постачальника платформи електронного підпису компанії повинні враховувати такі аспекти, як безпека даних, відповідність законодавчим вимогам, надійність і доступність сервісу, а також вартість і умови підписки.

Модель SaaS (програмне забезпечення як послуга) пропонує клієнтам ряд переваг, таких як масштабованість, нижча вартість та доступ до останніх оновлень без додаткових витрат на оновлення програмного забезпечення. Проте, ця модель також змушує клієнтів відмовитися від контролю над обробкою та зберіганням своїх даних, що створює виклики у забезпеченні відповідності, особливо в контексті Директиви про захист даних (95/46/ЕС) та регулювання з боку FCA (Фінансової контрольної агенції).

Автентифікація підписантів часто включає використання електронної пошти, що є достатнім для більшості транзакцій у світі. Для забезпечення більшої впевненості, клієнти можуть використовувати двофакторну автентифікацію, наприклад через SMS, одноразові паролі або аутентифікацію на основі знань. Двофакторна автентифікація забезпечує більшу строгість процесу, залишаючись при цьому менш громіздкою та дешевшою, ніж отримання AES або QES.

Ці додаткові послуги автентифікації зазвичай надаються третіми сторонами і перепродаються постачальником платформи. Клієнти повинні вимагати від постачальника гарантії щодо якості цих послуг або наполягати на тому, що будь-які послуги, які перепродаються постачальником від третьої сторони, передаються з гарантіями.

Щодо інтеграції з іншими корпоративними додатками, багато провідних платформ вже інтегровані з такими системами, як Salesforce, Microsoft і Google. Вони також пропонують API, що дозволяє клієнтам інтегрувати електронні підписи з власними бізнес-системами. Ця функціональність є важливою для клієнтів, але стандартні умови постачальника не завжди гарантують успішну інтеграцію. Клієнти повинні вимагати технічного завдання для інтеграції платформи з іншими програмами та гарантій від постачальника, що інтеграція буде функціонувати належним чином.

Гарантії, які надає постачальник платформи електронного підпису, зазвичай є обмеженими, особливо у порівнянні зі стандартними умовами SaaS. Основною гарантією, яку повинен надавати постачальник, є забезпечення, що платформа виробляє електронний підпис, який відповідає вимогам політик безпеки та положень ЄС про електронні підписи. Якщо підпис є AES, постачальник повинен також гарантувати, що підпис та відповідний цифровий сертифікат відповідають і вимогам Закону України «Про електронні документи та електронний документообіг».

Однак, постачальники зазвичай уникають гарантування того, що створений електронний підпис є дійсним для будь-якого конкретного договору з юридичною силою. Це пов'язано з тим, що постачальник не має інформації про конкретний

договір, який підписується, про регулюючий закон або юрисдикцію, де договір може бути примусово виконаний. Визначення, чи може договір бути укладено в електронній формі за допомогою певного типу електронного підпису, залишається на розсуд клієнта та його юристів. Крім того, постачальник, швидше за все, вимагатиме від клієнта гарантії, що використання платформи відповідає всім відповідним законам і нормативним актам.

Провідні провайдери платформ електронного підпису часто роблять важливі заяви про своє дотримання та відповідність встановленим технічним стандартам, які затверджені авторитетними організаціями, такими як ETSI (Європейський інститут телекомунікаційних стандартів), ISO (Міжнародна організація зі стандартизації) та CEN (Європейський комітет з нормалізації). Такі технічні стандарти, наприклад CAdES (Розширені формати електронного підпису), XAdES (Розширені XML-формати електронного підпису) та PAdES (PDF-формати електронного підпису), відіграють важливу роль для клієнтів і їхніх головних технічних директорів при виборі платформи.

Важливо визнати, що хоча дотримання технічних стандартів є важливим інструментом для демонстрації відповідності вимогам міжнародних стандартів та законів, це не замінює гарантії того, що платформа створює підписи, які відповідають вимогам політик безпеки.

Що стосується угод про рівень обслуговування (SLA), постачальники не завжди добровільно надають такі гарантії, тому клієнти повинні наполягати на них і переконатися, що постачальник підтримує платформу до необхідного стандарту. У випадку, якщо рівень обслуговування нижчий за стандарт, клієнту повинні бути виплачені компенсаційні кредити. Однак, право на припинення контракту у випадку постійних порушень SLA може бути важко досягти.

Одним з ключових показників у SLA є доступність платформи. Провідні провайдери зазвичай використовують мультисерверні архітектури в кількох центрах обробки даних для забезпечення високої доступності, так що планове чи екстрене технічне обслуговування не впливає на роботу платформи. Вони можуть

брати на себе зобов'язання забезпечувати 99,9% або навіть 100% доступність протягом терміну дії контракту.

Провідні постачальники платформ електронного підпису, як правило, прагнуть обмежити свою фінансову відповідальність перед клієнтом до суми, сплаченої за 12 місяців, що передували даті виникнення претензії. В деяких випадках, після переговорів, вони можуть погодитися збільшити максимальну суму відповідальності до загальної суми, сплаченої замовником за весь період дії договору. Також вони зазвичай виключають відповідальність за спеціальні, непрямі та наслідкові збитки [10].

Більшість постачальників також намагаються виключити свою відповідальність за втрату або пошкодження даних, стверджуючи, що клієнти повинні самостійно здійснювати резервне копіювання усіх підписаних електронних документів на платформі. Однак, клієнти повинні вимагати включення відповідальності за втрату або пошкодження даних, якщо це сталося через помилку постачальника.

У зв'язку з новим Загальним регламентом про захист даних (GDPR), який значно збільшує максимальні штрафи за порушення законів про захист даних, відшкодування збитків клієнтам за порушення цих законів стає більш актуальним. Новий регламент встановлює максимальний штраф у розмірі до 4% від річного світового обороту клієнта або 20 мільйонів євро. В результаті, деякі постачальники починають погоджуватися на окрему межу відповідальності, яка може становити від двох до п'яти разів більше вартості угоди.

Однак важливо зазначити, що клієнти повинні бути уважними при визначенні умов SLA, особливо в контексті доступності платформи та резервного копіювання даних. Вони повинні переконатися, що постачальник зобов'язаний підтримувати платформу на високому рівні та гарантувати, що інтеграція з іншими системами відповідає встановленим специфікаціям[11].

Висновки до першого розділу

Проаналізовано поняття цифрового підпису. Зазначено, що електронні та цифрові підписи стають ключовими інструментами у цифровому епосі для забезпечення безпеки та юридичної валідності різноманітних онлайн-транзакцій, документацій та державних послуг. Ці технології забезпечують надійний та визнаний спосіб електронного підпису документів.

Досліджено вітчизняне та міжнародне законодавство, що регламентує особливості функціонування електронних цифрових підписів. Державна регуляція у сфері реалізується через два ключові органи: Національний банк України, який встановлює технологічні стандарти, в тому числі безпеку платежів, та Департамент спеціальних телекомунікаційних систем та захисту інформації при Службі безпеки України, відповідальний за вимоги щодо захисту інформації.

Зазначено вимоги щодо цифрових підписів, особливості та їх класифікації. Виокремлено вимоги щодо постачальників послуг, що відповідальні за розробку та видачу цифрових підписів.

2 ДОСЛІДЖЕННЯ АЛГОРИТМІВ ТА СТАНДАРТІВ СТВОРЕННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

2.1. Цифровий сертифікат

Цифровий сертифікат схожий на паспорт, але складається з бітів. Отримавши цифровий сертифікат, особа, комп'ютер або організація можуть безпечно обмінюватися інформацією. Використання сертифікатів полегшується за допомогою PKI.

Кожен сертифікат надає ідентифікаційну інформацію, є стійким до підробок і може бути перевірений центром сертифікації (CA). Інша назва цифрового сертифіката — сертифікат відкритого ключа, оскільки сертифікат містить ідентифікаційну інформацію, наприклад унікальний відкритий ключ власника сертифіката. ЦС є довіреною організацією, яка видає цифрові сертифікати, керує ними та може відкликати їх. Майже кожен ЦС використовує реєстраційний орган (RA), який діє як посередник у процесі сертифікації. RA — це орган, який перевіряє запити користувачів і повідомляє ЦС, чи повинен ЦС видавати сертифікат чи ні. ЦС, окрім видачі сертифікатів, відповідає за керування сертифікатами. Коли сертифікат відкликано, він додається до списку відкликаних сертифікатів (CRL). Цей список відіграє важливу роль у процесі оцінки сертифіката.

Список загальнодоступний і використовується для відхилення сертифікатів, які інакше можуть бути прийняті як дійсні. Коли документ підписується цифровим підписом, одержувач перевіряє, чи немає в цьому списку сертифіката, який використовується для підписання документа. Якщо він є в CRL, то підпис недійсний. CRL зазвичай зберігається в каталозі, який також містить дійсні та заблоковані сертифікати.

Необхідно зауважити, що якщо сертифіката немає в CRL, але дата й час підпису не входять у період часу, коли сертифікат дійсний, тоді підпис також недійсний.

Цифрові сертифікати використовуються в поєднанні з HTTPS для забезпечення односторонньої або взаємної автентифікації, а також безпечного зв’язку між клієнтом і сервером.

На рис.2.1 показано приклад сертифіката та його використання. Веб-сайти, які вимагають високого рівня безпеки (наприклад, державні, банківські веб-сайти та веб-сайти електронної комерції), матимуть сертифікат SSL із розширеною перевіркою. URL-адреса сайтів із таким сертифікатом відображається багатьма браузерами як зелена URL-адреса, яка вказує на те, що веб-сайт є надійним і має дійсний цифровий сертифікат [12].

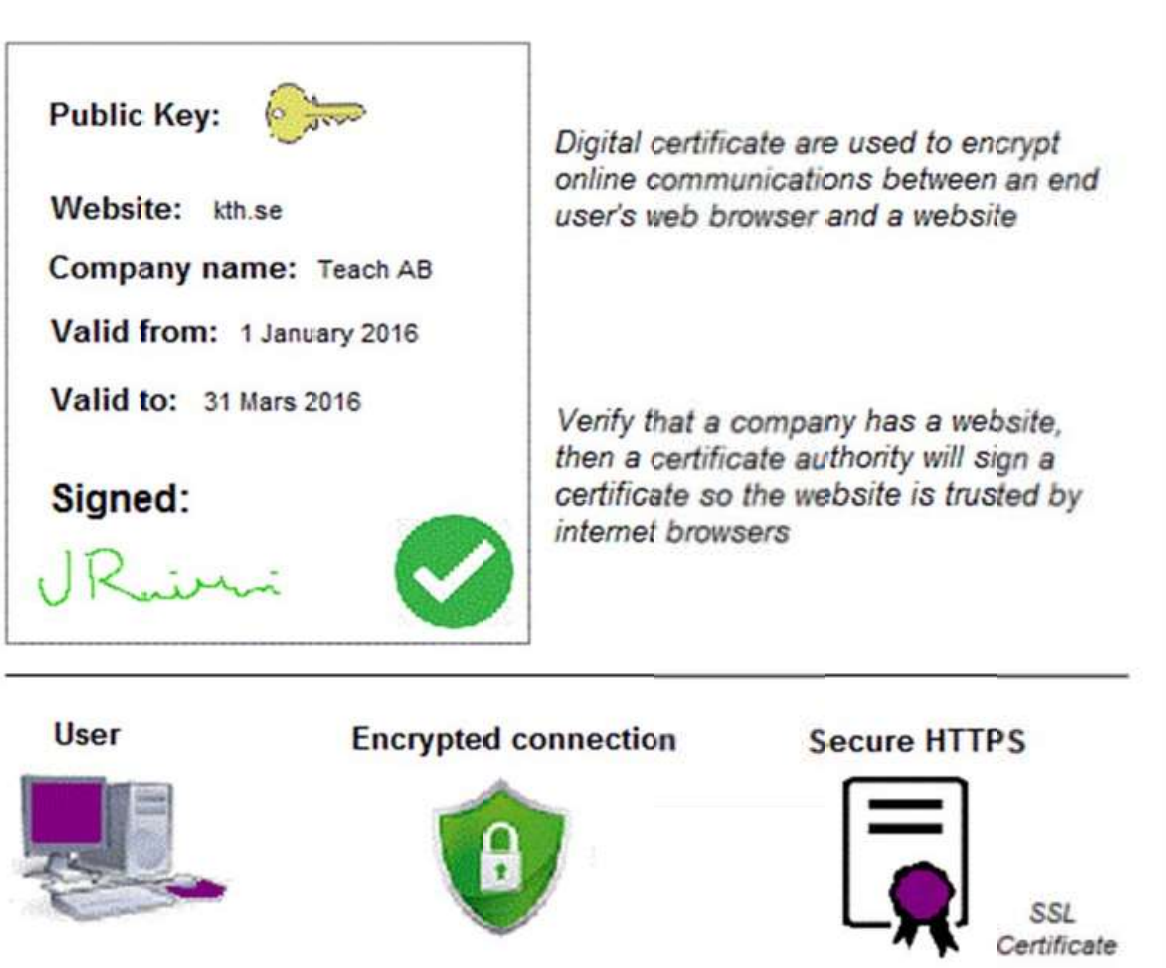

Рис.2.1. Приклад цифрового сертифіката та приклад з’єднання між клієнтом і сервером через SSL

За замовчуванням ряд сертифікатів ЦС попередньо інстальовано на комп’ютері під час інсталяція операційної системи або вбудовано у веб-браузер.

Таким чином, користувач/комп’ютер може знати, чи є веб-сайт із даним сертифікатом довіреним чи ні – на основі неявної довіри до цих ЦС із «вбудованими» або попередньо налаштованими сертифікатами. Однак слабкою стороною є те, що в більшості випадків кінцевий користувач не знає, яким центрам сертифікації він насправді повинен довіряти.

Сертифікат може бути реалізований як жорсткий або м’який сертифікат залежно від того, де знаходяться закриті ключі розташовані. Жорсткий сертифікат зберігає закритий ключ на смарт-картці, тому ці ключі більш безпечні обробляється, ніж коли цей ключ зберігається у файлі, і в результаті сертифікат вважається більшим надійний. У випадку з програмним сертифікатом закритий ключ зберігається у файлі. Цей файл може бути передано на флешці, диску, хмарне сховище чи інший тип сховища та зазвичай захищено паролем. Цей тип сертифіката зазвичай вважається менш безпечним, ніж «твердий» сертифікат. Однак фактичний рівень безпеки залежить від шифрування, яке використовується для зберігання закритого ключа.

2.2. Схеми та стандарти створення цифрових підписів та сертифікатів

Цифрові системи є сучасними технологічними рішеннями проблем, з якими стикаються електронні підписи. Вони надають одержувачу криптографічні засоби для перевірки цілісності, а також забезпечують автентифікацію автора та даних, таким чином забезпечуючи більш сильну властивість неспростування. Вони також можуть, за певних обставин у певних юрисдикціях, дозволити юридичне нотаріальне засвідчення. Оскільки вони є математичними конструкціями, які покладаються на обчислювальну неможливість розв’язання складних проблем, вони вразливі до неправильного вибору алгоритмічних параметрів.

Цифрові системи, як правило, більш уразливі до фізичного втручання, ніж програмні атаки – якщо ви можете отримати фізичний доступ до сервера, це часто є легшим вектором атаки, ніж криптографічно захищені програмні рішення.

RSA. Rivest-Shamir-Adleman (RSA) — це (асиметрична) криптосистема з відкритим ключем (рис.2.2). Спирається на модульну арифметику та розкладання добутків великих простих чисел на прості множники і дозволяє користувачеві генерувати ключі довільної довжини. RSA вважають повільним алгоритмом – інші схеми відкритих ключів зазвичай пропонують кращу продуктивність (швидше генерування ключів, шифрування та дешифрування) для певного рівня безпеки. Зазвичай використовується для передачі спільних (симетричних) криптографічних ключів.

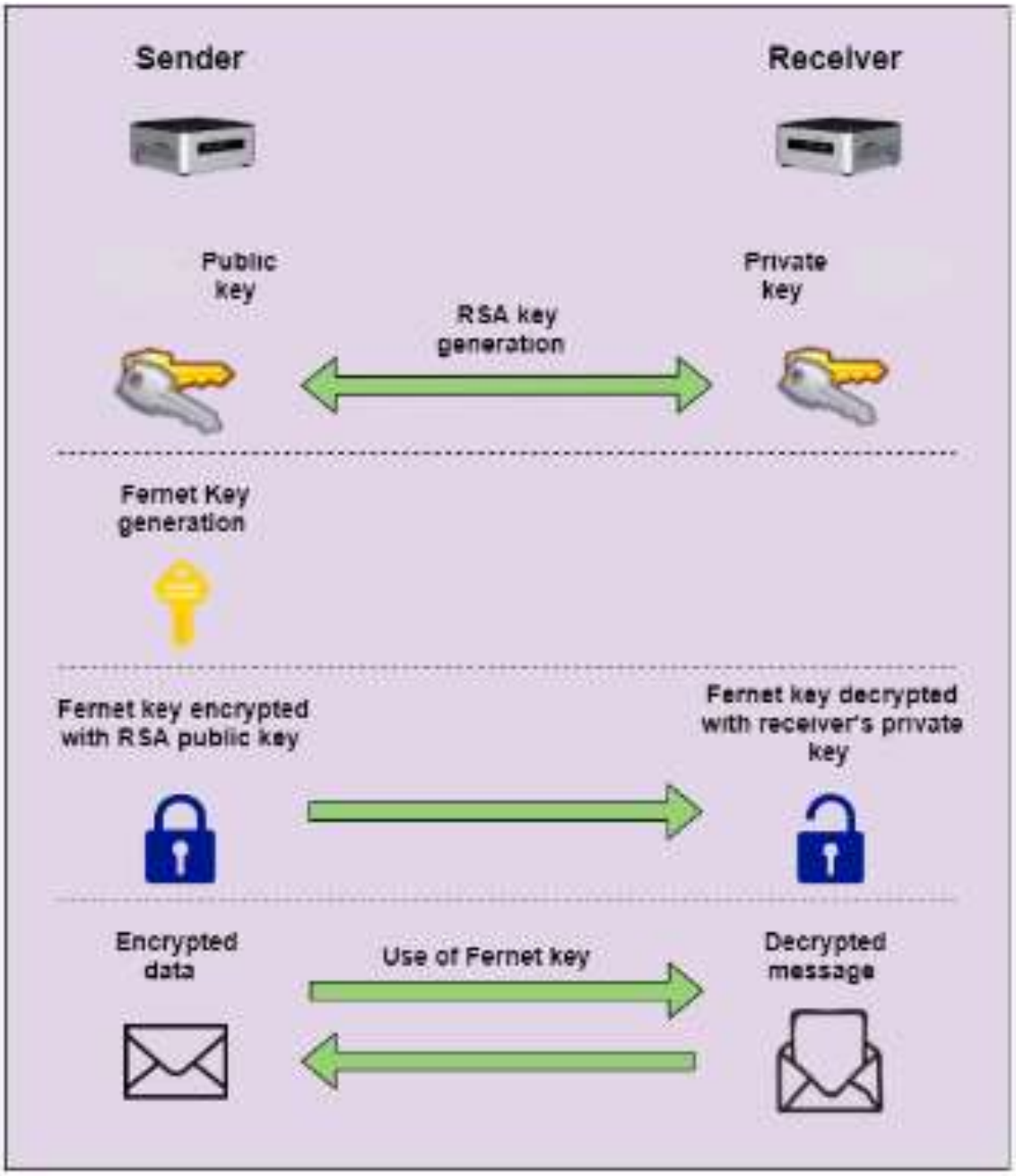

Рис.2.2. Приклад реалізації RSA

У класичному випадку, з класичними комп’ютерами, сита загального поля чисел виявилися найкращим інструментом взагалі для чисельного розбиття схем RSA. Нещодавно було факторизовано RSA-250 (829-бітний ключ RSA). Крім того, невдалий вибір пар ключів може становити загрозу, як і певні вразливості реалізації програмного забезпечення. Уразливості також існують на апаратному рівні, звичайно, що забезпечило чудові вектори атак; Завдяки вибраним зашифрованим текстам і можливості вимірювання навколишнього звуку під час операцій дешифрування на комп’ютері дослідники змогли проаналізувати записаний звук для відновлення ключів RSA. І, зокрема, це може не обмежуватися RSA. Існує ряд варіацій RSA, а саме: RSA-PKCS#1 v1.5, RSA-PSS, ймовірнісна схема підпису, яка може бути більш безпечною, ніж RSA-PKCS#1 v1.5, ефективний RSA, залежна RSA, Carmichael RSA, спільний RSA, Multi Prime RSA, загальний простий RSA, CRT-RSA, та перебалансований CRT-RSA [13].

DSA. Алгоритм цифрового підпису — це федеральний стандартний алгоритм обробки інформації для використання з цифровими підписами, що базується на модульній арифметиці та проблемі дискретного логарифму (рис.2.3). DSA є варіантом схем підпису Шнорра та Ель-Гамала. Національний інститут стандартів і технологій США (NIST) прийняв DSA як частину стандарту цифрового підпису (DSS) у FIPS-186 у 1994 році. Вона, як і RSA, є однією зі старих криптосистем, яка все ще використовується сьогодні. Зроблено чотири редакції, а п’ята в роботі. Редакція 4 дозволяє генерувати ключ довжиною 1024, 2048 або 3072 біт. Розміри ключів довжиною 1024 і 2048 наразі вважаються небезпечними.

Запропонований п’ятий перегляд стандарту FIPS186 рекомендує, використовувати DSA для генерації цифрового підпису, хоча це дозволяє продовжувати використання застарілі версії спеціально для цілей перевірки існуючих підписів. Наприклад, OpenSSH вимкнув підтримку DSS (і, відповідно, DSA) за замовчуванням ще в 2015 році, нібито через проблеми безпеки [14].

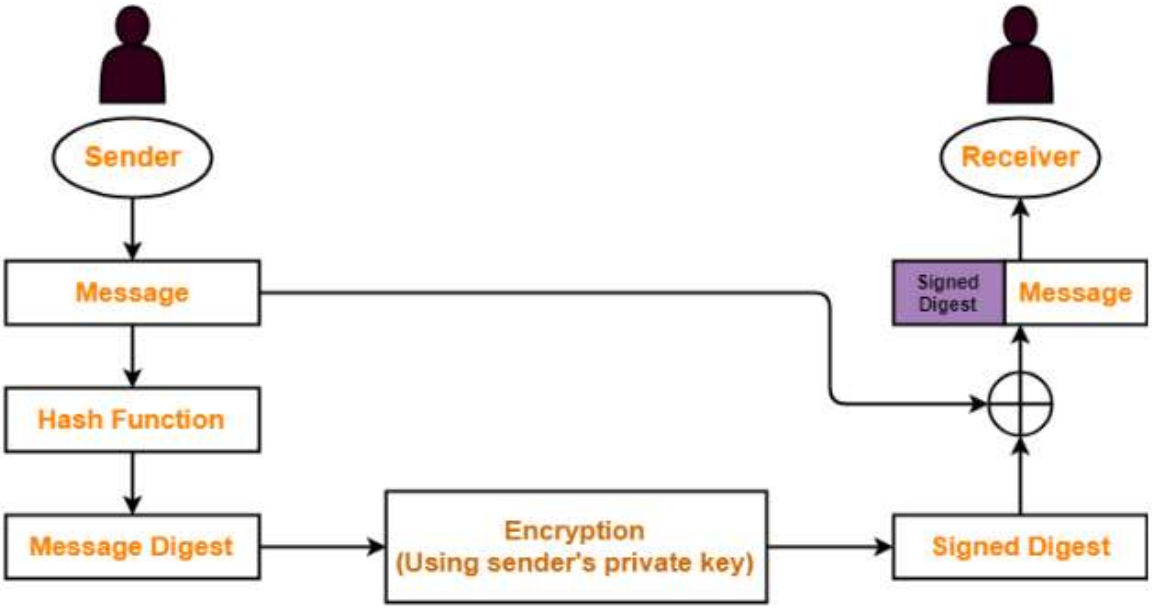

Рис.2.3. Приклад роботи DSA

X.509. X.509 — це стандартизований формат цифрового сертифіката, який використовує PKI для перевірки того, що відкритий ключ належить певному користувачу, комп'ютеру чи службі, як зазначено в сертифікаті. Стандарт X.509 є ключовим засобом безпечного спілкування в Інтернеті та електронною поштою. Сертифікати X.509 включають таке:

- Версія вказує, яка версія X.509 застосовна до цього сертифіката;
- Серійний номер/Ідентифікатор алгоритму підпису — унікальне ціле число, присвоєне центром сертифікації визначає алгоритм (RSA або DSA), який потрібно використовувати з підписом;
- Назва постачальника визначає, який ЦС підписав і видав сертифікат;
- Період дії інтервал часу, протягом якого сертифікат дійсний (виражений датою початку та закінчення);
- Ім'я суб'єкта/ім'я особи/інформація про відкритий ключ, на яку видається сертифікат предмета містить матеріал відкритого ключа та ідентифікатор алгоритму;
- Розширення (необов'язково). Наприклад: унікальний ідентифікатор емітента та ідентифікатор унікальний суб'єкт.

Сертифікат X.509 використовується в багатьох формах криптографії, включаючи: TLS/SSL, Secure/Multipurpose Internet Mail Extensions (S/MIME), HTTPS та смарт-карти [15].

TLS/SSL. Сертифікат безпеки транспортного рівня (TLS) або рівня захищених сокетів (SSL) є версією сертифіката X.509, але має розширене використання ключа. Сертифікат SSL використовується разом із криптографічним протоколом SSL для забезпечення безпечного зв'язку через комп'ютерну мережу. Наприклад, як частина HTTPS, сертифікат SSL широко використовується веб-сайтами електронної комерції, що дозволяє користувачам купувати продукти чи послуги через веб-сайт.

Основною метою протоколу SSL є забезпечення цілісності даних між двома взаємодіючими комп'ютерними програмами (тому це часто розглядають як протокол прикладного рівня). Цей зв'язок зазвичай відбувається між клієнтом (веб-браузером) і сервером (веб-сторінкою). Необхідно зауважити, що найнадійніша форма цього захисту вимагає, щоб і клієнт, і сервер мали сертифікат, який можна перевірити [16].

ECDSA. Стандарт цифрового підпису еліптичної кривої є варіантом DSA, схваленого NIST, який використовує дискретні логарифми, але в контексті криптографії еліптичної кривої. Обґрунтування цього полягає в тому, що важко знайти дискретний логарифм випадкового елемента еліптичної кривої відносно загальновідомої базової точки. Криптографія з еліптичною кривою пропонує рівні безпеки, еквівалентні старим криптосистемам при значно менших розмірах ключів. Найкращими криптоаналітичними інструментами для зламу ECDSA є алгоритм гігантського кроку за кроком і метод факторизації Полларда [17].

Стандарти криптографії з відкритим ключем (PKCS). Набір стандартних методів криптографії з відкритим ключем, опублікований RSA Security Inc. на початку 1990-х років. PKCS #7 (сьогодні відомий як Cryptographic Message Syntax (CMS)) визначає загальний синтаксис повідомлення, який включає криптографічні деталі, такі як цифрові підписи та шифрування. Одна з головних переваг CMS полягає в тому, що вона дозволяє багаторазову інкапсуляцію, де одна інкапсуляція

(конверт) може бути вкладена в іншу. Крім того, попередньо інкапсульовані дані можуть бути підписані цифровим підписом певної сторони. Разом із вмістом повідомлення можна підписувати довільні атрибути, наприклад час підписання. Це передбачає додаткові атрибути, такі як контрпідписи, пов'язані з підписом (RFC 5652).CMS підтримує різні архітектури для керування ключами на основі сертифікатів, де X.509 є найпоширенішим форматом сертифіката.

Abstract Syntax Notation One (ASN.1) — це стандарт, який описує правила та структури для представлення кодування, передачі та декодування даних у телекомунікаціях. Значення CMS генеруються за допомогою стандарту ASN.1 із базовими правилами кодування (BER-кодування). Значення представлено у вигляді рядків октетів (послідовність байтів).

Ще одна техніка CMS — від'єднання підпису повідомлення. Цей метод використовується S/MIME під час надсилання електронної пошти. Вбудовування підпису в повідомлення має як переваги, так і недоліки. Перевага полягає в тому, що для вбудовування підпису в повідомлення не потрібна підтримка з боку операційних систем або проксі-шлюзів, що дозволяє уникнути ненавмисного видалення. Основним недоліком є те, що вбудовування підпису в повідомлення змінює семантику повідомлення.

CMS також є основою для S/MIME, який використовує шифрування та підписання для забезпечення безпеки автентифікації, цілісності та незаперечення походження [18].

EdDSA. Алгоритм цифрового підпису кривої Едвардса — це схема цифрового підпису, яка використовує варіант підпису Шнорра та базується на скручених кривих Едвардса. Він розроблений, щоб перевершити продуктивність попередніх схем цифрового підпису. Має ряд переваг:

• Висока продуктивність з точки зору перевірки одним підписом (тобто порівняно менша кількість циклів процесора для даного рівня безпеки, ніж інші системи), пакетної перевірки (тобто паралельної обробки), підписання та генерації ключів;

• Високий рівень безпеки як функція циклів ЦП;

• Надійні ключі сеансу в тому сенсі, що випадковість використовується лише під час генерації ключа, а не тоді, коли ключ використовується для створення (або перевірки) підписів. Це робить систему менш вразливою до погано розроблених генераторів псевдовипадкових чисел;

• Стійкість до колізій у хеш-функціях – тобто алгоритм не порушується хеш-колізіями, що є результатом неправильного вибору хеш-функцій;

• Немає секретних індексів масиву – алгоритм не читає секретні адреси в оперативній пам’яті. Таким чином, система захищена від різноманітних атак із сторонніх каналів, які залежать від витоку інформації через кеш ЦП;

• Немає секретних умов розгалуження – аналогічно, алгоритм не виконує умовних розгалужень на основі секретних даних. Таким чином, система також захищена від атак зі сторонніх каналів, які залежать від витоку інформації через блок прогнозування розгалужень;

• Маленькі підписи та ключі щодо того, що записується в пам'ять; це відбувається тому, що зберігається стиснута версія довшого підпису або ключа, який за потреби розпаковується.

Розширені електронні підписи CMS. CMS Advanced Electronic Signatures (CAdES) — це набір розширень оригінальної CMS. CAdES розширює CMS, щоб забезпечити загальну основу для електронних підписів для використання в заявках на закупівлю, контрактах або рахунках-фактурах. CAdES визначає точні профілі підписаних даних CMS, тому Європейський регламент eIDAS (EU 910/2014) сумісний із CAdES (рис.2.4).

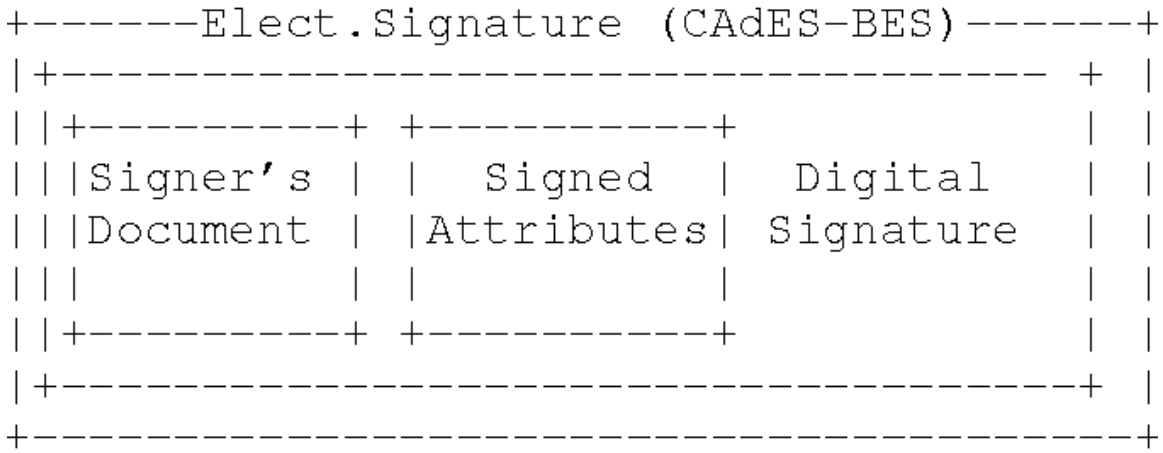

Рис.2.4. Формат електронного підпису з даними перевірки CAdES

Європейський регламент eIDAS — це регламент електронної ідентифікації та довірчих послуг для електронних транзакцій на внутрішньому ринку ЄС. З липня 2014 року він є юридично обов'язковим у всіх державах-членах ЄС, і якщо електронний підпис створено відповідно до eIDAS, тоді цей підпис має такий самий правовий статус, як і власноручний підпис.

Якщо електронний підпис реалізований на базі CAdES, то він має статус вдосконаленого електронного підпису, до якого пред'являються наступні вимоги:

• має унікальне посилання на підписанта;

• має можливість ідентифікувати підписанта;

• підписант є єдиним, хто контролює дані, які використовуються для створення підпису;

• можна визначити, чи були дані, додані до підпису, змінені після підписання.

Великою перевагою використання CAdES є те, що документ з електронним підписом може залишатися дійсним протягом тривалого часу. Якщо підписувач або перевіряюча сторона пізніше спробує спростувати дійсність підпису, CAdES можна використовувати для спростування цієї відмови.

Існує 3 різні eIDAS-сумісні реалізації вдосконалених електронних підписів через цифровий підпис: XAdES, PAdES і CAdES. Кожен має свою сферу застосування - в залежності від призначення[19].

PKCS #12. Стандарт криптографії з відкритим ключем (PKCS) №12 описує синтаксис передачі особистої ідентифікаційної інформації. Цей синтаксис можна використовувати для закритих ключів, сертифікатів, різних секретів і розширень(рис.2.5).

Програми, веб-браузери, комп'ютери тощо, які підтримують цей стандарт, створюють зручне середовище для імпорту, експорту та використання єдиного набору особистих даних. Це середовище надає переваги користувачам із різними ролями в компанії, оскільки вони можуть мати кілька цифрових ідентифікаторів – кожен із різним призначенням. В Adobe Sign кілька ідентифікаторів є важливим інструментом для багатьох компаній. Наприклад, працівник може виконувати адміністративні ролі, а також бути частиною проекту. Як інший приклад,

генеральний директор національної компанії має великий авторитет у цій конкретній компанії, але ця сама особа також може бути членом правління іншої міжнародної групи. Тому багатьом користувачам необхідно перемикатися між ролями, щоб відповідний ідентифікатор використовувався для підпису (для різних цілей) кожного типу повідомлення та/або документа. Ця техніка використання кількох ідентифікаторів, кожен з яких має певну роль, також може бути використана, навіть якщо користувач використовує різні методи сертифікації.

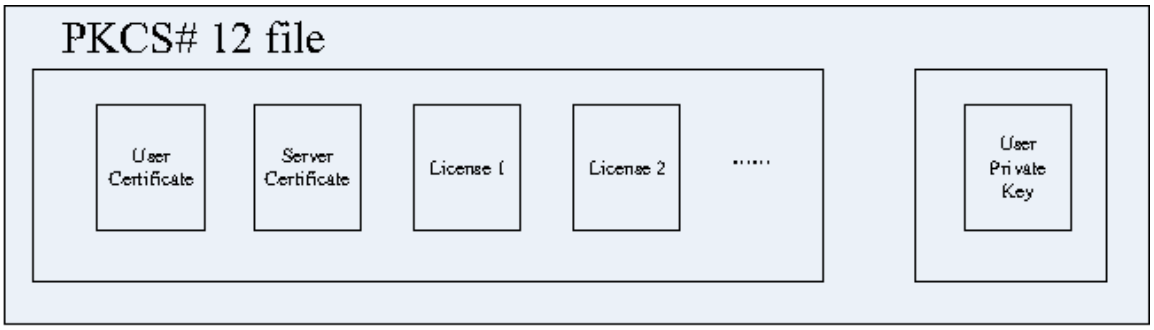

Рис.2.5. Структура файлу PKCS #12

PKCS #12 — це стандарт, який використовує кілька режимів конфіденційності та цілісності для безпосередньої передачі особистої інформації. Найбільш безпечний із цих режимів конфіденційності та цілісності вимагає, щоб вихідна та цільова платформи мали довірені пари відкритих/приватних ключів (щоб їх можна було використовувати для цифрових підписів і шифрування). Якщо надійні пари відкритих/приватних ключів недоступні, стандарт підтримує режими з низьким рівнем безпеки, наприклад режими конфіденційності та цілісності на основі пароля.

PKCS#12 може бути реалізований апаратно. Наприклад, деякі апаратні реалізації пропонують фізичну безпеку через стійкі до втручання маркери, такі як смарт-карти та пристрої Міжнародної асоціації карт пам’яті персональних комп’ютерів (PCMCIA) [20].

Спрощений протокол доступу до каталогу (LDAP). Це протокол для доступу до служб каталогу, зокрема до служб каталогу на основі X.500. LDAP — це стандартний протокол треку Internet Engineering Task Force (IETF), який описано в RFC 4511. LDAP використовує кодування ASN-1. Запити до каталогу можна

використовувати для доступу до інформації у загальнодоступному «Інтернеті» або в межах корпоративної «інтрамережі». LDAP є «полегшеною» версією протоколу доступу до каталогу (DAP), оскільки початкова версія LDAP не містила функцій безпеки. У каталозі записується, що та де розташовано, а також можливість доступу до атрибутів цих сутностей.

Система доменних імен (DNS) — це система каталогів, яка використовується для встановлення зв’язку між доменним іменем і адресами певних мережевих адрес (і навпаки). LDAP дозволяє користувачам шукати інформацію про осіб, не знаючи заздалегідь, де знаходяться відповідні записи, при цьому скорочується час пошуку. Каталог LDAP має структуру, подібну до ієрархії дерева (рис.2.6).

Каталоги LDAP можуть бути розподілені на кількох серверах. Перевага цього розповсюдження полягає в тому, що кожен сервер LDAP може мати репліку повного каталогу шляхом періодичної синхронізації з головною копією. LDAP використовує модель клієнт-сервер, де клієнти підключаються до серверів і роблять запити. Якщо сервер отримує запит від користувача, він за потреби передає запит на інший LDAP-сервер і забезпечить єдину скоординовану відповідь користувачеві.

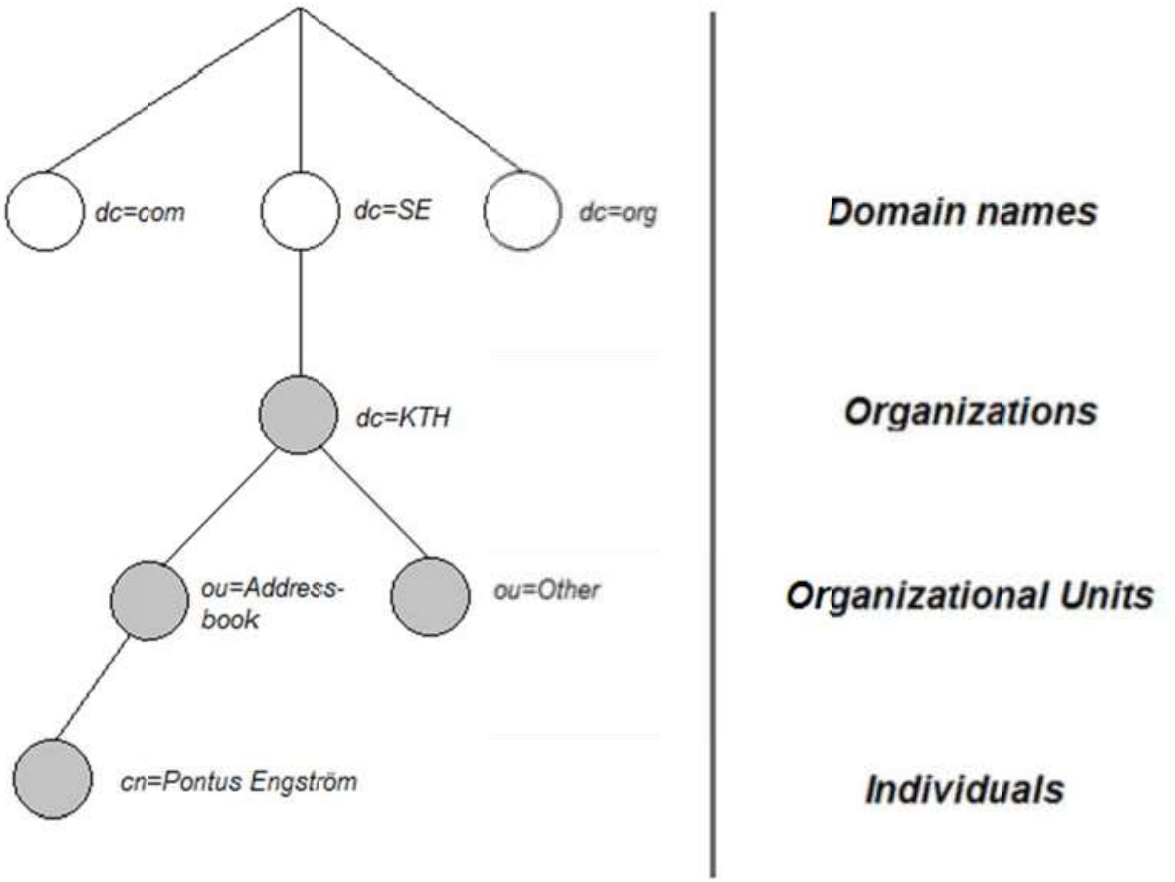

Рис.2.6. Дерево каталогів LDAP із використанням іменування на основі домену

Незалежно від того, до якого сервера LDAP підключається клієнт, усі вони можуть отримати доступ до записів у каталозі. Якщо ім’я представлено одному серверу LDAP, воно посилається на той самий запис іншого сервера LDAP. Ця функція важлива для глобальної служби каталогів. LDAP використовує спеціальний атрибут під назвою objectClass, який визначає, які атрибути є обов’язковими та дозволеними для запису. Значення атрибута objectClass визначають правила схеми, яким має підкорятися запис.

Схема. Схема — це тип документа, який описує та пов’язує атрибути та класи об’єктів. Щоб створити об’єкт певного класу, цей клас спочатку має бути визначений у схемі. Усі атрибути, які використовує об’єкт, мають бути визначені в схемі. Схеми записуються як звичайні документи, а потім перетворюються та вставляються до бази даних LDAP. Якщо сервер LDAP не може знайти реалізацію схеми, то класи об’єктів і атрибути, які описує схема, не використовуватимуться.

Тому дуже важливо, щоб кожен елемент у схемі ідентифікувався глобально унікальним ідентифікатором об’єкта (OID). Усі OID використовують ієрархічну структуру та організацію, яка використовує LDAP або X.500 може створювати скільки завгодно гілок від свого кореневого OID. OID — це деревоподібний ряд чисел, розділених крапками (.).

Атрибут. Атрибут зазвичай має унікальне ім'я, що містить деякі дані. Кожен атрибут є членом одного або кількох класів об’єктів. Атрибути можуть мати різні типи даних (синтаксис ключового слова), такі як рядки, цілі числа, логічні значення, двійкові тощо. Атрибути можуть бути частиною ієрархії, де дочірні атрибути успадковують усі характеристики батьківського атрибута. Ієрархія використовується для спрощення та скорочення атрибутів, коли багато атрибутів мають спільні властивості, напр. максимальна довжина та чутливість до регістру. Інший істотною властивістю є те, що атрибути можуть бути необов’язковими або обов’язковими.

Представлення атрибутів може бути здійснене як одним значенням, так і кількома значеннями. За визначенням, single означає, що буде присутнє лише одне значення даних, а multi означає, що атрибут може з’явитися кілька разів у записі/класі об’єкта, причому кожен екземпляр матиме різне значення. Прикладом одного значення може бути атрибут адреси електронної пошти, де значення може бути одним або декількома визначеннями атрибута, кожне з різною адресою електронної пошти. Кілька значень небажані для паролів, оскільки має прийматися лише одне значення.

Клас об'єктів. Класи об’єктів зазвичай є контейнерами для атрибутів, де кожен клас об’єктів має унікальне ім’я. Як згадувалося в розділі 2.7.2, об'єктний клас визначає, чи є властивість атрибутів необов'язковою чи обов'язковою. Тип об’єктних класів може бути СТРУКТУРНИМ, ДОПОМІЖНИМ або АБСТРАКТНИМ. Ключове слово STRUCTURAL вказує на те, що певний клас об’єктів містить атрибути та може формувати запис у інформаційному дереві каталогу (DIT). DIT — це система LDAP, структурована як ієрархія об’єктів. У кожному записі дозволено лише один СТРУКТУРНИЙ об’єктний клас, але він

може бути частиною ієрархії як SUP, де SUP зазвичай вказує, що об’єктний клас має батьківський (вищий) об’єктний клас. Клас об’єкта ABSTRACT вказує на неіснуючий об’єктний клас, який використовується для зручності, наприклад, верх об’єктного класу, який зазвичай закінчує ієрархію об’єктного класу. Останній об’єктний клас є ДОПОМІЖНИМ, який включає атрибути та може використовуватися з будь-яким СТРУКТУРНИМ об’єктним класом для формування запису (RFC 4512) [21].

PAdES. PDF Advanced Electronic Signatures (PAdES) — це набір обмежень і розширень до стандарту ISO 2008 PDF 1.7, що робить його придатним для розширених електронних підписів. Багато елементів, зазначених у документі, було включено до редакції PDF 2.0 ISO 2020.

У документації PAdES детально описано, як запровадити електронні підписи у форматі PDF, щоб вони відповідали вимогам eIDAS як для вдосконалених електронних підписів (AdES), так і для кваліфікованих електронних підписів (QES). Оскільки впровадження цих технологій потребує передових криптографічних інструментів, читачам пропонується вибрати криптографічні пакети відповідно до рекомендацій ETSI 119 312.

PAdES визначає діапазон різних атрибутів, які використовуються, щоб надати користувачам можливість вказати, як семантично обробляти їхні підписи. Ось деякі з найважливіших синтаксичних атрибутів

• content-type, який описує тип вмісту даних, що підписуються;

• дайджест повідомлення, дайджест (хеш) повідомлення - пропонує одержувачу спосіб перевірити цілісність даних;

• час підписання, який визначає час, коли підписувач (імовірно) виконав процес підписання;

• контрпідпис, який дозволяє користувачеві підписати комбіновані дані та підпис іншого користувача. Це дозволяє здійснювати різновид багатофакторної перевірки на рівні підпису. Його можна використовувати для перевірки підписів на корпоративному або розподіленому рівні.

Подальші специфікації детально описуються для так званого сховища безпеки документів (DSS). Воно містить додаткові дані, необхідні для перевірки підпису, необов'язково з інформацією, пов'язаною з перевіркою (VRI), яка пов'язує дані перевірки з конкретним підписом.

Введення цих розширень у формат дозволяє підтримувати довгострокову перевірку (LTV) підписів PDF. У документації PAdES визначено чотири рівні підпису. Вони впорядковані за підвищенням рівня безпеки:

• Рівень B-B містить вимоги щодо включення підписаних і деяких непідписаних атрибутів під час створення підпису;

• Рівень B-T містить вимоги щодо створення та включення до існуючого підпису довіреного токена, який доводить, що сам підпис фактично існував у певну дату та час;

• Рівень B-LT містить вимоги щодо включення в документ підпису всіх матеріалів, необхідних для підтвердження підпису. Цей рівень спрямований на довгострокову доступність матеріалу перевірки;

• Рівень B-LTA передбачає вимоги до включення електронних позначок часу, які дозволяють перевіряти підпис через тривалий час після його створення. Цей рівень спрямований на забезпечення довгострокової доступності та цілісності матеріалу перевірки.

Вони призначені для того, щоб запропонувати варіанти поводження з використанням життєвого циклу ключа. У документі містяться певні вказівки щодо цього, вказуючи, що найбільш безпечні параметри, PAdES-B-LT і PAdES-B-LTA, підходять, якщо необхідно зберегти технічну дійсність підпису протягом певного періоду часу після створення, враховуючи, що закінчення терміну дії сертифіката, відкликання та застарілість алгоритму можуть викликати занепокоєння[22].

2.3. Аналіз алгоритмів хешування

Хеш-алгоритми — це математичні функції, що відображають вхідні значення m на вихідні хеші h(m). Ці вихідні значення називаються хешами. Такі алгоритми

є життєво важливими для архітектури цифрових підписів. Щоб хеш-алгоритм вважався корисним, надійним і безпечним, необхідно виконати ряд властивостей. Найбільш важливими для використання з підписами є такі:

• Детермінізм. Враховуючи деяке вхідне повідомлення m, яке потрібно хешувати, алгоритм повинен завжди повертати той самий конкретний хеш h(m);

• Довільні вхідні значення. Функція має використовуватися для будь-якого довільного вхідного повідомлення, незалежно від його довжини;

• Вихідні дані однакової довжини. Усі хеші (вихідні значення алгоритму) повинні мати однакову довжину, незалежно від довжини та складу вхідних даних;

• Непередбачуваність результату. Вихід не повинен бути легко передбачуваним без фактичного виконання алгоритму хешування. Більш конкретно, алгоритм має відображати ефект лавини, який означає, що перевертання одного біта вхідного значення має перевертати непередбачуваний вибір – але в середньому половину – бітів у виході;

• Односторонній. Не повинно бути жодного легкого способу обчислення вхідного значення для певного вихідного хешу;

• Стійкість до зіткнень. Враховуючи відповідну довжину вихідних даних (хешів) і деяке повідомлення з відповідним хешем, буде важко знайти інше повідомлення з таким самим хешем. Крім того, геш-алгоритм повинен бути дуже стійким до зіткнень, що означає, що буде дуже важко знайти будь-які два входи m з однаковим хешем h(m). Бажана сильна стійкість до зіткнень через справжній «парадокс дня народження» статистики;

• Вибрана міцність безпеки. Алгоритм хешування має певним чином регулюватися – наприклад, кількість використовуваних внутрішніх ітераційних раундів, розмір блоків або розмір самого хешу – щоб користувач міг вибрати рівень безпеки (вимірюється в бітах), що відповідає їхнім потребам.

Алгоритм безпечного хешування. Алгоритми безпечного хешування SHA-0, SHA-1 і SHA-2 — це три алгоритми криптографічного хешування, опубліковані Національним інститутом стандартів і технологій США як стандарт безпечного

хешування. Вони використовують конструкцію Merkle-Damg˚ard як основу для стійкої до зіткнень криптографічної хеш-функції.

Функція Merkle-Damg˚ard приймає вхідні дані фіксованої довжини, що називається блоком. Ці безпечні алгоритми хешування використовують блоки довжиною 512 або 1024. Це означає, що довші повідомлення розділяються на блоки відповідного розміру. Якщо блок (як правило, останній блок у повідомленні) коротший за необхідну довжину, його доповнюють так, щоб досягти необхідної довжини. На рис.2.7 показано загальну структуру конструкції Меркла-Дамгарда.

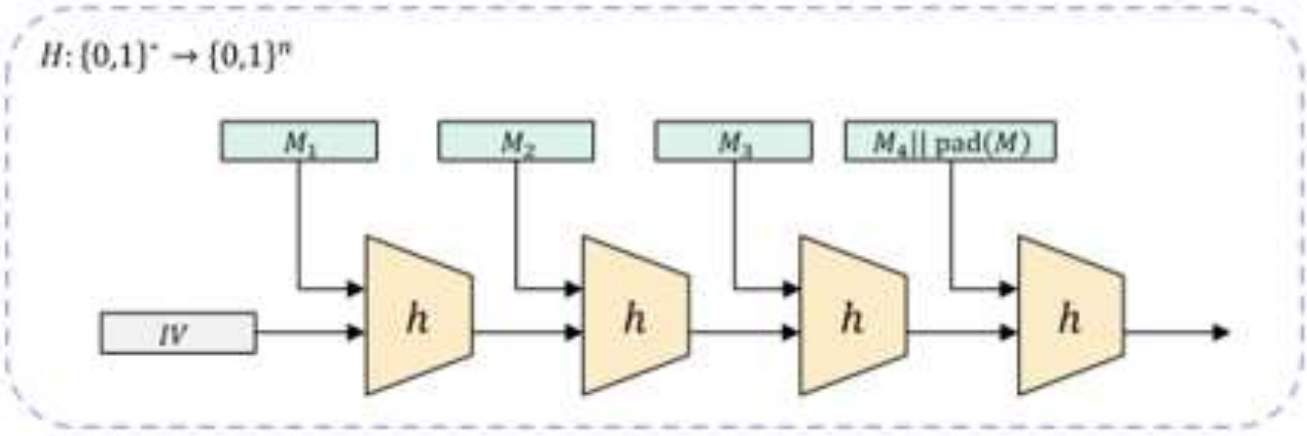

Рис.2.7. Зображення, що відображає загальну структуру конструкції Меркла-Дамгарда

Варто виокремити, що вектор ініціалізації (позначений як IV), використовується як блок введення зліва.

Блоки послідовно обробляються ітераційним кроком алгоритму. Це називається функцією стиснення. Він приймає два блоки введення і виводить лише один. Блоки, які використовуються як вхідні дані, — це ще необроблений «поточний» блок і вже оброблений «попередній» блок, тобто вихід функції стиснення на її попередньому кроці. Це детермінований процес, але з добре розробленою функцією стиснення він непередбачуваний [23].

Оскільки вихід функції стиснення потребує двох блоків як вхід, перша ітерація функції вимагає додаткового блоку, який називається вектором ініціалізації. Зазвичай це nonce – число, що використовується один раз. IV — це

бітовий потік такої ж довжини, як і блоки самого повідомлення, і вибір такого вектора також залежить від певних міркувань безпеки.

Перші два алгоритми безпечного хешування необхідно підтримувати лише з метою перевірки застарілого вмісту. Існують атаки, які дають трохи кращі результати, ніж груба сила проти SHA-2, але алгоритм все ще вважається безпечним для більшості цілей. Певні версії SHA-2 також вважаються вразливими до атак розширення довжини. Той факт, що вразливості були відомі для SHA-0 і SHA-1, які самі мають внутрішню структуру, подібну до SHA-2, спонукав бажання створити алгоритм хешування, принаймні настільки ж безпечний, як SHA-2, але з радикально відмінною внутрішня структура. Вважалося, що якщо один алгоритм буде зламаний, то на його місце повинен прийти інший. Тому NIST провів конкурс на розробку хеш-алгоритму, який буде прийнято як новий стандарт SHA-3.

Звичайно, були й інші міркування щодо вибору цього нового стандарту хеш-алгоритму. Фактори, перераховані NIST, були такими:

• Безпека:

– Широта застосування хеш-функції;

– Будь-які особливі вимоги до хеш-функції, коли вона використовується для підтримки коду автентифікації повідомлення з хеш-кодом, псевдовипадкових функцій або рандомізованого хешування;

– Додаткові вимоги до безпеки хеш-функцій;

– Оцінки щодо їх стійкості до атак;

– Інші фактори розгляду.

• Вартість і ефективність:

– Ефективність обчислення, яка стосується відносної швидкості та продуктивності алгоритму для заданої міцності безпеки;

– Вимоги до пам’яті, які включають розмір коду та вимоги до оперативної пам’яті для реалізації програмного забезпечення. Він також враховує кількість логічних елементів, необхідних для реалізації в апаратному забезпеченні;

• Алгоритм і характеристики реалізації. Це стосується таких якісних показників, як гнучкість і простота алгоритму кандидата. Це можна вважати більш

суб'єктивними показниками, ніж перелічені вище, але оцінку цих факторів все одно можна визначити шляхом громадського консенсусу.

– На гнучкість впливає здатність ефективно працювати на широкому діапазоні платформ, або можливість підтримувати паралельну обробку, або бути більш ефективним за допомогою простих розширень набору інструкцій;

– Простота алгоритму визначається міркуваннями про те, наскільки легко його зрозуміти й проаналізувати. Прості та зрозумілі дизайни вселяють більше довіри, що може підвищити рівень впровадження.

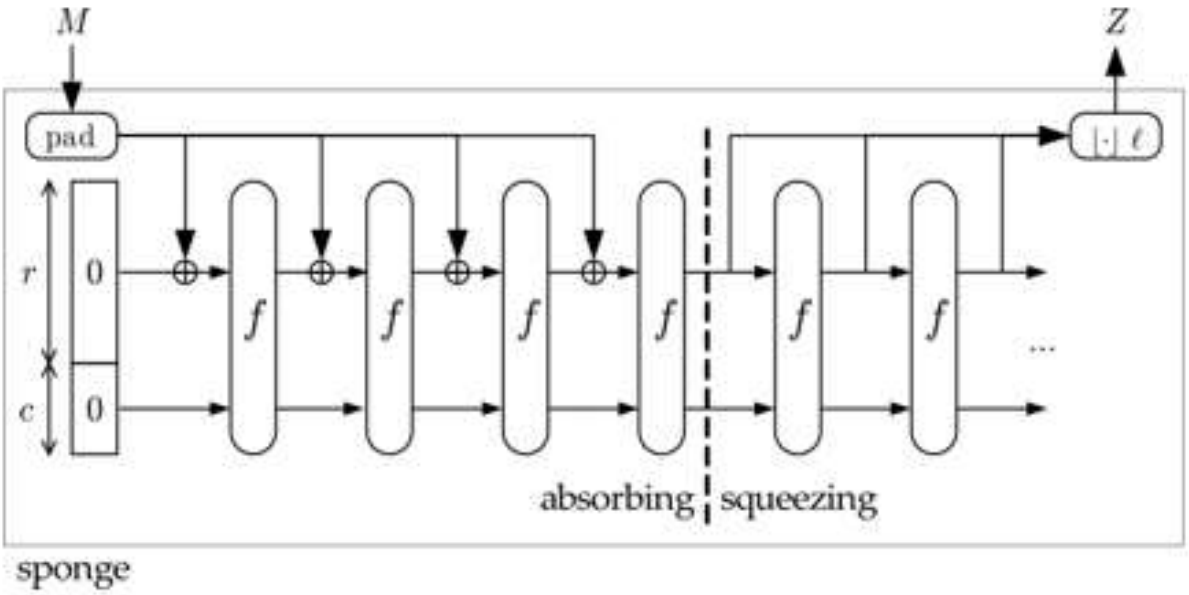

Рис.2.8. Конструкція губки SHA-3, яка обробляє вхідні дані будь-якої довжини у вихідні дані довжини, вибраної користувачем

Технічні характеристики алгоритму були опубліковані як FIPS 202. У той час як попередні ітерації SHA базувалися на конструкції Меркле-Дамгарда, SHA-3 натомість базується на конструкції губки (рис.2.8). Розробники називають конструкцію губки простим ітераційним процесом для побудови функції з довільною вхідною довжиною та фіксованою вихідною довжиною. Внутрішня функція - це перестановка вхідних бітів. Спочатку він запускається на етапі поглинання, де обробляються блоки повідомлення разом із доповненням[24].

Після обробки всього повідомлення алгоритм переходить до фази стискання, в якій він продовжує застосовувати функцію внутрішньої перестановки до

внутрішнього стану перед виведенням блоку. Як вихід можна вибрати довільну кількість блоків.

2.4. Особливості реалізації традиційних схем електронного підпису

Особливості реалізації традиційних схем електронного підпису включають:

- Невідмова. Завдяки унікальності закритого ключа (ключа підпису) відправник не може заперечити надсилання повідомлення, адже цей ключ є відомим тільки йому, і ніхто інший не може ним скористатися для підпису;
- Конфіденційність. Використання хеш-функцій та шифрування забезпечує захист від несанкціонованого доступу. Шифрування з використанням публічного ключа гарантує, що лише володар відповідного приватного ключа зможе розшифрувати та прочитати повідомлення;
- Цілісність. Цифровий підпис забезпечує перевірку того, що повідомлення не було змінено в процесі передачі. Якщо повідомлення буде змінено, то цифровий підпис не буде відповідати хешу повідомлення;
- Автентифікація. Використовуючи сертифікат відкритого ключа, одержувач може перевірити, що повідомлення дійсно надіслано автором. Це забезпечує впевненість в ідентичності відправника.

На рис.2.9 показано, як відправник генерує підпис, а потім надсилає і повідомлення, і підпис, і як одержувач перевіряє повідомлення та підпис шляхом порівняння двох хешів. Після обчислення хешу відправник шифрує цей хеш за допомогою свого закритого ключа, тому будь-хто може перевірити, що хеш розшифрованого повідомлення та хеш переданого повідомлення збігаються, таким чином гарантуючи, що повідомлення має не було змінено та що відправник є тим, за кого себе видає. Цей процес називається перевіркою підпису.

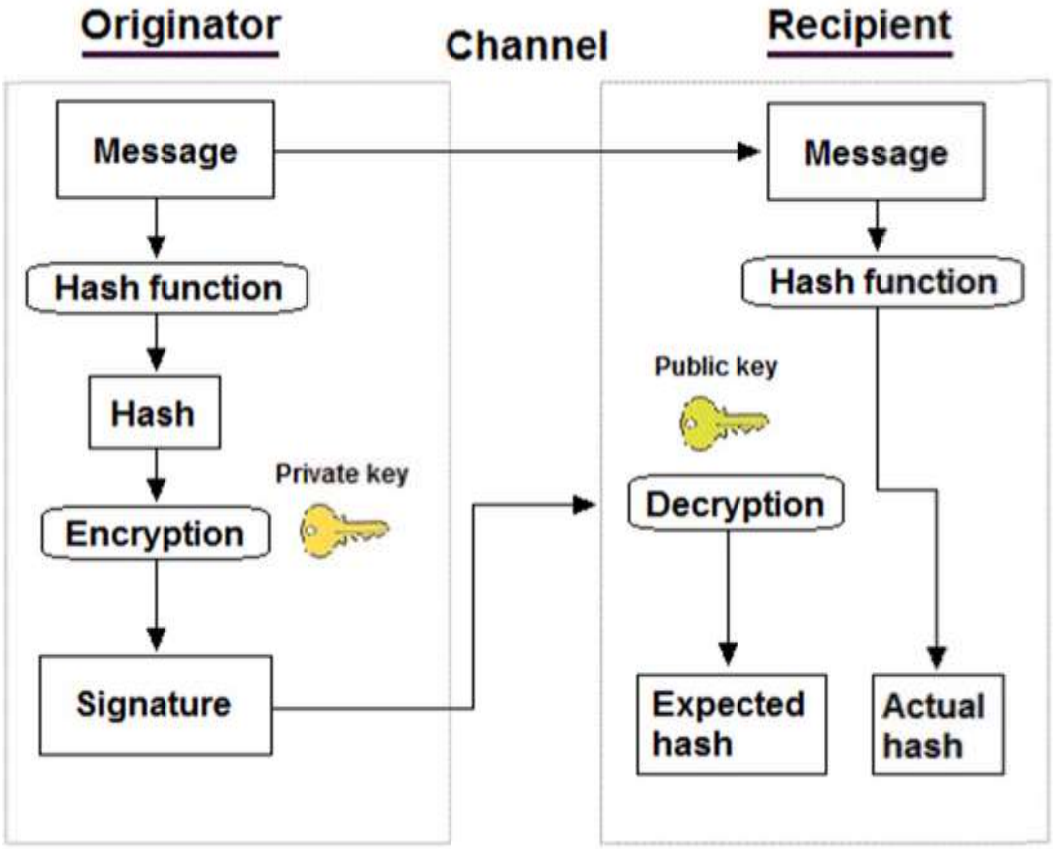

Рис.2.9. Генерація та перевірка цифрового підпису за допомогою хеш функції і пари ключів відправника

Схеми цифрового підпису складаються з таких основних елементів:

- Алгоритм генерації ключів - створює пару ключів (приватний та відкритий). Приватний ключ зберігається в таємниці, тоді як відкритий ключ розповсюджується серед потенційних одержувачів;
- Алгоритм підпису - приймає повідомлення та приватний ключ, генерує цифровий підпис, використовуючи хеш-функцію для створення дайджесту повідомлення, який потім шифрується за допомогою приватного ключа;
- Алгоритм перевірки - приймає повідомлення, відкритий ключ та цифровий підпис. Порівнює хеш повідомлення з розшифрованим хешем у цифровому підписі, щоб перевірити дійсність підпису.

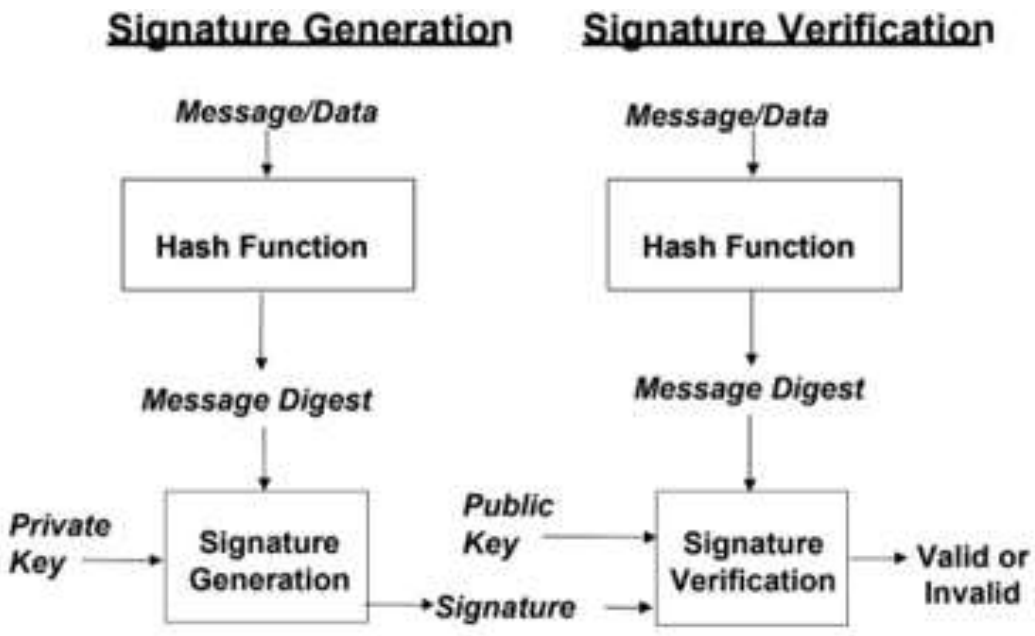

Рис.2.10. Пов’язані процеси підписання та перевірки підписів

На рис.2.10 демонструється взаємозв'язок між процесами підписання та перевірки. Зліва показано, як приватний ключ використовується для створення підпису з хешу повідомлення, а праворуч - як відкритий ключ використовується для перевірки цього підпису [25].

Висновки до другого розділу

Досліджено алгоритми та стандарти створення електронних цифрових підписів.

Зазначено, що цифрові системи є сучасними технологічними рішеннями проблем, з якими стикаються електронні підписи. Вони надають одержувачу криптографічні засоби для перевірки цілісності, а також забезпечують автентифікацію автора та даних, таким чином забезпечуючи більш сильну властивість неспростування.

Виокремлено особливості реалізації традиційних схем електронного підпису, що включають: невідмовність, конфіденційність, цілісність та автентифікацію. Проведено аналіз алгоритмів хешування.

3 МЕХАНІЗМИ ТА ЗАСОБИ БЕЗПЕЧНОЇ ІНТЕГРАЦІЇ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ У ДОКУМЕНТООБІГ ОРГАНІЗАЦІЇ

3.1 Використання цифрового підпису у PDF

Пакет Adobe Acrobat, розроблений компанією Adobe, являє собою комплексне рішення для роботи з PDF-документами. Цей пакет включає як безкоштовні, так і платні версії: Adobe Acrobat Reader DC для базового перегляду PDF-документів та Adobe Acrobat DC як преміум-опцію. Суфікс «DC» (Document Cloud) вказує на інтеграцію з хмарною інфраструктурою Adobe, запущеною в 2015 році, що розширює можливості роботи з документами.

Adobe Acrobat пропонує версії як у вигляді традиційних настільних програм, так і в онлайн-форматі через веб-інтерфейс Acrobat.com. Онлайн-версія забезпечує легкий доступ до документів через веб-браузери. Преміум-версії надають користувачам розширені інструменти для створення, редагування та управління PDF-файлами.

З точки зору безпеки, Adobe Acrobat включає функції для додавання, перевірки та перегляду цифрових підписів. Програма дозволяє користувачам використовувати електронні підписи в різних стилях, у тому числі з використанням видимих графічних підписів. Ці підписи можуть бути створені з використанням зображень, збережених на пристрої чи в інтернеті, або створені вручну за допомогою миші, графічного планшета чи сенсорного екрана. Базове криптографічне рішення використовує цифровий сертифікат інфраструктури відкритого ключа [26].

Функція «Запит електронних підписів» дозволяє запитувати підписи від інших користувачів. Преміум-користувачі отримують необмежену кількість використань цієї функції. Після введення інформації про підписантів, копія PDF-документа завантажується на сервери Adobe, а підписанти отримують посилання для підписання документа. Сервери Adobe зберігають детальну інформацію про

обставини підписання, включаючи особисті дані підписантів, дату та час доступу та підписання.

Adobe Acrobat Sign – це окрема, більш функціональна та дорожча послуга передплати, призначена головним чином для корпоративних користувачів. Ця послуга включає власні цифрові сертифікати та ширший спектр функцій, включаючи підтримку кваліфікованих часових позначок, зазначених в eIDAS, особливо для користувачів з ЄС.

PDF (Portable Document Format) є одним з найбільш широко використовуваних форматів у документообігу сучасних організацій. У форматі PDF інформація про цифрові підписи зберігається у спеціальному словнику підписів. Цей словник може містити як обов'язкові, так і необов'язкові елементи. Управління цими записами здійснюється спеціалізованим обробником підписів. Додаткові елементи можуть використовуватися або ігноруватися, проте розробникам рекомендується дотримуватися стандартних практик управління цими записами. Рекомендується, щоб імена приватних записів починалися з імені зареєстрованого обробника, після якого ставиться крапка (.), щоб уникнути конфліктів іменування.

Цифрові підписи у PDF генеруються шляхом обчислення хешу (дайджесту) вмісту документа, після чого цей хеш зберігається в документі. Для перевірки підпису та встановлення, чи не було документа змінено, здійснюється повторний розрахунок хешу та його порівняння з збереженим у документі. Розбіжність між розрахованим та збереженим хешами вказує на те, що документ було змінено після підписання.

Реалізація цифрових підписів у PDF підтримує використання асиметричної криптографії та інфраструктури відкритих ключів для перевірки автентичності підписувача та цілісності документа. Такі підписи, застосовані коректно, забезпечують надійність у підтвердженні автентичності та цілісності документа, що є критично важливим у сфері електронної комерції, наприклад, при використанні документів як рахунків-фактур. Захист цифрових документів від несанкціонованих змін запобігає потенційним шахрайським діям, таким як

перенаправлення фінансових платежів на неправильні рахунки. Таким чином, інтегровані функції безпеки PDF дозволяють пом'якшити певні загрози, пов'язані з цифровими документами.

Останні редакції стандарту PDF, зокрема ISO 32000-2, детально описують, як слід імплементувати цифрові підписи та відповідну підтримуючу інфраструктуру в документах PDF. Від процесорів PDF, що відповідають стандарту ISO 32000-2, очікується повна імплементація цих специфікацій.

Стандарт передбачає різні типи електронних підписів, включаючи біометричні підписи, такі як вбудовані зображення рукописних підписів, відбитки пальців або сканування сітківки ока. Крім того, він включає математичні конструкції, такі як цифрові підписи, засновані на асиметричному шифруванні. Важливу роль в автентифікації документів відіграє програмний компонент, відомий як обробник підпису, відповідальний за підписання та перевірку підписів. Процесори PDF повинні забезпечувати сумісність між різними обробниками підписів, так що підписи, створені за допомогою одного обробника, мають бути валідно перевірені іншими обробниками[27].

Стандарт PDF 2.0 також вимагає підтримки цифрових підписів на основі синтаксису криптографічного повідомлення (CMS) та стандартів CAdES (CMS Advanced Electronic Signatures). Він визначає чотири основні дії, пов'язані з електронними підписами в PDF:

- Додавання електронних підписів до документа;
- Перевірка електронних підписів у документі;
- Інтеграція словників цифрових підписів та інформації для перевірки;
- Включення словників часових міток для документів.

Стандарт також забезпечує відповідність загальноприйнятим стандартам безпеки інформації. CMS, як синтаксис криптографічного повідомлення, використовується для цифрового підпису, обробки, автентифікації або шифрування вмісту повідомлення. CMS описує інкапсуляційний синтаксис для захисту даних, підтримуючи цифрові підписи та шифрування. Цей синтаксис дозволяє вкладення інкапсуляцій одна в одну і підписання часових міток або інших

атрибутів разом із вмістом повідомлення. Таким чином, можна забезпечити додаткові заходи безпеки, такі як контрпідписи, пов'язані з основним підписом.

Інфраструктура відкритих ключів (Public Key Infrastructure, PKI) є комплексною системою, що включає в себе набір людських ресурсів, політик, електронної інфраструктури та програмного забезпечення, необхідних для ефективного використання шифрування на основі відкритих ключів. Це включає процеси створення, використання, зберігання, розповсюдження та відкликання цифрових сертифікатів.

PKI є фундаментальною для сучасних схем цифрового підпису. Процес генерації сертифіката включає прив'язку пари відкритого та закритого ключів до ідентифікаційної інформації, перевіреної постачальником довірчих послуг, який веде публічний реєстр для видачі та публікації сертифікатів. Статус відкликання сертифіката перевіряється через такі служби, як Список відкликаних сертифікатів (CRL) та Інтернет-протокол статусу сертифіката (OCSP).

CRL – це список, що містить часові мітки та ідентифікує відкликані сертифікати. Цей список підписується центром сертифікації або емітентом списку відкликаних сертифікатів та публікується для загального доступу. Для забезпечення конфіденційності інформації CRL завантажуються повністю.

OCSP – це протокол, який дозволяє отримувати інформацію про статус відкликання цифрових сертифікатів. OCSP надає більш актуальну інформацію, ніж CRL, та може включати додаткові дані про статус сертифікатів. OCSP вимагає менше пропускної здатності та забезпечує більшу конфіденційність, ніж перевірка через CRL. Якщо сертифікат відкликано, будь-які підписи, створені із використанням асоційованого закритого ключа, зазвичай вважаються недійсними, за винятком випадків, коли підписи мають криптографічно захищену часову мітку. Тоді лише підписи, створені після компрометації сертифіката, вважаються недійсними.

Таблиця 3.1

Записи в словнику підписів

Ключ	**Тип**	**Значення**
Фільтр	Ім’я	Назва бажаного підпису для використання під час перевірки підпису
Зміст	Рядок байтів	Значення підпису
Сертифікат	Масив або рядок байтів	Масив рядків байтів, що представляє використаний ланцюжок сертифікатів x.509 під час підписання та перевірки підписів, які використовують PKC, або рядок байтів, якщо ланцюжок має лише один запис
ByteRange	Array	Масив із парами цілих чисел, що описують фактичний діапазон байтів для обчислення дайджесту

У контексті PDF-файлів існують два основних підходи до обчислення відтворюваного дайджесту:

- Дайджест діапазону байтів - обчислюється для певного діапазону байтів у файлі, визначеного записом ByteRange. Зазвичай включає весь файл, включно із словником підписів, але без самого значення підпису (Зміст).
- Дайджест об’єктів - вибірково обчислюється для піддерева об’єктів у файлі, починаючи з кореневого об’єкта. Отриманий дайджест, разом з інформацією про процес його обчислення, розміщується у сигнатурному довідковому словнику., позначеному записом ByteRange (табл.3.1). Зазвичай цим діапазоном є весь файл, включаючи словник підписів, але за винятком самого значення підпису (Зміст). Якщо присутній дайджест діапазону байтів, значення словника підписів мають бути прямими об’єктами.
- Дайджест об’єктів - обчислюється шляхом вибіркового перегляду піддерева об’єктів у пам’яті. Починаючи з об’єкта, на який посилається, який зазвичай є кореневим об’єктом. Отриманий дайджест разом із іншою інформацією про те, як він був обчислений, поміщається в сигнатурний довідковий словник.

Таблиця 3.1 надає конкретний опис записів у словнику підписів PDF, коли виконується обчислення дайджесту діапазону байтів. Це включає деталі про варіації в записі «Зміст» в залежності від наявності атрибуту ByteRange.

Якщо ByteRange присутній, значення «Зміст» відображається як шістнадцяткове представлення дайджесту діапазону байтів. У випадку відсутності ByteRange, значення «Зміст» визначає дайджест словника підписів, окрім самого запису «Зміст». Зазвичай, значення «Зміст» представляє собою або PKCS#7 у форматі ASN.1 (DER) для відкритих ключів, або PKCS#1 у форматі DER для бінарних даних.

У записі «Сертифікат» перша частина масиву повинна містити сертифікати підпису та інші сертифікати, що використовуються для перевірки автентичності підпису. Вони можуть бути застосовані для перевірки значення підпису, що міститься у вмісті.

У випадках, коли використовується необов'язковий запис «Фільтр» зі значеннями adbe.pkcs7.detached або adbe.pkcs7.sha1, запис «Сертифікат» не використовується, і ланцюг сертифікації вставляється в PKCS#7 у «Зміст».

У записі ByteRange масив містить початкове зміщення та довжину байтів для кожного діапазону. Ці діапазони використовуються для обчислення дайджесту, який не включає сам підпис, що знаходиться у записі «Зміст».

У контексті власноручних підписів, як правило, необхідний надійний орган, наприклад нотаріус, для засвідчення підписання значущих документів. Нотаріус вважається довіреною особою, тому підпис, засвідчений ним, визнається дійсним в рамках ланцюга довіри. Аналогічно, у моделі цифрових підписів із використанням PKI, центр сертифікації виконує роль схожу до нотаріуса, засвідчуючи підпис та видаючи (і підписуючи) сертифікат [28].

Згідно з даними Adobe, наступні компоненти PKI безпосередньо пов’язані із забезпеченням довіри:

Таблиця 3.2

Компоненти PKI

Центр сертифікації (CA)	Центр, який продає/видає цифрові ідентифікатори. CA підписує власний сертифікат і зазвичай є кореневим сертифікатом у верхній частині ланцюжка сертифікатів.
Проміжні сертифікати (ICA)	Орган, який діє як посередник між кінцевим користувачем та кореневим сертифікатом. ICA надає такі послуги, як політика, мітки часу, списки відкликань тощо.
Сертифікат кінцевої сутності (EE)	Сертифікат користувача/підписувача, який є останнім елементом у ланцюжку сертифікатів.
Цифровий ідентифікатор	Це представлення ITU-T X.509 v.3 даних, які зазвичай пов’язані з особою чи організацією. Цей цифровий ідентифікатор зазвичай зберігається в безпечний спосіб, наприклад, захищений паролем файл на комп’ютері, смарт-карті, USB-накопичувачі тощо. Цей цифровий ідентифікатор містить сертифікат відкритого ключа, закритий ключ і деякі додаткові дані.
Сертифікат відкритого ключа	Сертифікат відкритого ключа включає частину відкритого ключа, пара відкритий/приватний ключ разом з атрибутами та пов’язаними розширеннями (наприклад, із зазначенням власника сертифіката, терміну дії та дозволеного використання).
Приватний ключ	Генерація ключа створює пару відкритого та закритого ключів. Секретний ключ використовується для перевірки вхідних повідомлень і підпису вихідних.

Інфраструктура відкритих ключів (Public Key Infrastructure, PKI) є ключовим компонентом для безпеки цифрових комунікацій і документообігу, включаючи роботу з PDF. PKI об'єднує різні елементи, включаючи адміністративні структури, політики, електронну інфраструктуру та програмне забезпечення, необхідні для створення, управління та розповсюдження цифрових ідентифікаторів. Це також

включає сервери LDAP, сервери часових позначок, списки відкликань сертифікатів, та інші компоненти, які забезпечують безпеку і надійність PKI.

Процес генерації ключів може відбуватися як на рівні користувача з подальшим підписанням відкритого ключа центром сертифікації (ЦС), так і здійснюватися довіреною стороною, яка генерує пару ключів і підписує сертифікат для відкритого ключа. При цьому, коли пара ключів і сертифікат зберігаються на смарт-картці, виробник смарт-картки може забезпечити їх попередньо згенерованими ключами і підписаним сертифікатом. Важливо звернути увагу на потенційний ризик, пов'язаний з можливістю виробника знати закритий ключ.

Цифровий ідентифікатор (Digital ID) є важливим елементом PKI, який асоціюється з особою або організацією і може бути порівняний з електронними документами, що підтверджують особу. Він містить таку інформацію, як особисте ім'я, електронна адреса, відомості про ЦС, що видало сертифікат, серійний номер, та терміни дії сертифіката. Цифровий ідентифікатор складається з пари ключів: відкритого ключа, який застосовується для шифрування даних, і закритого ключа для їх розшифрування. При підписанні PDF-файлу використовується закритий ключ, тоді як відкритий ключ інкорпорується в сертифікат, який розповсюджується іншим сторонам для перевірки підпису та особи підписувача. За замовчуванням, цифровий ідентифікатор зберігається у захищеному паролем файлі, що забезпечує безпеку закритого ключа, який є єдиним засобом для розблокування зашифрованої інформації.

В програмному забезпеченні Adobe Acrobat Reader DC користувачі мають змогу самостійно генерувати свій цифровий ідентифікатор або отримувати його від ЦС. В залежності від конкретного використання, кожен тип сертифіката має свої переваги. Наприклад, при самостійному створенні цифрового ідентифікатора в Adobe Acrobat, користувач генерує власний сертифікат з прив'язкою до відкритого ключа, що створений програмою, з подальшим самопідписанням цього сертифіката. Це особливо корисно у випадках, де сторони вже мають встановлені взаємні довірчі відносини.

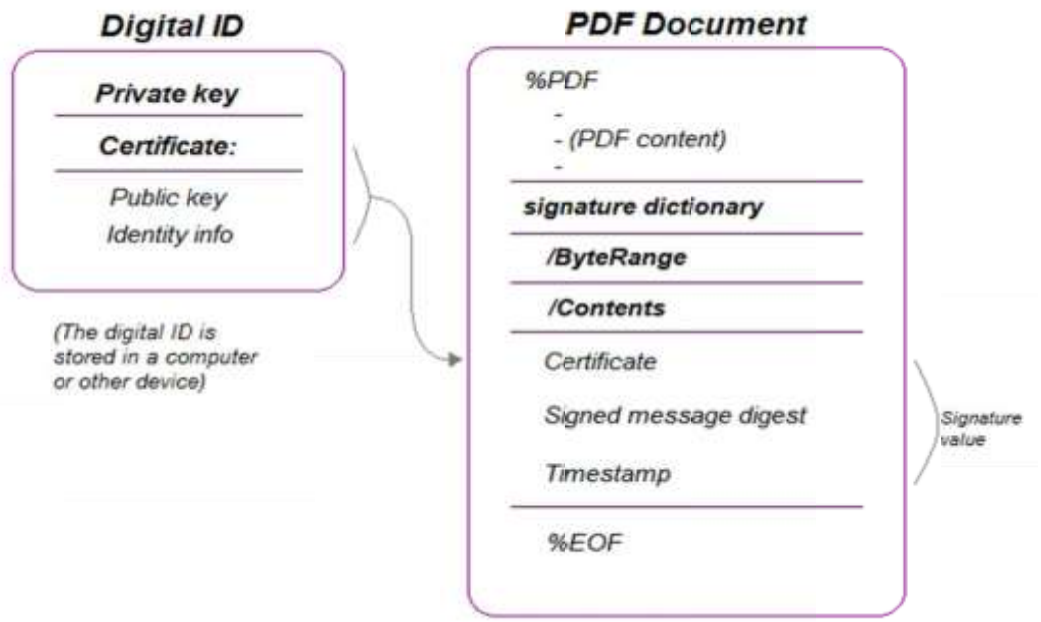

Рис.3.1. Цифровий ідентифікатор у підписаному PDF-документі

Цифровий підпис у форматі PDF. Формати файлів, відмінні від PDF, часто вимагають двох різних програм для обробки документа та його підпису, а також управління двома окремими файлами для кожного підписаного документа.

На відміну від цього, інтеграція підпису безпосередньо у PDF-документ дозволяє програмам для перегляду відтворювати документ для перегляду і одночасно перевіряти підпис[29].

Рис.3.2. Приклад цифрового підпису в Adobe Reader DC

PDF-документи можуть містити частини, підписані різними сторонами, що дозволяє вносити зміни в документ без анулювання підписів інших частин. Це особливо корисно в робочих процесах, де кілька людей повинні читати та підписувати документ.

Обробка та безпека цифрових підписів. Обробник підпису, вбудований в програмне забезпечення, таке як Adobe Acrobat, використовує технологію криптографії відкритого/приватного ключа (Public/Private Key, PPK), яка є формою асиметричної криптографії.

Словник підписів визначає обробника підпису, який буде використовуватися для обробки конкретного підпису. Процес підписання PDF-документа включає наступні кроки:

- Документ перетворюється на потік байтів.
- PDF-файл записується на диск із заздалегідь визначеним місцем для підпису в масиві ByteRange.
- Після обчислення підпису, місце, визначене для підпису, заповнюється актуальними даними.
- Хеш-значення обчислюється для байтів документа, визначених масивом ByteRange, з використанням алгоритму SHA-256.
- Хеш-значення шифрується особистим ключем підписувача, після чого генерується PKCS#7 у шістнадцятковому форматі.
- Об'єкт підпису розміщується у файлі PDF.

Перевірка підпису. Перевірка підпису включає порівняння розшифрованого хеш-значення із локально згенерованим хешем, використовуючи відкритий ключ підписувача з його сертифіката. Якщо вони співпадають, підпис вважається дійсним і засвідчує, що документ не був змінений з моменту підписання. Важливо розрізняти надійність підпису (яка залежить від конфігурації програми одержувача) та його дійсність (яка залежить від підпису ЦС на сертифікаті).

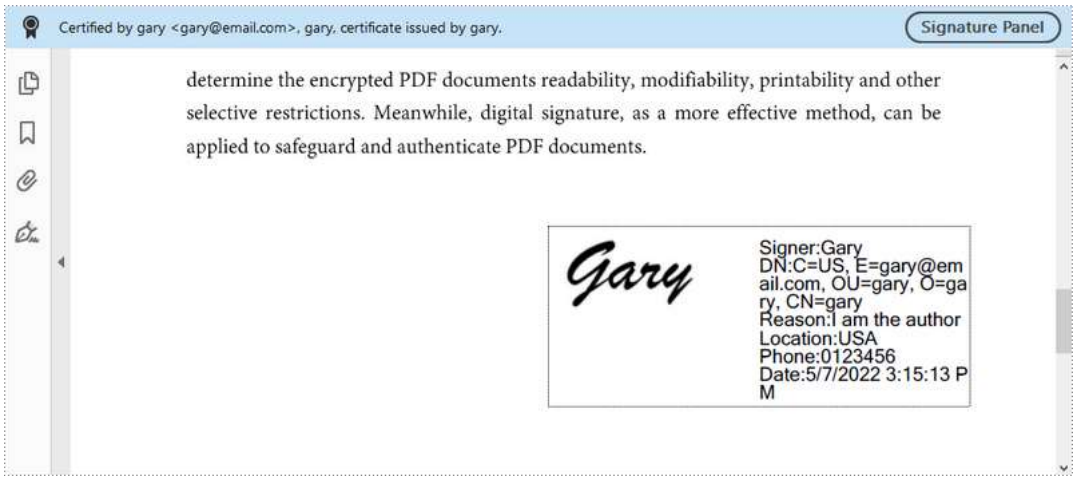

Рис.3.3. Приклад PDF-файл, до якого було додано два підписи через онлайн-функцію підпису Adobe

Програмне забезпечення Adobe підтримує програму Adobe Certified Document Services (CDS) з моменту її запуску в 2005 році. CDS дозволяє третім сторонам, переважно корпораціям, отримати статус довірених центрів сертифікації в рамках інфраструктури відкритих ключів Adobe. Згодом, Adobe ініціювала програму Adobe Approved Trust List (AATL), а CDS поступово виводиться з використання на користь AATL. Втім, сертифікати, зареєстровані через CDS, залишаються дійсними для перевірки старих підписів, а нові сертифікати реєструються через AATL.

Користувачі програм Adobe можуть налаштувати використання алгоритмів цифрових підписів. З 2017 року за замовчуванням використовується алгоритм SHA-256 для створення дайджестів документів. Також рекомендовано використовувати RSA-PSS з ключем мінімум 2048 біт для забезпечення безпеки підписів.

Хоча більшість розробок Adobe зосереджена в США і не вимагає публікації детальної документації про практики сертифікатів, на відміну від таких сертифікатів як BankID, Buypass чи Commfides, компанія все ж опублікувала коротку документацію з цих питань. Важливо, що Adobe дотримується належних практик безпеки, включаючи внутрішнє та зовнішнє тестування на проникнення, розвинуту автоматизацію безпеки, перевірки безпеки в коді, моделювання загроз

та класифікацію даних. Ці заходи знижують ризик вразливостей в програмному забезпеченні Adobe, що є ключовим, враховуючи широке розповсюдження їхніх продуктів і велику базу користувачів[30].

3.2. Використання цифрового підпису у Microsoft Office

Пакет програмного забезпечення Microsoft Office включає комплекс інструментів для створення текстових документів, електронних таблиць та презентацій, підтримуючи зберігання у різноманітних форматах файлів, включно з експортом у формат Portable Document Format (PDF). З 2007 року, пакет Office використовує формат файлу XML для зберігання даних, де кожен документ Office (наприклад, .docx, .xlsx, .pptx) є стиснутим архівом XML-файлів, що розпаковується при завантаженні в пам'ять комп'ютера.

Особливо важливо для безпеки є те, що пакет Office підтримує цифровий підпис документів. Ці підписи інтегровані як окремі файли у спеціальну папку «xmlsignatures» в структурі XML-архіву. Це забезпечує додатковий рівень захисту, оскільки підписи можна перевірити на автентичність.

Користувачі можуть підписувати лише цілі документи, а не окремі їхні розділи. Автор документа має можливість підготувати документ так, щоб дозволити кільком користувачам підписувати один і той же документ, при цьому підписи зберігаються окремо і не впливають на валідність інших підписів.

Щодо вибору між видимими та невидимими електронними підписами, користувачі можуть додавати невидимі підписи безпосередньо до документа. Для створення видимого підпису спочатку в документ вставляється рядок підпису, а потім користувач додає зображення свого власноручного підпису у вказане місце.

Обидва типи електронних підписів криптографічно захищені за допомогою цифрового підпису, який використовує приватний ключ цифрового сертифіката, обраного користувачем. Цей підхід забезпечує високий рівень безпеки, оскільки сертифікати та приватні ключі є основою для перевірки автентичності та цілісності підписів. Інтерфейс для вибору та управління цифровими сертифікатами є

інтуїтивно зрозумілим і забезпечує легке управління цифровими підписами у документах Office.

Рис.3.4. Вибір цифрового сертифікату в Microsoft Office

Корпорація Microsoft розпоряджається власною інфраструктурою відкритих ключів, проте не займається видачею цифрових сертифікатів для кінцевих користувачів. Їх інфраструктура переважно використовується для сертифікації програмного забезпечення. Користувачі, які прагнуть додати цифровий підпис до своїх документів або програм, мають звертатися до зовнішніх, акредитованих центрів сертифікації, або генерувати власний цифровий сертифікат.

У контексті безпеки та захисту документів, пакет програмного забезпечення Microsoft Office включає можливість додавання електронних підписів до документів. При додаванні цифрового підпису до документа, він автоматично переходить у режим лише для читання, що запобігає ненавмисному або несанкціонованому редагуванню. Якщо підпис видаляється, документ втрачає свій захист і повертається до режиму редагування.

Інтерфейс Microsoft Office сповіщає користувачів про наявність цифрового підпису в документі, відображаючи горизонтальні банери, які повідомляють, що документ позначено як остаточний та містить підпис. Приклад такого документа в Microsoft Word можна побачити на рис.3.5.

Рис.3.5. Приклад підписаного документа в Microsoft Word

Користувачі мають можливість переглянути всі підписи у документі за допомогою окремого режиму перегляду підписів, доступного через інтерфейс. Цей режим надає детальну інформацію про кожен підпис, забезпечуючи додатковий рівень прозорості та безпеки.

Що стосується вразливостей у програмному забезпеченні Microsoft Office, база даних CVE Details фіксує численні випадки. Втім, виявлені вразливості зазвичай швидко усуваються через систематичні оновлення програмного забезпечення. Велика кількість виявлених вразливостей не обов'язково свідчить про слабкість програмного забезпечення; це часто відображає широку базу користувачів та інтенсивність використання продуктів Microsoft.

Корпорація Microsoft також дотримується високих стандартів безпеки в своїх об'єктах, включаючи заходи фізичного та цифрового контролю доступу, захист від стихійних лих, відповідність галузевим стандартам та державним регуляціям. Ці заходи гарантують високий рівень безпеки для розробки та підтримки їхнього програмного забезпечення.

Відносно підтримки хеш-алгоритмів та алгоритмів цифрового підпису, Microsoft Office надає широкий спектр опцій для забезпечення цифрової безпеки. Користувачі можуть вибирати серед різних алгоритмів та розмірів ключів, що надає гнучкість та адаптацію до різних сценаріїв безпеки. Ці параметри конфігурації дозволяють користувачам налаштовувати рівень захисту відповідно до їхніх конкретних потреб.

Криптографічні методи, які лежать в основі цифрових підписів, базуються на складних математичних операціях, виконуваних над цифровими даними. Ці операції, хоча й є фундаментальними на рівні примітивів, часто видаються віддаленими від повсякденного досвіду звичайних користувачів. Люди, як правило, сприймають і взаємодіють з технологіями на більш високому рівні абстракції, ніж тому, що представлено на рівні бітів та байтів.

Ця відстань між фундаментальними криптографічними операціями та їхнім сприйняттям та використанням у повсякденному житті аналогічна способу, яким людський мозок абстрагує складні фізичні процеси. Наприклад, ми не замислюємося над окремими вібраціями молекул повітря, коли сприймаємо звук; натомість ми фокусуємося на більш високому рівні абстракції, такому як музика або мова.

В контексті криптографічних застосунків, це означає, що важливо забезпечити, щоб кінцеві користувачі мали доступ до інтуїтивно зрозумілих інтерфейсів, які приховують складність підставних криптографічних операцій. Такі інтерфейси дозволяють користувачам безпечно використовувати цифрові підписи, не заглиблюючись у технічні деталі процесу.

Крім того, безпека цифрових підписів залежить не лише від математичних алгоритмів, а й від способів їх реалізації та інтеграції у програмне забезпечення та системи. Це включає заходи для захисту від зловмисного програмного забезпечення, злому, інших видів кібератак, а також від помилок в реалізації, які можуть призвести до уразливостей. Використання надійних криптографічних бібліотек та постійне оновлення програмного забезпечення для виправлення

виявлених вразливостей є ключовими елементами для забезпечення безпеки цифрових підписів на практиці[31].

3.3. Використання цифрового підпису у BankID

Система BankID в Україні є державною системою віддаленої ідентифікації, розробленою Національним банком України. Ця система дозволяє громадянам легко і безпечно отримувати доступ до різноманітних онлайн послуг. Серед таких послуг - адміністративні (державні), фінансові, комерційні та інші. Для користування системою необхідно мати відкритий рахунок у банку, який є учасником системи, та доступ до мобільного або інтернет-банкінгу цього банку.

Електронна дистанційна ідентифікація в системі BankID НБУ відбувається шляхом передачі персональних даних від банку (абонента ідентифікатора), де відкрито рахунок користувача, до абонента надавача послуг. Цей процес ініціюється власником персональних даних, і передача інформації відбувається в зашифрованому вигляді.

За станом на другий квартал 2023 року, система налічує 127 учасників, серед яких 39 банків-ідентифікаторів та 88 абонентів — надавачів послуг. У цьому кварталі система зазнала збільшення числа учасників, включаючи небанківські фінансові установи та різноманітні комунальні та комерційні організації.

Наразі 99,9% власників платіжних карток в Україні можуть отримати доступ до широкого спектру дистанційних послуг завдяки системі BankID НБУ, що свідчить про її широке поширення і популярність[32].

Сервіс використовується як фактор автентифікації користувача, і він доступний як для особистих, так і для професійних цілей. Для особистого користування він використовується для підтвердження особи під час входу в банк, а також для низки публічних цифрових сервісів. Після початкової процедури входу він також використовується для будь-яких наступних перевірок автентифікації. Такі додаткові перевірки є звичайними для здійснення фінансових переказів, доступу до конфіденційної інформації в державних архівах та для електронного

підпису документів. На рис.3.6 показано, як виглядає процедура входу до системи BankID.

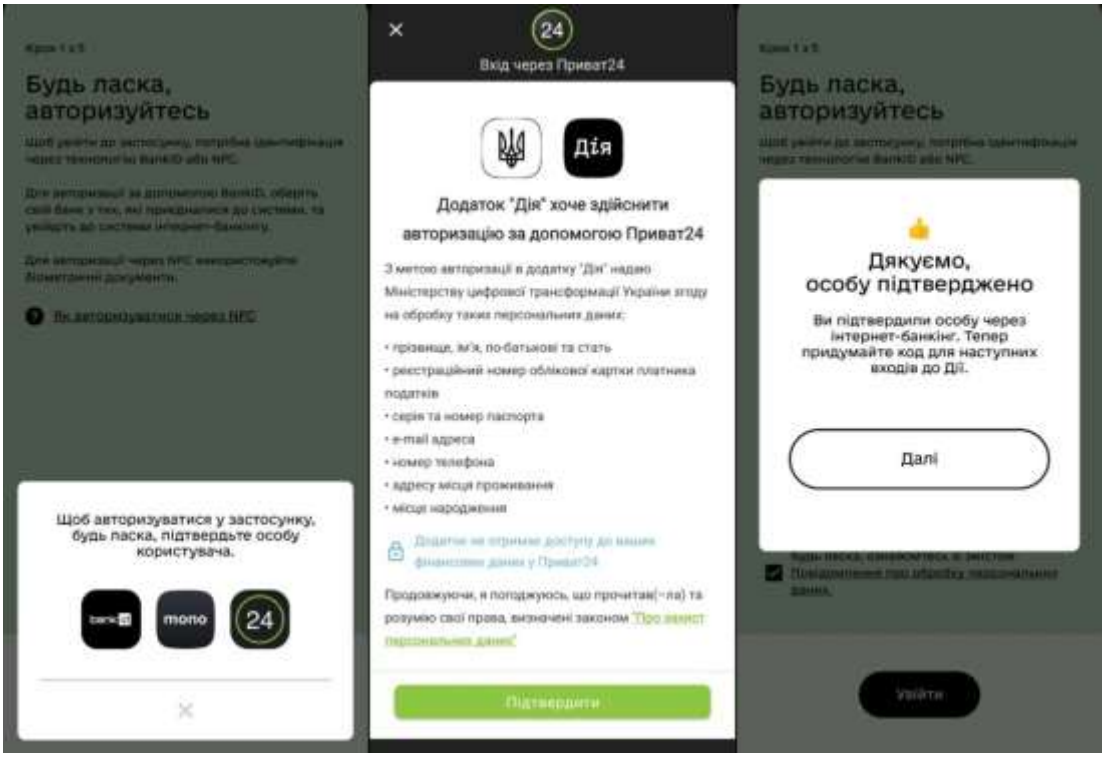

Рис.3.6. Процедура входу в BankID

Окрема програма «Дія» надає користувачеві просту підказку. Якщо користувач натискає кнопку, щоб підтвердити, що він справді є користувачем, який входить у систему, йому потрібно буде ввести свій пароль – той самий, який використовується для кодової мікросхеми.

Існує також опція біометричного розпізнавання обличчя або сканування відбитків пальців, які все ще знаходяться в стадії розробки. У самій програмі BankID ця функція наразі доступна для певних користувачів. Однак деякі банки впровадили такі функції незалежно для всіх своїх користувачів у своїх власних запатентованих програмах. Приклад - використовувати системи Face ID від Apple у своїх програмах. Це використовує власне програмне забезпечення безпеки Apple для розпізнавання обличчя[33].

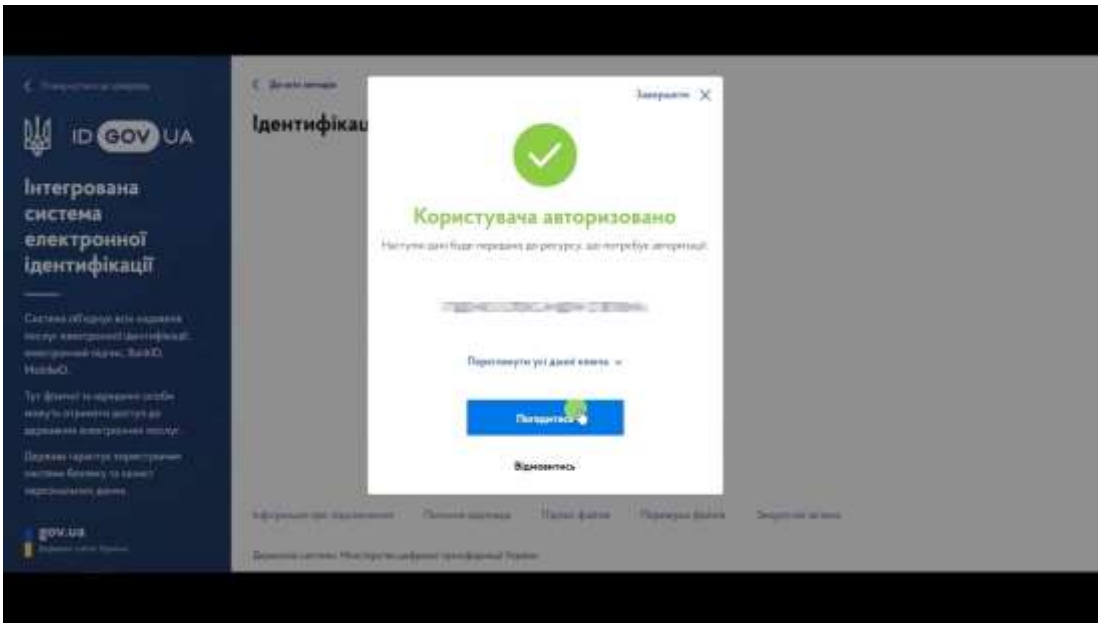

Рис.3.7. Приклад успішної авторизація з використанням BankID

Сервіси BankID використовують RSA як обраний алгоритм підпису. RSA зазвичай вважається повільним, але він безпечний для достатньо великих розмірів ключів і рекомендований для використання з цифровими підписами NSA, NIST та ENISA. Розмір ключа принаймні 2048 біт є загальною рекомендацією для використання з RSA вже майже десять років.

Кореневий центр сертифікації інфраструктури відкритих ключів, керованої АЦСК, використовує 4096-бітні ключі. Його основна роль у системі – підписувати ключі для реєструючих органів, банків. Самі банки видають своїм кінцевим користувачам сертифікати та ключі. Сертифікати рівня RA та сертифікати кінцевого користувача (як для особистої, так і для службової версії служби) генеруються з розміром ключа 2048 біт.

Використання автентифікації BankID для доступу до систем цифрового підпису є простою справою для більшості користувачів; вони, як правило, вже мають досвід використання послуг BankID для входу в свої системи онлайн-банкінгу. Таким чином, показники зручності використання, ймовірно, будуть досить хорошими для більшості користувачів.

Рис.3.8. Результати діяльності системи BankID НБУ (3 квартал 2023 року)

Впровадження автентифікації BankID в існуючі системи може бути дещо складним. У BankID є бібліотеки та API, які можна впровадити безпосередньо в існуючу електронну архітектуру. Проте у BankID є партнери, готові надати всі ці види послуг. Загалом існує широка підтримка впровадження послуг BankID.

Сервіси підпису, доступні через партнерів BankID, мають форму низки архітектурних підходів, які будуть знайомі багатьом користувачам. Існують портали підписання, доступні через браузери, а також є програми для мобільних і настільних операційних систем. Усе це може надати користувачам доступ за допомогою послуг BankID. Отримавши доступ, користувачі можуть підписувати власні документи, а також можуть надсилати документи іншим користувачам для підписання.

Це свідчить про те, що BankID пропонує хорошу зручність використання. Пристрої легко освоїти, і вони достатньо ефективні для частих користувачів, хоча слід зазначити, що впровадження біометрії в сервіси може зробити їх ефективнішими. Вони також настільки прості, що не потребують запам’ятовування багатьох деталей про системи. Користувачі загалом знайомі з концепцією автентифікації, тому системи зрозумілі. Показники задоволеності важко оцінити, і

їх було б легше зібрати за допомогою більш експериментального підходу, заснованого на опитуванні, але системи BankID, здається, задовольняють потреби своїх користувачів.

Сервіси BankID загалом здаються хорошим вирішенням проблеми впровадження інфраструктури цифрового підпису; вони забезпечують хорошу безпеку та досить зручність використання[33].

3.4 Порівняння показників безпеки використання цифрових підписів у досліджених рішеннях

На основі критеріїв оцінки та попередньої аргументації властивостей зручності використання та безпеки кожного продукту підсумовано наступну оцінку:

BankID. Послуги BankID відповідають високим стандартам безпеки, використовуючи фортеці-клас шифрування та аутентифікаційні протоколи. Однак, оскільки зловмисники часто цілять на кінцевих користувачів, важливо використовувати надійні паролі та уникати підозрілих посилань чи запитів. Також рекомендується регулярно оновлювати програмне забезпечення та використовувати двофакторну аутентифікацію для додаткового рівня захисту.

Adobe Acrobat. Adobe Acrobat використовує передові методи шифрування для захисту PDF-документів, включаючи захист паролем та цифрові підписи. Для забезпечення найвищого рівня безпеки, важливо регулярно оновлювати програмне забезпечення, щоб враховувати найсвіжіші виправлення вразливостей. Користувачам також слід бути обережними при відкритті PDF-файлів з невідомих джерел, оскільки вони можуть містити шкідливі скрипти або вразливості.

Microsoft Office. Microsoft Office забезпечує різні рівні безпеки, включаючи захист від вірусів та шкідливого програмного забезпечення через інтеграцію з Microsoft Defender та іншими антивірусними рішеннями. Регулярні оновлення програмного забезпечення є ключовими для підтримки безпеки, особливо з огляду на поширеність Microsoft Office як цілі для кібератак. Крім того, використання

цифрових підписів в Microsoft Office вимагає налаштувань безпеки та можливо залучення сертифікованих центрів сертифікації для забезпечення правильного управління ключами.

Висновки до третього розділу

Досліджено механізми та засоби безпечної інтеграції електронних цифрових підписів у документообігу організації. Зазначено, що Adobe Acrobat використовує передові методи шифрування для захисту PDF-документів, включаючи захист паролем та цифрові підписи.

Виокремлено поняття інфраструктури відкритих ключів (Public Key Infrastructure, PKI), що є комплексною системою та включає в себе набір людських ресурсів, політик, електронної інфраструктури та програмного забезпечення, необхідних для ефективного використання шифрування на основі відкритих ключів.

Досліджено особливості програмного забезпечення Microsoft Office, що включає комплекс інструментів що підтримує цифровий підпис документів. Зазначено, що використання цифрових підписів в Microsoft Office вимагає налаштувань безпеки та можливо залучення сертифікованих центрів сертифікації для забезпечення правильного управління ключами.

Досліджено систему BankID в Україні, що є державною системою віддаленої ідентифікації, розробленою Національним банком України. Сервіси та послуги BankID відповідають високим стандартам безпеки, використовуючи протоколи шифрування та аутентифікації.

4 ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЇ ШЛЯХОМ ВПРОВАДЖЕННЮ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ В ДОКУМЕНТООБІГ

4.1 Викоремлення критеріїв користувачів

Звичайний домашній користувач. Враховуючи потреби звичайного домашнього користувача у сфері цифрового підпису, важливо адаптувати послуги до їхніх специфічних вимог щодо зручності та безпеки.

Зручність використання. Звичайні домашні користувачі зазвичай не мають великих вимог до ефективності цифрових підписів, оцінюючи їх більше за доступність і простоту використання. Вони можуть бути задоволені послугами, що пропонуються такими сервісами, як Поштова служба, з недорогою оплатою за підпис та мінімальними технічними вимогами. Інтерфейс таких послуг зазвичай зрозумілий і веде користувача крок за кроком, що зменшує ризик плутанини або помилок.

Безпека. Для звичайного користувача важлива базова безпека, що забезпечує певний ступінь неспростування, без необхідності використання особистих цифрових сертифікатів. Важливо, щоб користувачі були освічені щодо потенційних фішингових атак та інших форм шахрайства, особливо при отриманні допомоги від сторонніх осіб.

У менш формальних випадках, де юридичні ризики низькі, користувачі можуть вибрати більш традиційні форми автентифікації, наприклад, перевірку особистості через електронний лист від відомого відправника або телефонний дзвінок.

Такий підхід дозволяє домашнім користувачам ефективно використовувати цифрові підписи з урахуванням їхніх специфічних потреб та технічної компетентності, при цьому забезпечуючи необхідний рівень безпеки та зручності.

Малий бізнес. Для малого бізнесу, критерії використання цифрових підписів та сертифікатів варіюються в залежності від їхніх конкретних потреб, типу бізнесу, та вимог їхніх ділових партнерів.

Технічні вимоги та цифрові сертифікати. Малому бізнесу може знадобитися використання власних цифрових сертифікатів для забезпечення більшої автентичності та цілісності документів. Такі сертифікати можуть бути сформовані внутрішньо і поділені з довіреними діловими партнерами, які встановлять їх у своїй бібліотеці довірених сертифікатів.

Вибір програмного забезпечення. Малі підприємства можуть використовувати загальнодоступні програми, такі як Microsoft Office або PDF-процесори (наприклад, Adobe Acrobat або Foxit Reader), для додавання цифрових підписів до PDF-документів. Це забезпечує відповідність юридичним вимогам щодо безпеки, включаючи цілісність документа, автентифікацію підписувача та неспростовність.

Обмін з широким колом партнерів. Якщо малий бізнес має широкий коло ділових партнерів або велику клієнтську базу, може виникнути потреба використовувати цифрові сертифікати, сертифіковані зовнішніми, акредитованими центрами сертифікації. Такий підхід, характерний для великих корпорацій, дозволяє забезпечити вищий рівень довіри та сумісності з різноманітними сторонами.

Заходи безпеки. Малі підприємства повинні активно впроваджувати політики кібербезпеки для захисту їхніх ділових даних, включаючи цифрові підписи.

Важливо регулярно оновлювати програмне забезпечення та системи безпеки, а також забезпечувати, щоб усі співробітники були обізнані щодо потенційних кіберзагроз і методів їх запобігання.

Таким чином, малий бізнес може оптимізувати використання цифрових підписів, враховуючи їх конкретні потреби та рівень взаємодії з діловими партнерами та клієнтами, при цьому забезпечуючи необхідний рівень безпеки та автентичності

Великі корпорації та державні установи. Для великих корпорацій та державних установ, вибір та управління рішеннями для цифрового підпису вимагає особливого підходу, з огляду на їхній масштаб, різноманітність операцій та значну кількість співробітників та клієнтів.

Ефективність і зусилля. Великі корпорації часто зосереджені на підвищенні ефективності робочих процесів, оцінюючи це з точки зору часу та витрачених зусиль. Вони можуть виправдати вищі витрати на передові послуги цифрового підпису через економію часу та ресурсів у довгостроковій перспективі.

Інфраструктура відкритих ключів та центри сертифікації. Створення власної інфраструктури відкритих ключів з широко довіреним кореневим центром сертифікації може бути оптимальним рішенням для великих корпорацій з множинністю внутрішніх та зовнішніх співробітників та партнерів.

Альтернативно, платити акредитованому центру сертифікації за перевірку та управління цифровими сертифікатами може бути практичним вибором, особливо для організацій, що не мають ресурсів для розвитку власної інфраструктури.

Індивідуальні цифрові сертифікати. Великим корпораціям часто потрібні індивідуальні цифрові сертифікати для кожного співробітника, особливо для тих, хто активно залучений у процеси підпису.

Вибір платформи для підпису. Корпорації можуть використовувати такі рішення, як Adobe Acrobat Sign або інші комерційні портали для підписання (наприклад, BankID, Postal Service, Buypass,), в залежності від їхніх конкретних потреб та критеріїв ефективності.

Заходи безпеки. Великі корпорації повинні активно впроваджувати комплексні стратегії кібербезпеки для захисту своїх цифрових підписів та пов'язаних з ними даних. Регулярні оновлення та моніторинг безпеки є ключовими для запобігання шахрайству та іншим кіберзагрозам.

Таким чином, для великих корпорацій та державних установ, вибір та управління рішеннями для цифрового підпису вимагає балансу між ефективністю, масштабованістю та безпекою, враховуючи їхні унікальні вимоги та складність операцій [34].

4.2 Отримання кваліфікованого електронного підпису (КЕП)

КЕП можна отримати у структурах, що надають електронні довірчі послуги, або в акредитованих центрах сертифікації ключів (АЦСК). Фізичні особи мають можливість отримати КЕП безкоштовно через банківський сервіс, наприклад, «Приват24» від Приватбанку.

Деякі банки пропонують цю послугу лише для юридичних осіб або за плату. АЦСК «Центр сертифікації ключів України» надає послугу створення КЕП на платній основі (рис.4.1). Перелік всіх структур, що надають КЕП, доступний на офіційному сайті Міністерства цифрової трансформації України.

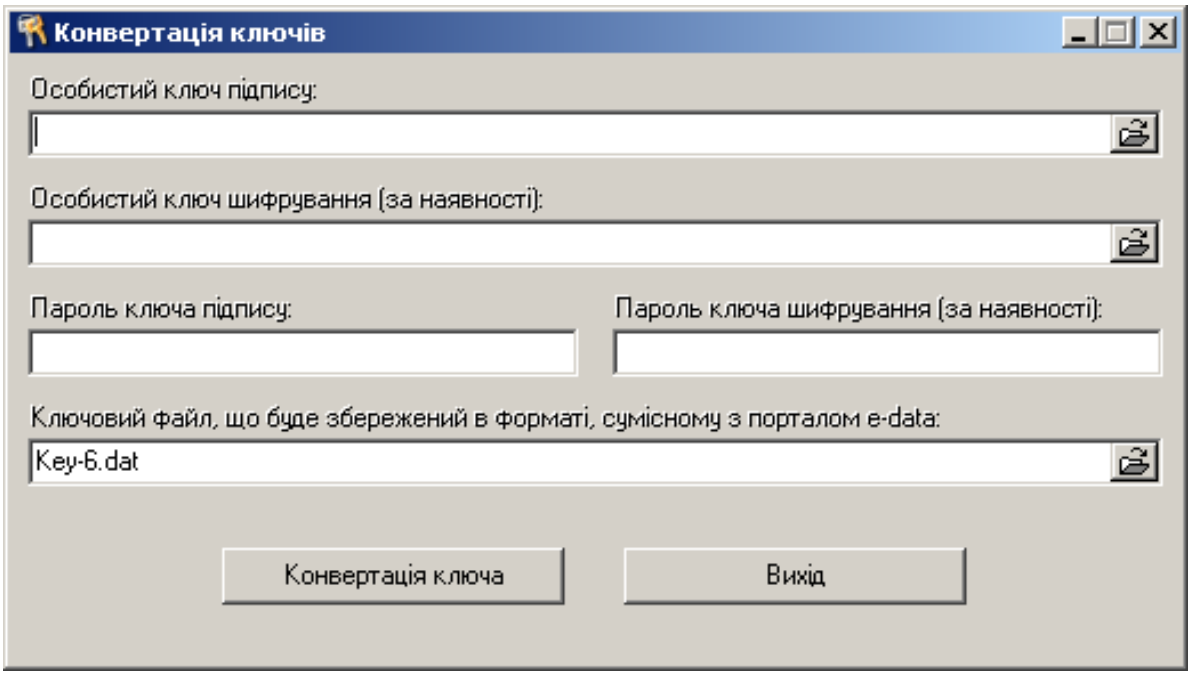

Рис.4.1. Конвертація ключів за допомогою АЦСК «Центр сертифікації ключів України»

Отримання ЕЦП у Приватбанку. Приватбанк надає послугу створення електронного цифрового підпису (ЕЦП) безкоштовно для своїх клієнтів. Для цього необхідно зайти в розділ «Бізнес» у головному меню «Приват24» і вибрати відповідну опцію для фізичних осіб. Процес включає етапи верифікації та створення пароля для доступу до хмарного сховища ЕЦП. Після створення підпису файл ключа у форматі *.jks під назвою «pb_ІПН фізособи» автоматично

завантажиться на пристрій. Користувач також отримає електронний лист із підтвердженням випуску кваліфікованого електронного підпису на його ім'я.

Отримання ЕЦП в ДПС. Інформаційно-довідковий департамент Державної податкової служби (ДПС) надає послуги з випуску ЕЦП. Для отримання підпису необхідно заповнити реєстраційні заяви та зібрати відповідні документи, форми та зразки яких доступні на офіційному сайті ДПС. З усіма документами потрібно звернутися до представника кваліфікованого постачальника електронних довірчих послуг. Центральний засвідчувальний орган Мінцифри також має Довірчий список кваліфікованих постачальників електронних довірчих послуг.

Отримання ЕЦП через «Дію». ЕЦП можна згенерувати через мобільний додаток «Дія», доступний на Android та iOS. Для цього необхідно авторизуватися в застосунку, у меню вибрати «Дія.Підпис» та використовуючи фронтальну камеру підтвердити особу (рис.4.2.). Після успішної верифікації слід створити пароль із п'яти цифр, після чого підпис буде сформовано і доступний у тому самому розділі меню «Дія.Підпис»[35].

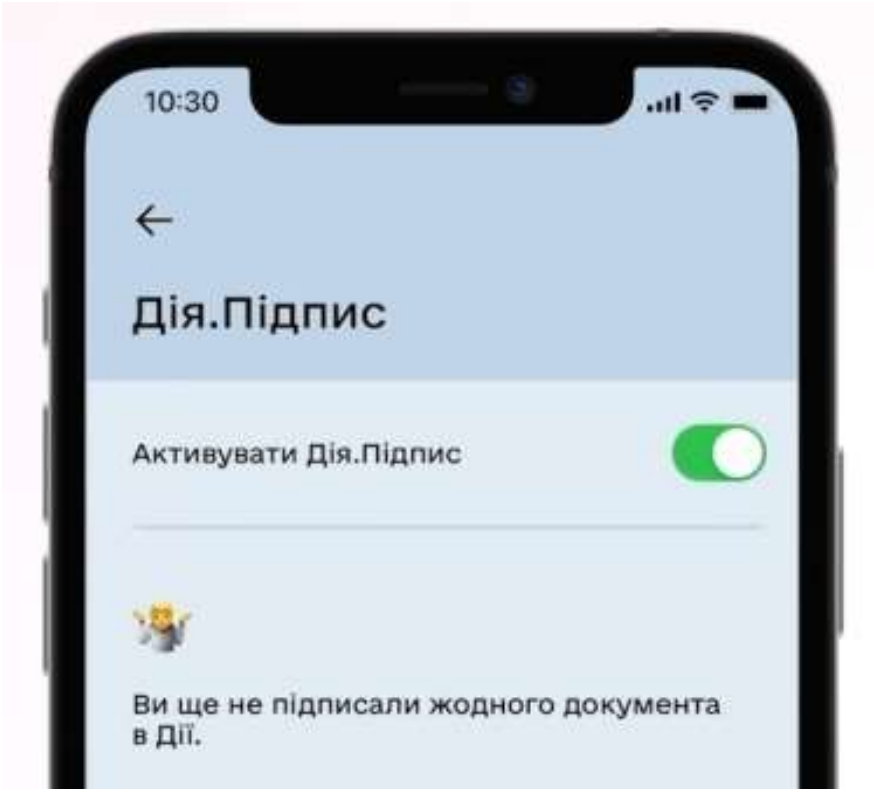

Рис.4.2. Активація віддаленого КЕП через «Дія.Підпис»

4.3. Алгоритм генерації ключів в АЦСК «Центр сертифікації ключів України»

Крок 1. Для генерації особистого ключа необхідно обрати підпункт «Згенерувати ключі» в пункті меню «Особистий ключ» (рис.4.3).

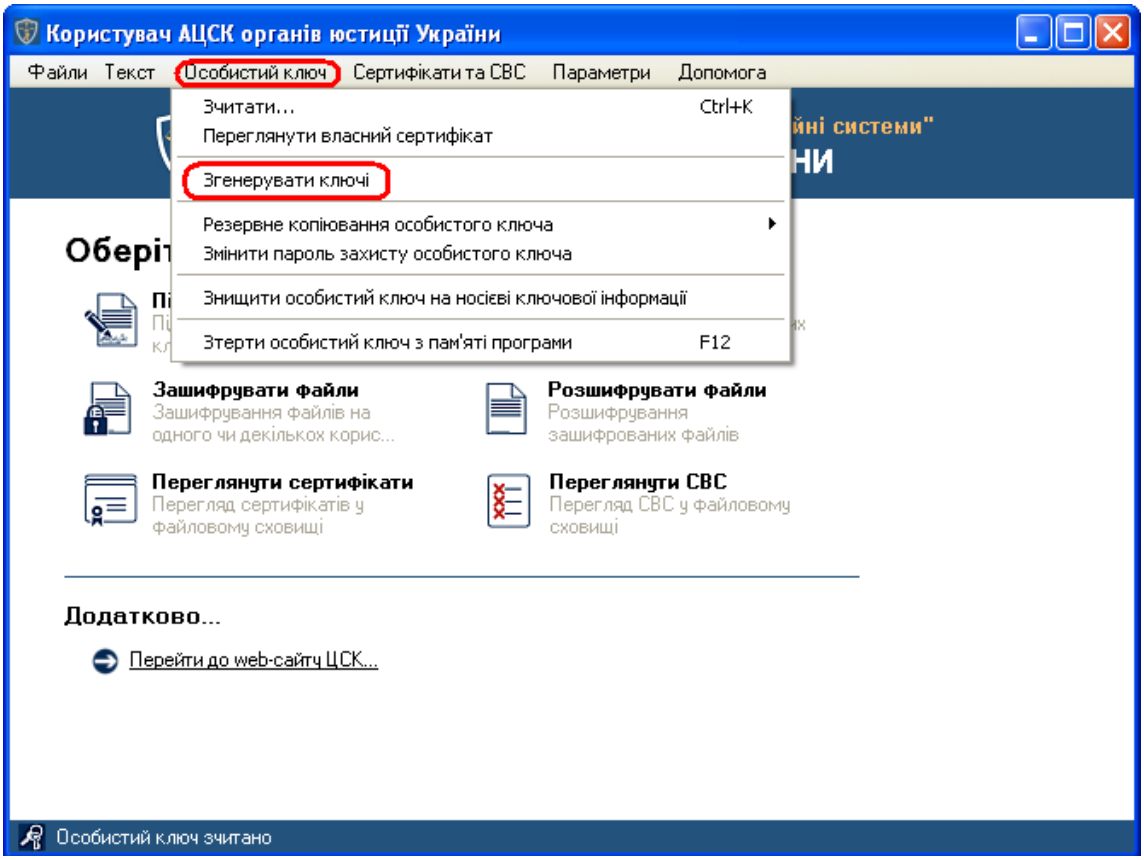

Рис.4.3. Приклад генерації особистого ключа в АЦСК

Крок 2. У вікні генерації ключів необхідно встановити параметр «Використовувати окремий ключ для протоколу розподілу», при цьому буде згенеровано дві ключові пари, одна з яких буде використовуватись для підписання даних, а друга (ключ протоколу розподілу) буде використовуватись для шифрування даних.

Крок 3. Для продовження генерації ключа необхідно натиснути кнопку «Далі» (рис.4.4.).

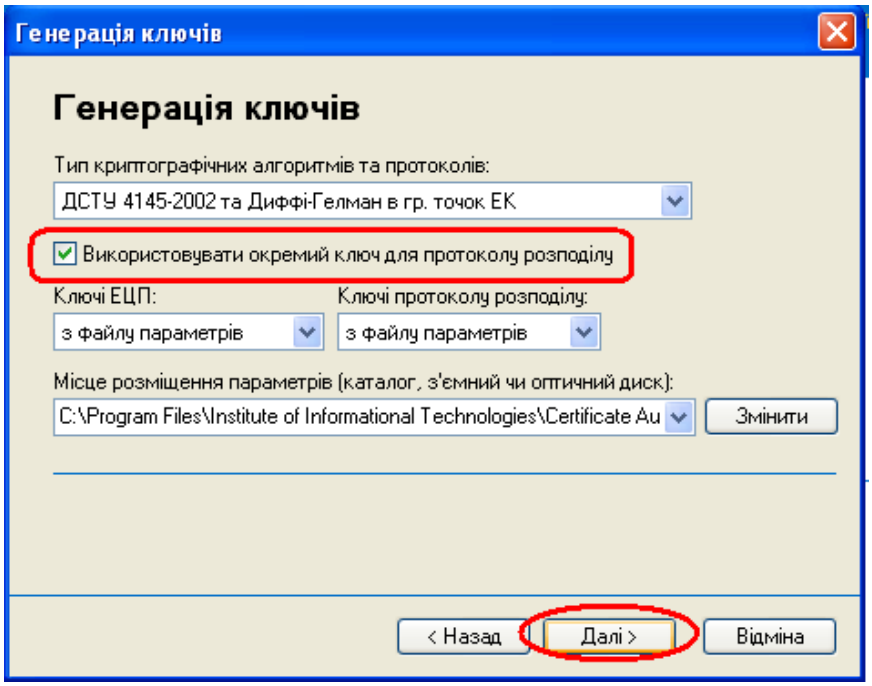

Рис.4.4. Приклад налаштування окремого ключа для протоколу розподілу

Крок 4. Після появи вікна запису особистого ключа, необхідно обрати з'ємний носій, на який буде записано особистий ключ, ввести пароль захисту до нього та натиснути кнопку «Записати» (рис.4.5).

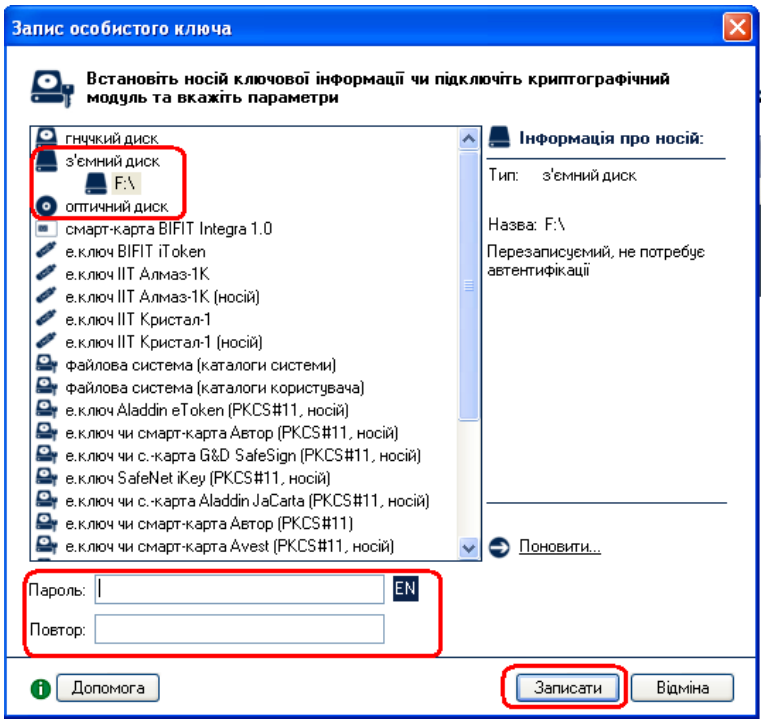

Рис.4.5. Вибір з'ємного носія

Обидва особистих ключа (для підпису та шифрування) будуть записані у вигляді одного файлу особистого ключа – Key-6.dat.

Крок 5. Після запису особистого ключа на з'ємний носій буде виведено вміст запиту на формування сертифіката з відкритим ключем ЕЦП та запиту на формування сертифіката з відкритим ключем протоколу розподілу. Для продовження генерації необхідно натиснути «ОК» (рис.4.6).

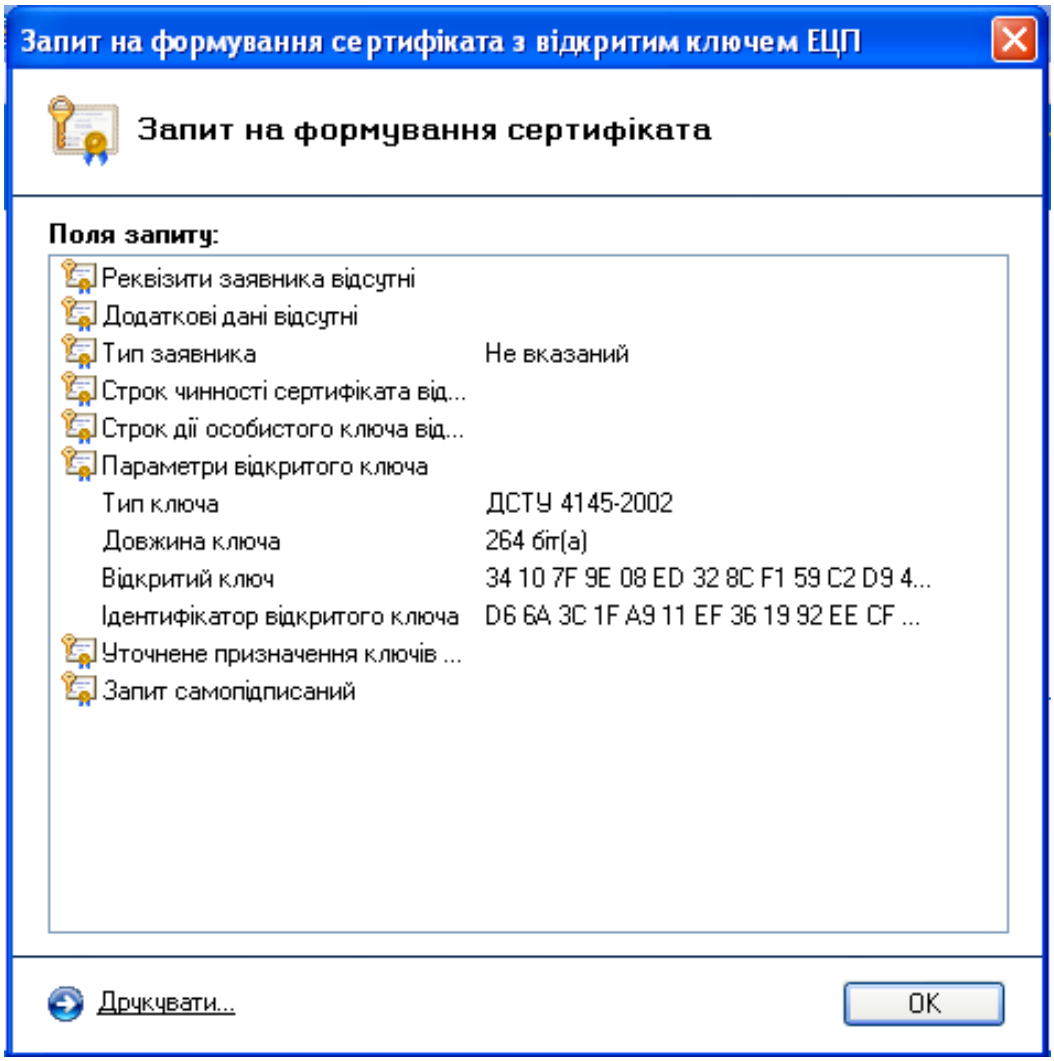

Рис.4.6. Крок продовження генерації ключів

Крок 6. Для передачі запитів на формування посилених сертифікатів до АЦСК необхідно зберегти їх у файл (рис.4.7). Для цього необхідно встановити параметр «Зберегти у файл» та натиснути кнопку «Далі».

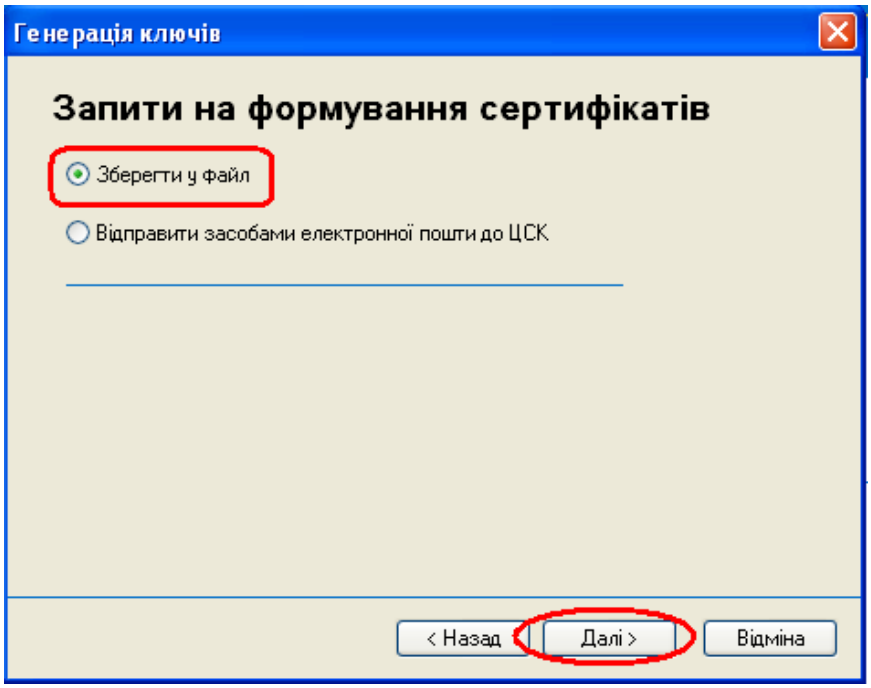

Рис.4.7. Крок збереження файлів

Крок 7. Запити повинні бути записані на носій інформації чи на жорсткий диск. Для цього необхідно натиснути кнопку «Змінити» (рис.4.8) та вказати необхідний носій інформації та ім’я запитів на формування сертифікатів у файл.

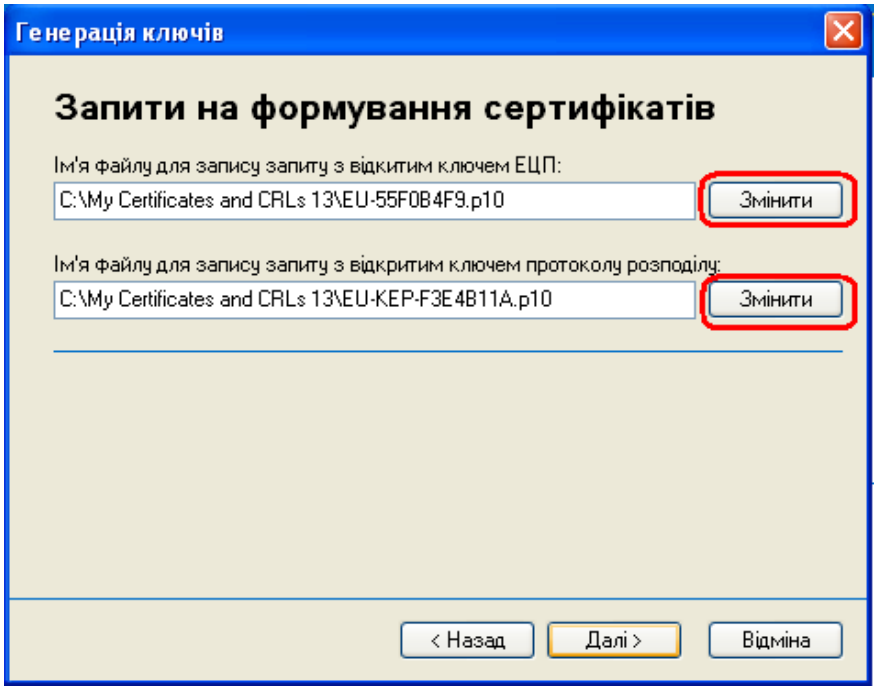

Рис.4.8. Приклад внесення змін щодо носіїв інформації та імені запитів

Для коректної ідентифікації запитів з відкритим ключем ЕЦП та протоколом розподілу користувача файл запиту на формування сертифіката повинен обов'язково зберігатись з ім'ям у наступному форматі:

«EU-XXXXXXXX-Прізвище.p10» та «EU-KEP-XXXXXXXX-Прізвище.p10», де: Прізвище – прізвище підписувача; EU-XXXXXXXX.p10 та EU-KEP-XXXXXXXX.p10 – унікальне ім'я файлу запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад: EU-69PH0S9W-Іванов.p10; EU-KEP-KB50S67Z-Іванов.p10 [36].

Крок 8. Для завершення генерації необхідно натиснути кнопку «Завершити» (рис.4.9).

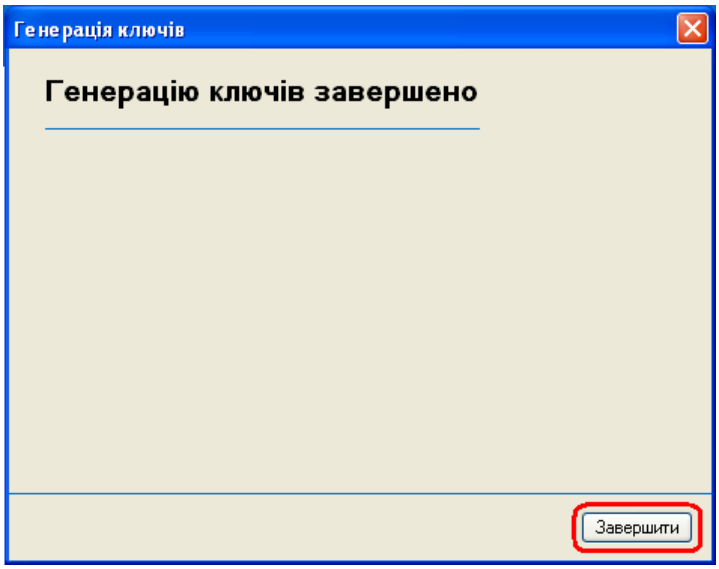

Рис.4.9. Завершення генерації ключів

Крок 9. Після цього, запити разом з комплектом реєстраційних документів можуть бути передані до пункту реєстрації користувачів АЦСК для формування посилених сертифікатів.

4.4 Використання мобільного додатку eSign для генерації цифрового підпису

Крок 1. Доступ до додатку можна отримати в Play Market. Для цього необхідно внести в пошуковому рядку «eSign».

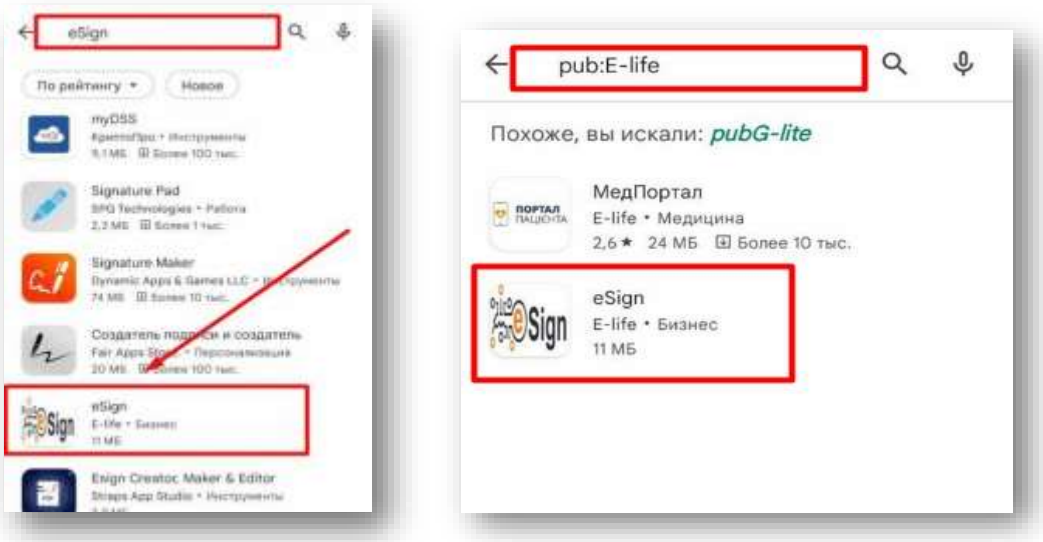

Рис.4.10. Завантаження додатку eSign

Крок 2. Після завантаження мобільного додатку eSign, необхідно авторизуватися. Логін – це фактичний номер телефону. Пароль – це пароль від КЕП. Після успішної авторизації

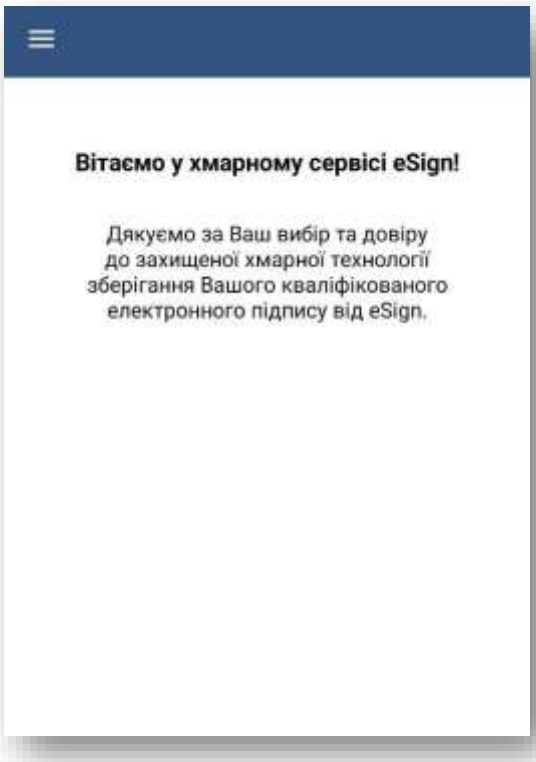

Рис.4.11. Приклад успішної регістрації в мобільному додатку eSign

Крок 3. Наступним кроком необхідно звернутися до сервісу для підписання документів (рис.4.12). Наприклад: ЦЗО (Центральний засвідчувальний орган) [37].

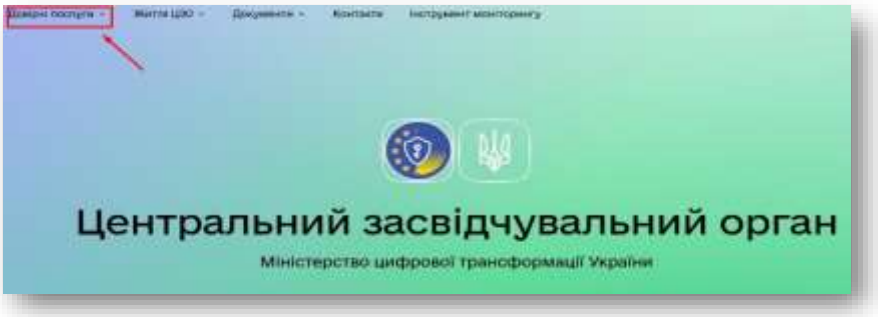

Рис.4.12. Звернення до сайту ЦЗО

Необхідно звернутися до вкладинки «Довірчі послуги» та натиснути «Підписати документ» (рис.4.13).

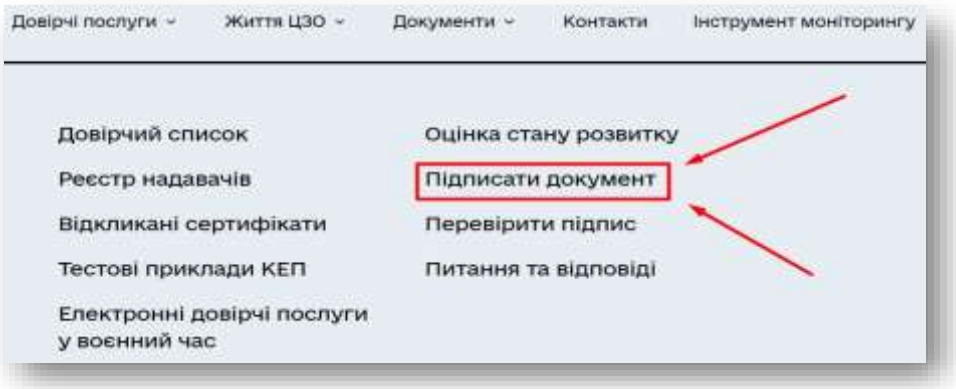

Рис.4.13. Приклад підписання документів на сайті ЦЗО

Крок 4. Серед запропонованих варіантів підписання необхідно обрати «Електронного підпису».

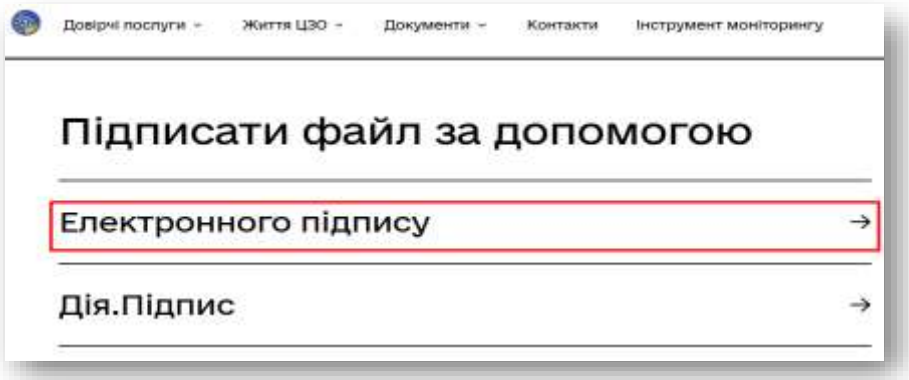

Рис.4.14. Приклад вибору механізму підпису файлу

Крок 5. Наступним кроком необхідно обрати тип підписки, тип сервісу підпису, ввести ідентифікатор користувача (ідентифікаційний код платника податків) та натиснути «Зчитати».

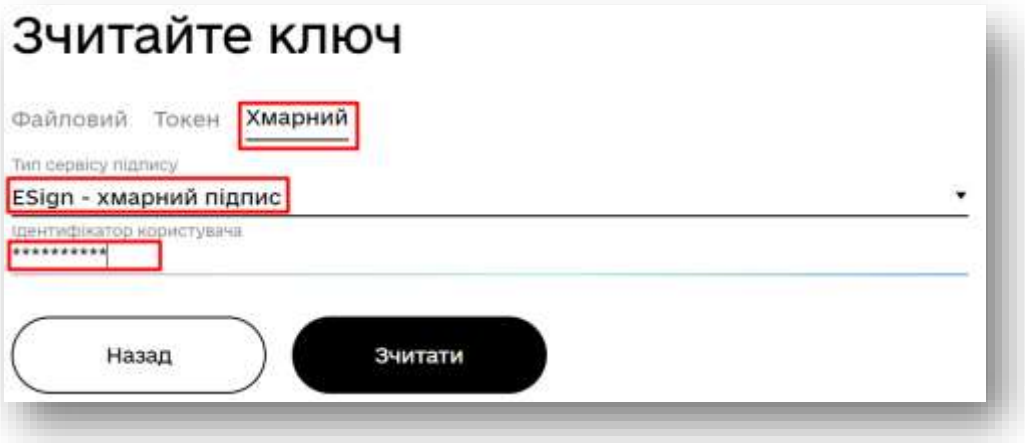

Рис.4.15. Введення ідентифікатора користувача

Крок 6. В додатку з’явиться сповіщення про підтвердження підписання. Необхідно перевірити введені дані, та натистунити «Далі».

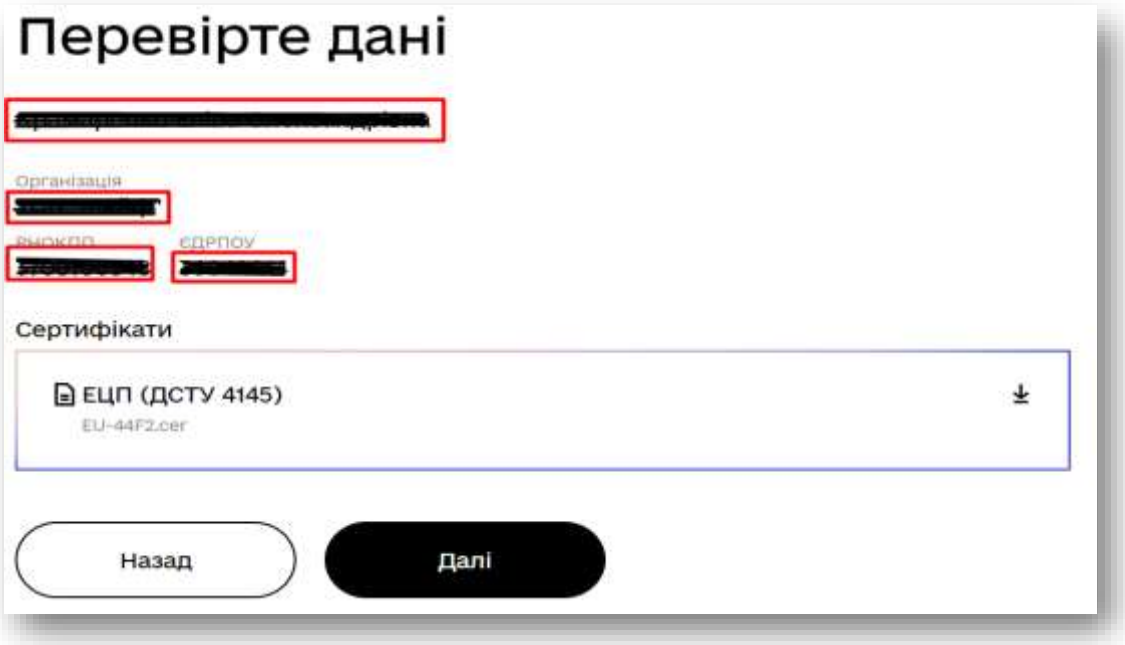

Рис.4.16. Перевірка даних

Після перевірки даних, необхідно ввести повторно пароль від ключа і натиснути «Підписати».

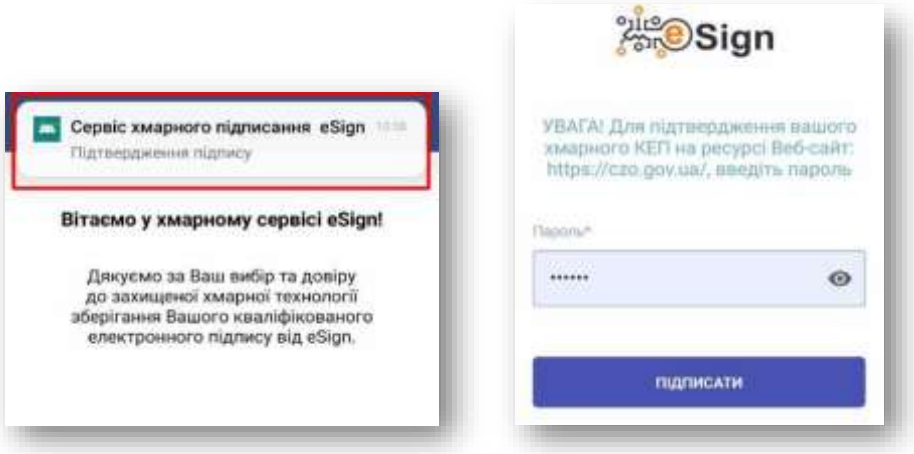

Рис.4.17. Приклад підписання

Крок 7. Наступним кроком необхідно повернутися на сайт ЦЗО, та повторно перевірити дані. Обрати потрібні налаштування (або залишити стандартні). Обрати документ який потрібно підписати і натиснути «Підписати».

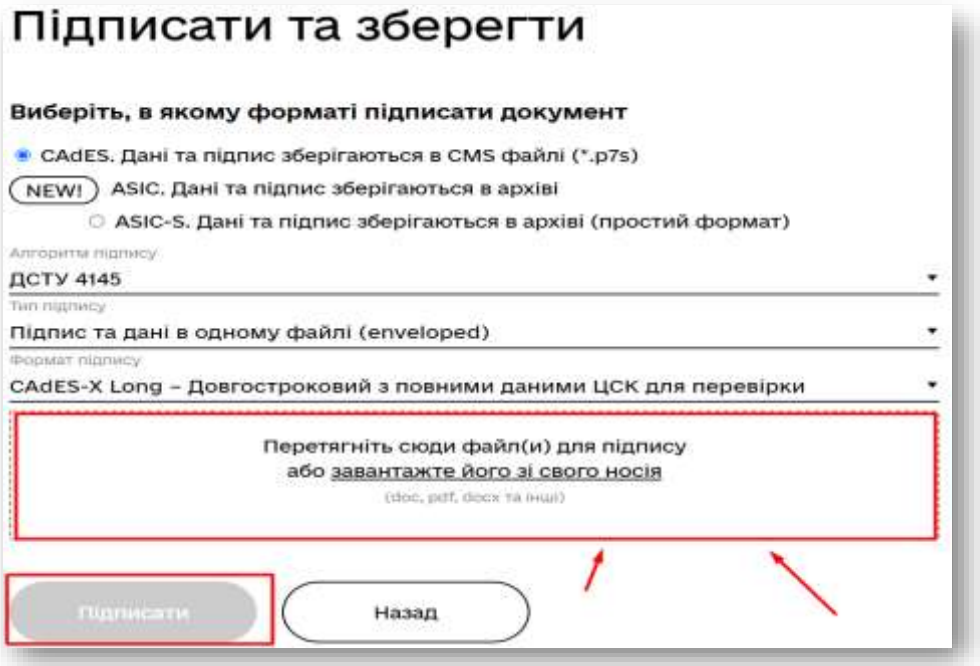

Рис.4.18. Фінальні перевірки перед підписом документів

Після цих кроків, документ вважається підписаним і його можна завантажити (рис.4.19).

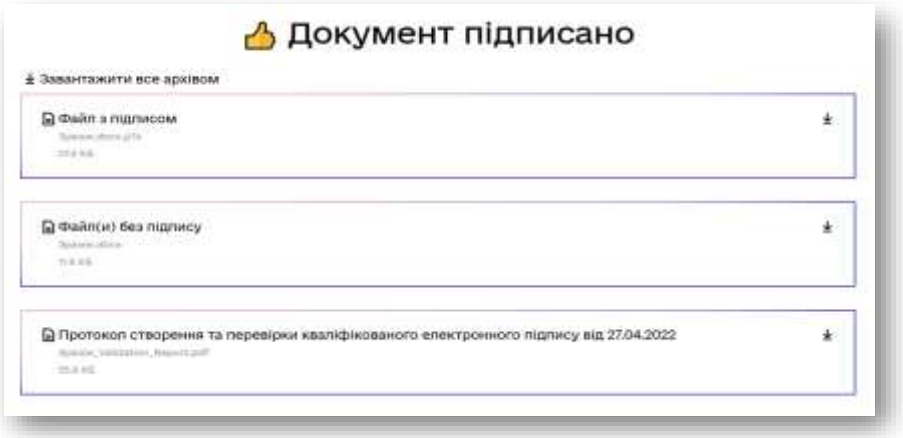

Рис.4.19. Приклад варіантів завантаження документу після підпису

4.5. Перевірка сертифікатів в Реєстрі документів довільних форматів

При використанні електронних підписів (ЕП) з сертифікатами, виданими іншими Акредитованими Центрами Сертифікації Ключів (АЦСК), необхідно забезпечити доступ до відповідних адрес служби часової мітки (TSP), протоколу перевірки статусу сертифікату (OCSP) та протоколу управління сертифікатами (CMP).

Активація цього сервісу дозволяє проводити перевірку чинності сертифікатів електронних підписів. Користувач може обрати метод перевірки: безпосередньо через сервер OCSP або використовуючи список відкликаних сертифікатів.

Перевірка сертифікатів у модулі реєстру документів різних форматів:

- *Вибір документа.* Виділити документ (вхідний або вихідний) з електронним підписом. У контекстному меню обрати опцію «Властивості», щоб відкрити відповідне вікно. У зазначеному вікні відображається інформація, пов’язана з підписом документа.
- *Збереження змін.* Для збереження внесених змін необхідно натиснути «Зберегти та вийти». При внесенні змін у налаштуваннях системи, необхідно обрати «Застосувати» для збереження цих змін. Якщо зміни не вносилися, кнопка «Застосувати» буде неактивною. Щоб закрити вікно налаштувань без збереження змін, натиснути «Відмінити».

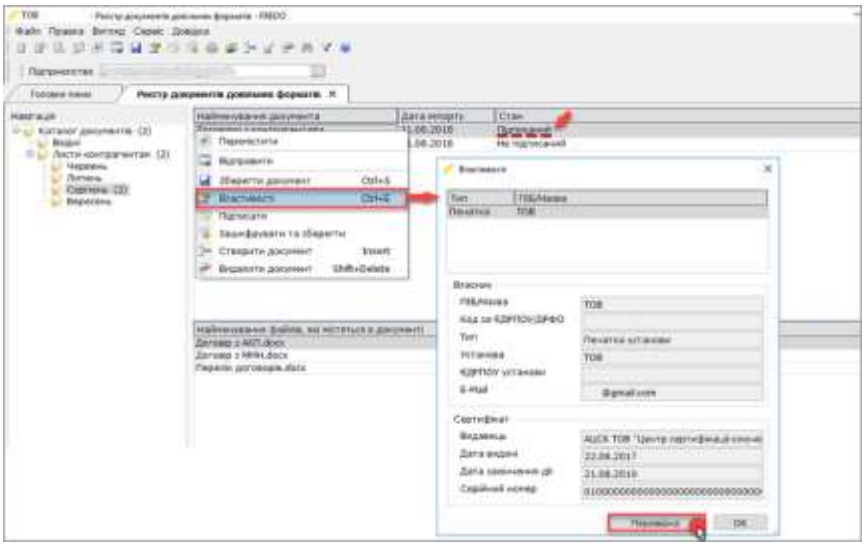

Рис.4.20. Перевірка документів

- *Заходи безпеки та захисту.* Важливо переконатися, що використовувані електронні підписи та їхні сертифікати відповідають стандартам безпеки. Необхідно регулярно оновлювати списки довірених сертифікатів та перевіряти чинність підписів, щоб уникнути використання скомпрометованих або відкликаних сертифікатів. Під час введення даних у систему, необхідно переконатися, що документ, який підписується, є вірним, та уникати шахрайських або фішингових атак[38].

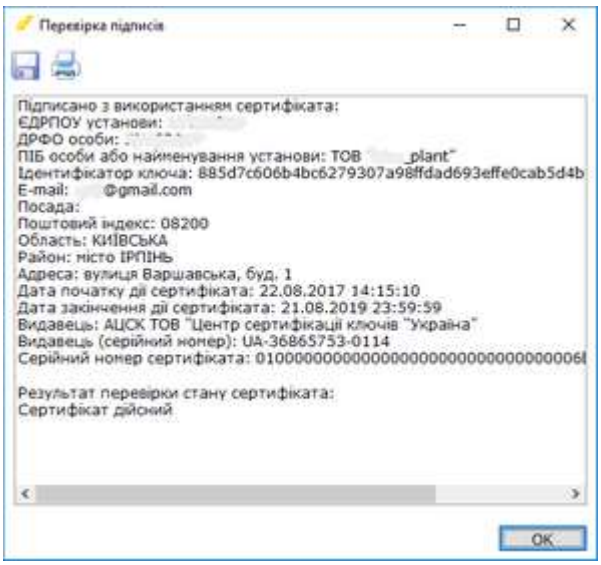

Рис.4.21. Огляд параметрів документів

Виконуючи ці кроки, можна ефективно та безпечно управляти електронними підписами у організації [39].

Висновки до четвертого розділу

Виокремлено критерії користувачів, так як потреби малого бізнеса, державних установ та звичайного користувача щодо створення та використання цифрових підписів відрізняються.

Зазначено, що для звичайного користувача важлива базова безпека, що забезпечує певний ступінь неспростування, без необхідності використання особистих цифрових сертифікатів; для малих підприємств повинні активно впроваджуватися політики кібербезпеки для захисту їхніх ділових даних, включаючи цифрові підписи; для великих корпорацій повинні активно впроваджуватися комплексні стратегії кібербезпеки для захисту своїх цифрових підписів та пов'язаних з ними даних. Регулярні оновлення та моніторинг безпеки є ключовими для запобігання шахрайству та іншим кіберзагрозам.

Досліджено платформи для створення цифрового підпису. Приведено алгоритм отримання кваліфікованого електронного підпису (КЕП). Приведено особливості отримання ЕЦП у Приватбанку, в Інформаційно-довідковому департаменті Державної податкової служби (ДПС) та через «Дію».

Приведено особливості перевірки сертифікатів в Реєстрі документів довільних форматів, адже при використанні електронних підписів з сертифікатами, виданими іншими АЦСК, необхідно забезпечити доступ до відповідних адрес служби часової мітки (TSP), протоколу перевірки статусу сертифікату (OCSP) та протоколу управління сертифікатами (CMP).

Розроблено алгоритм генерації ключів в АЦСК «Центр сертифікації ключів України» та алгоритм використання мобільного додатку eSign для генерації цифрового підпису.

ВИСНОВКИ

В кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

1. Проаналізовано поняття цифрового підпису та досліджено вітчизняне та міжнародне законодавство, що регламентує особливості функціонування електронних цифрових підписів.

2. Зазначено вимоги щодо цифрових підписів, особливості та їх класифікації та досліджено алгоритми та стандарти створення електронних цифрових підписів.

3. Виокремлено особливості реалізації традиційних схем електронного підпису, що включають: невідмовність, конфіденційність, цілісність та автентифікацію. Проведено аналіз алгоритмів хешування.

4. Досліджено механізми та засоби безпечної інтеграції електронних цифрових підписів у документообігу організації, особливості програмного забезпечення Microsoft Office, що включає комплекс інструментів що підтримує цифровий підпис документів.

5. Досліджено платформи для створення цифрового підпису. Приведено алгоритм отримання кваліфікованого електронного підпису (КЕП). Приведено особливості отримання ЕЦП у Приватбанку, в Інформаційно-довідковому департаменті Державної податкової служби (ДПС) та через «Дію».

6. Приведено особливості перевірки сертифікатів в Реєстрі документів довільних форматів, адже при використанні електронних підписів з сертифікатами, виданими іншими АЦСК, необхідно забезпечити доступ до відповідних адрес служби часової мітки (TSP), протоколу перевірки статусу сертифікату (OCSP) та протоколу управління сертифікатами (CMP).

7. Розроблено алгоритм генерації ключів в АЦСК «Центр сертифікації ключів України» та алгоритм використання мобільного додатку eSign для генерації цифрового підпису.

ПЕРЕЛІК ПОСИЛАНЬ

1. Electronic signature policy. [Електронний ресурс] - Режим доступу: https://k6legal.files.wordpress.com/2017/02/global-infrastructure-group-electronic-signature-policy-issue-2-may-16.pdf

2. How to avail electronic/digital signature facility for availing services. [Електронний ресурс] - Режим доступу: https://jakemp.nic.in/digital_sign.pdf

3. Закон України «Про електронні документи та електронний документообіг». [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15/print1274774604685720#Text

4. Закон України «Про електронний цифровий підпис» [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/852-15#Text

5. U.S. Department of Homeland Security. Office of Biometric Identity Management. [Електронний ресурс] - Режим доступу: http://www.biometrics.gov/ReferenceRoom/FederalPrograms.aspx

6. U.S. Congress. Electronic signatures in global and national commerce act. [Електронний ресурс] - Режим доступу: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

7. EU Directive 1999/93/EC. [Електронний ресурс] - Режим доступу: http://data.europa.eu/eli/dir/1999/93/oj/eng

8. UN General Assembly. United nations convention on the use of electronic communications in international contracts. [Електронний ресурс] - Режим доступу: https://treaties.un.org/doc/Treaties/2005/11/20051128%2004-23%20PM/Ch_X_18p.pdf

9. Entrust Inc. Digital Signatures. Entrust: Securing Digital Identities & Information. [Електронний ресурс] - Режим доступу: https://www.entrust.com/digital-signatures/

10. Dawn M. Turner. Understanding the Major Terms Around Digital Signatures. [Електронний ресурс] - Режим доступу: http://www.cryptomathic.com/news-events/blog/understanding-the-major-terms-

around-digital-signatures

11. Electronic signature platforms [Електронний ресурс] - Режим доступу: https://ec.europa.eu/futurium/en/system/files/ged/plc_article_on_e-signature_platforms_final_feb_2017.pdf

12. John Ross, Nick Pope, Denis Pinkas. Electronic Signature Formats for long term electronic signatures. [Електронний ресурс] - Режим доступу: https://tools.ietf.org/html/rfc3126

13. B. Kaliski. RSA-digital-signature-standards. [Електронний ресурс] - Режим доступу: https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/905slide.pdf

14. Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory. Vol. 22. No. 6. Pp.644–654. 1976. DOI: 10.1109/TIT.1976.1055638

15. R. Housley, W. Ford, W. Polk, D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459. [Електронний ресурс] - Режим доступу: http://www.rfc-editor.org/rfc/rfc2459.txt

16. Symantec Corporation. Buy and Compare SSL Certificates. [Електронний ресурс] - Режим доступу: https://www.symantec.com/ssl-certificates/compare-ssl-prices.jsp

17. T. Dierks, E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. [Електронний ресурс] - Режим доступу: http://www.rfc-editor.org/rfc/rfc5246.txt

18. R. Housley. Cryptographic Message Syntax (CMS). RFC 5652. [Електронний ресурс] - Режим доступу: http://www.rfc-editor.org/rfc/rfc5652.txt

19. Dawn M. Turner. eIDAS from directive to regulation. [Електронний ресурс] - Режим доступу: http://www.cryptomathic.com/news-events/blog/eidas-from-directive-to-regulation-legal-aspects

20. Sean Parkinson, Kathleen Moriarty, Michael Scott, Andreas Rusch, Magnus Nystrom. PKCS #12: Personal Information Exchange Syntax. [Електронний ресурс] - Режим доступу: https://tools.ietf.org/html/rfc7292

21. J. Sermersheim. Lightweight Directory Access Protocol (LDAP). RFC 4511 [Електронний ресурс] - Режим доступу: http://www.rfc-editor.org/rfc/rfc4511.txt

22. Andrew Betteridge. A Note on Electronic Signatures. [Електронний ресурс] - Режим доступу: http://www.ashfords.co.uk.

23. ISO/IEC 27000:2018. Information technology — security techniques — information security management systems — overview and vocabulary. [Електронний ресурс] - Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

24. NIST. Public key infrastructure testing — CSRC — CSRC. [Електронний ресурс] - Режим доступу: https://csrc.nist.gov/projects/pki-testing

25. NIST. FIPS202 - SHA3. [Електронний ресурс] - Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

26. Adobe Systems Incorporated. PDF Reference Adobe Portable Document Format [Електронний ресурс] - Режим доступу: http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf

27. Adobe Systems Incorporated. Digital Signatures in a PDF. Adobe Systems Incorporated. [Електронний ресурс] - Режим доступу: https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf

28. Adobe Systems Incorporated. Digital Signatures Workflow Guide: a guide for workflow owners. [Електронний ресурс] - Режим доступу: http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigSig_WorkflowGuide.pdf

29. Adobe. Adobe - PDF digital signatures. [Електронний ресурс] - Режим доступу: https://www.adobe.com/devnetdocs/etk_deprecated/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf

30. Adobe. E-signature pricing and plans — acrobat sign. [Електронний ресурс] - Режим доступу: https://www.adobe.com/sign/pricing/plans.html

31. Microsoft. Preinstalled Trusted Root Certificates. [Електронний ресурс] - Режим доступу: https://technet.microsoft.com/en-us/library/cc962063.aspx

32. BankID. [Електронний ресурс] - Режим доступу: https:// www.bankid.no/en/private/about-us

33. Про Систему BankID Національного банку. [Електронний ресурс] - Режим доступу: https://bank.gov.ua/ua/bank-id-nbu/

34. Кваліфікований надавач електронних довірчих послуг. «MASTERKEY». [Електронний ресурс] - Режим доступу: https://ca.masterkey.ua/

35. Віддалений кваліфікований електронний підпис «Дія.Підпис» (Дія ID) [Електронний ресурс] - Режим доступу: https://onlinebank.dp.ua/79-e-services/diia/915-viddalenij-kep-diya-pidpis-elektronnij-pidpis-v-smartfoni/

36. Кваліфікований електронний підпис/[Електронний ресурс] - Режим доступу: https://uakey.com.ua/page/esignature

37. Електронний підпис в Україні. [Електронний ресурс] - Режим доступу: http://surl.li/njese

38. Електронний реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів. [Електронний ресурс] - Режим доступу: https://czo.gov.ua/ca-registry

39. Перевірка підписів. [Електронний ресурс] - Режим доступу: https://fredo.com.ua/help/admcomanyparams_pp.htm

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА НА ТЕМУ:

«ТЕХНОЛОГІЯ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ В ОРГАНІЗАЦІЇ»

Керівник:
д.т.н, проф.
КОЖУХІВСЬКИЙ Андрій

Виконав:
здобувач вищої освіти
групи БСДМ-61 БОНДАРЄВ Ілля

Київ 2023

2

Об'єкт – процес безпечного застосування електронних цифрових підписів в організаційних операціях.

Предмет – механізми та засоби безпечної інтеграції електронних цифрових підписів у документообіг організації.

Мета – підвищення рівня інформаційної безпеки в організації шляхом впровадженню електронних цифрових підписів в документообіг.

- **Наукові завдання:**
- проаналізувати правові аспекти функціонування цифрових підписів в Україні та світі;
- дослідити алгоритми та стандарти створення електронних цифрових підписів;
- дослідити механізми та засоби безпечної інтеграції електронних цифрових підписів у документообігу організації;
- дослідити платформи для створення цифрових підписів в Україні.

3

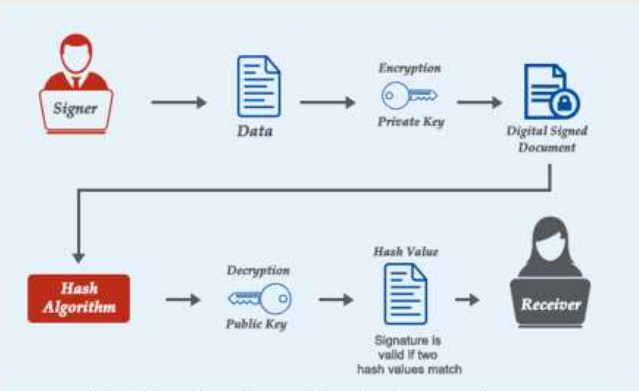

Рис.1. Послідовність реалізації цифрового підпису

ДОСЛІДЖЕННЯ АЛГОРИТМІВ ТА СТАНДАРТІВ СТВОРЕННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

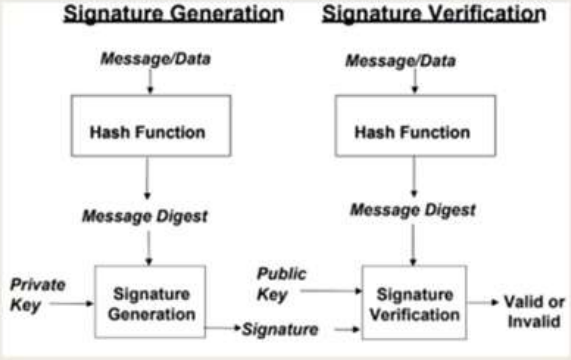

Рис.2. Пов'язані процеси підписання та перевірки підписів

ПОРІВНЯННЯ ПОКАЗНИКІВ БЕЗПЕКИ ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ

Рис.3.Процедура входу в BankID

Рис.4. Приклад PDF-файл, до якого було додано два підписи через онлайн-функцію підпису Adobe

Рис.5. Вибір цифрового сертифікату в Microsoft Office

ОТРИМАННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ (КЕП)

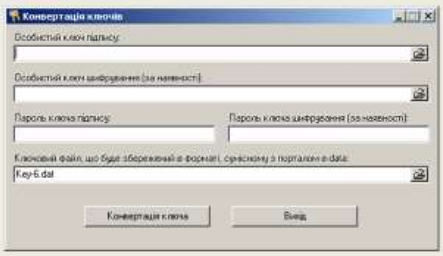

Рис.6. Конвертація ключів за допомогою АЦСК «Центр сертифікації ключів України»

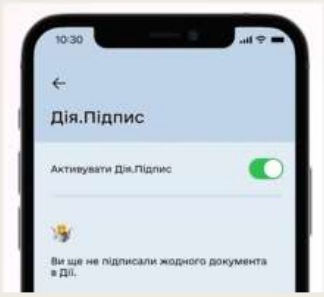

Рис.7. Активація віддаленого КЕП через «Дія.Підпис»

АЛГОРИТМ ГЕНЕРАЦІЇ КЛЮЧІВ В АЦСК «ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ УКРАЇНИ»

7

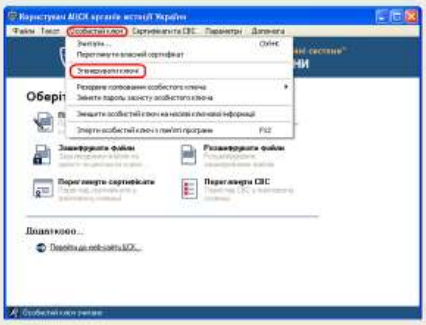

Рис.8. Приклад генерації особистого ключа в АЦСК

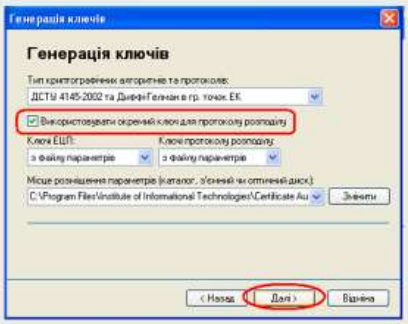

Рис.9. Приклад налаштування окремого ключа для протоколу розподілу

АЛГОРИТМ ГЕНЕРАЦІЇ КЛЮЧІВ В АЦСК «ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ УКРАЇНИ»

8

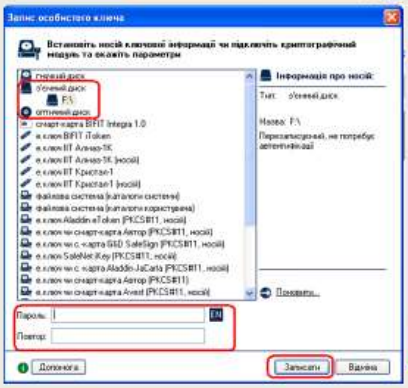

Рис.10. Вибір з'ємного носія

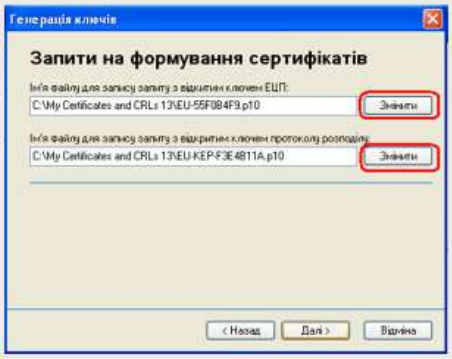

Рис.11. Приклад внесення змін щодо носіїв інформації та імені запитів

ВИКОРИСТАННЯ МОБІЛЬНОГО ДОДАТКУ ESIGN ДЛЯ ГЕНЕРАЦІЇ ЦИФРОВОГО ПІДПИСУ

9

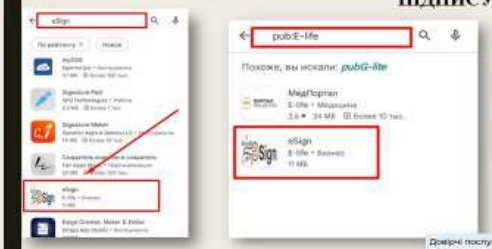

Рис.12. Завантаження додатку eSign

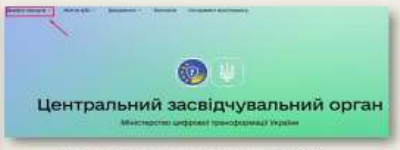

Рис.13. Звернення до сайту ЦЗО

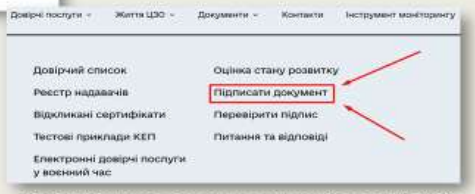

Рис.14. Приклад підписання документів на сайті ЦЗО

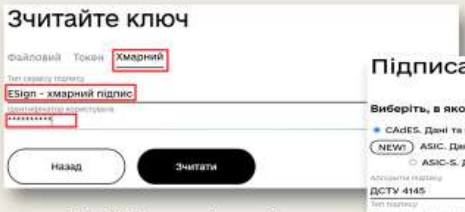

Рис.15. Введення ідентифікатора користувача

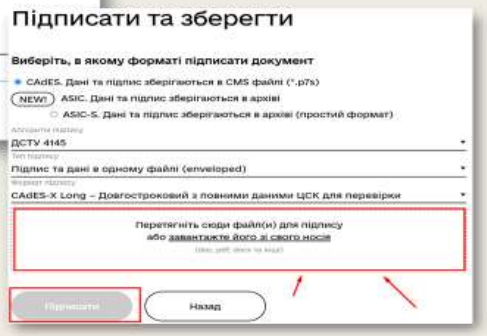

Рис.16. Фінальні перевірки перед підписом документів

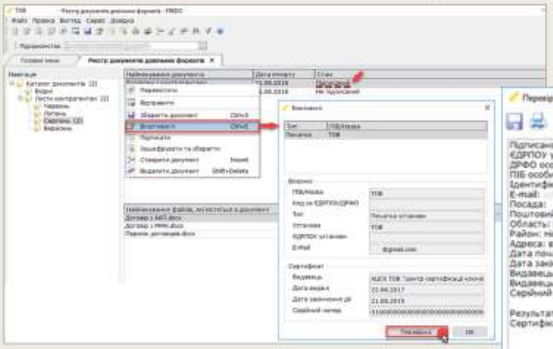

Рис.17. Перевірка документів

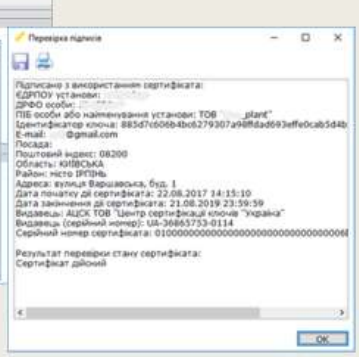

Рис.18. Огляд параметрів документів

Висновки

1. Проаналізовано поняття цифрового підпису та досліджено вітчизняне та міжнародне законодавство, що регламентує особливості функціонування електронних цифрових підписів.
2. Зазначено вимоги щодо цифрових підписів, особливості та їх класифікації та досліджено алгоритми та стандарти створення електронних цифрових підписів.
3. Виокремлено особливості реалізації традиційних схем електронного підпису, що включають: невідмовність, конфіденційність, цілісність та автентифікацію. Проведено аналіз алгоритмів хешування.
4. Досліджено механізми та засоби безпечної інтеграції електронних цифрових підписів у документообігу організації, особливості програмного забезпечення Microsoft Office, що включає комплекс інструментів що підтримує цифровий підпис документів.
5. Досліджено платформи для створення цифрового підпису. Приведено алгоритм отримання кваліфікованого електронного підпису (КЕП). Приведено особливості отримання ЕЦП у Приватбанку, в Інформаційно-довідковому департаменті Державної податкової служби (ДПС) та через «Дію».
6. Приведено особливості перевірки сертифікатів в Реєстрі документів довільних форматів, адже при використанні електронних підписів з сертифікатами, виданими іншими АЦСК, необхідно забезпечити доступ до відповідних адрес служби часової мітки (TSP), протоколу перевірки статусу сертифікату (OCSP) та протоколу управління сертифікатами (CMP).
7. Розроблено алгоритм генерації ключів в АЦСК «Центр сертифікації ключів України» та алгоритм використання мобільного додатку eSign для генерації цифрового підпису.