Тема 3. Основні дії з електронним документом

- Опис типового процесу електронного діловодства (життєвий цикл еДок)
  - Створення електронних документів
  - Перевірка електронних документів
  - Обмін електронними документами
  - Архівне зберігання електронних документів
  - Відображення електронних довірчих послуг на етапі життєвого циклу еДок
  - Практичне застосування електронних довірчих послуг для проходження життєвого циклу еДок
- Огляд наявних засобів для створення еДок на ринку України

Опис типового процесу електронного діловодства (життєвий цикл еДок)

Будь-який документ незалежно від його структури або змісту проходить ряд стадій, які в цілому називаються життєвим циклом документа. Життєвий цикл документа — період часу від моменту формування до моменту передачі в архів (на зберігання) або знищення.

Всі документи проходять через такі основні етапи життєвого циклу (деякі етапи можуть повторюватися, а деякі мають місце лише один раз):

- створення електронних документів;
- перевірка електронних документів;
- обмін електронними документами;
- архівне зберігання електронних документів (при цьому можливе або знищення електронних документів, або їх довічне чи тимчасове архівне зберігання).

Схема типового процесу електронного діловодства (життєвого циклу еДок) наведена на рис. 3.1. В підручниках з діловодства такого поняття як життєвий цикл еДок немає, є лише поняття «документообіг» – рух документів в організації з моменту їх створення або отримання до завершення виконання або відправлення. Розглянемо докладніше кожен етап життєвого циклу еДок.

Створення електронних документів. Життєвий цикл будь-якого документа починається з процесу його створення, який включає в себе підпроцеси створення проекту документа, його рецензування, виправлення, узгодження та підписання. Головними вимогами на цьому етапі є використання:

– єдиного формату файлу електронного документу;
– стандартизованих ЕЦП;
– єдиного формату даних електронного документообігу.

Формат даних електронного документообігу – визначені структура та зміст контейнера, призначеного для приймання-передавання даних в електронному документообігу

Контейнер – файл, структура і зміст якого відповідають вимогам специфікації формату ZIP та ISO/IEC 21320-1:2015

Сучасні наукові дослідження свідчать про необхідність стандартизації електронного документа як об'єкта. Так, у праці [18] зазначено: «Основною проблемою, яка значно знижує ефективність автоматизації облікових робіт, є проблема узгодження форматів представлення даних. Тому пошук прийнятного формату є принциповим для побудови великих (масштабу установи) інформаційних систем».

З іншого боку, використання старих заархівованих даних є складним завданням. Для установ, призначених для зберігання в електронному вигляді мільйонів документів, критично важливо використовувати формат, який зберігає первинний вигляд документа, має хорошу документацію, не залежить від виробника і операційної системи, підтримує пошук і є автономним, тобто не вимагає додаткових даних для перегляду документа [19].

Формат файлу PDF відповідає всім зазначеним вище вимогам, він стандартизований [20] і визнаний Міжнародною організацією зі стандартизації ISO форматом для цілей довгострокового архівування [21]. Саме тому розроблений компанією Adobe System відкритий міжоперабельний формат PDF/A-1 (розширення *.pdf) визначений в якості формату для створення текстових електронних документів в Переліку форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання [22], на який посилаються Вимоги до форматів даних електронного документообігу в органах державної влади [23].

Рисунок 3.1 – Типовий процес електронного діловодства (життєвий цикл еДок)

В рамках гармонізації Українського законодавства із законодавством ЄС в Україні було прийнято Закон України «Про електронні довірчі послуги», який імплементував EU Regulation 910/2014. В рамках прийняття підзаконних актів для Закону України «Про електронні довірчі послуги» та з метою досягнення гармонізації стандартів ЕЦП між Україною та ЄС було визначено три типи форматів ЕЦП – CadES, XAdES та PAdES. Ці стандарти сприятимуть обміну електронними документами всередині України, а також з державами-членами ЄС.

Під час підписування даних створюваний при цьому підпис має бути пов'язаний з даними, до яких він застосовується. Цього можна досягти або шляхом створення набору даних, що поєднує підпис та дані, які було підписано (наприклад, шляхом обгортання даних з підписом чи включення підпису в набір даних), або шляхом розміщення (відокремленого) підпису в окремому ресурсі з наявністю деяких зовнішніх засобів для асоціації підпису з даними, до яких він застосовується. Хоча при використанні відокремлених підписів мають

місце певні переваги, головною з яких є те, що вихідні об'єкти даних при цьому не модифікуються, залишається ризик того, що підпис стає відокремленим від даних, до яких він застосовується, і тому втрачається зв'язок між підписом та даними.

Тому в багатьох прикладних системах розроблено власні техніки для комбінування відокремленого підпису з підписаним об'єктом у контейнері певної форми, щоб їх було легше розподілити та гарантувати, що під час перевірки використовується коректний підпис та відповідні метадані. Ті самі вимоги застосовуються до асоціювання підтверджень часу (наприклад, до токенів часових штемпелів або записів доказів) та до пов'язаних з ними даних.

Метадані – дані про інформаційні об’єкти та їх окремі структури, що є складовими формату даних електронного документообігу, а також процеси, які відбуваються над цими інформаційними об’єктами

Хоча ZIP[1] надає базову структуру контейнера, яка може пов'язувати файли, що містять об'єкти даних (об'єкти-файли) та підпис(и), що до них застосовуються, існує визнана потреба в додатковій структурі та метаданих про асоціацію, наприклад, для зв'язування конкретного підпису з об'єктом-файлом, до якого він застосовується.

Тому Європейським інститутом зі стандартизації в області телекомунікацій ETSI (European Telecommunications Standards Institute) було розроблено низку стандартів, складовою частиною яких став ETSI EN 319 162-1:2016 [24]. В цьому стандарті визначено стандартизоване використання типів контейнерів для встановлення спільного способу асоціювання файлів, що містять об'єкти даних, з файлами, що містять цифрові підписи та/або підтвердження часу. Завдяки використанню загальної форми контейнеру та пов'язаної інформації полегшиться обмін даними та інтероперабельність між різними службами підписування та валідації.

Цей стандарт призначений для покриття контейнерів, включаючи цифрові підписи та підтвердження часу, що підтримуються сертифікатами PKI та відкритих ключів, і спрямований на задоволення загальних вимог міжнародного співтовариства щодо забезпечення довіри до та конфіденційності електронних транзакцій, включаючи, крім іншого, застосовні вимоги Регламенту (ЄС) № 910/2014 [4, 5].

Отже, в [23] вимагається поєднувати міжнародний стандарт з подання архівного PDF і формат даних контейнера, що відповідає вимогам [24]. Саме ця комбінація гарантує збереження візуального подання еДок і вбудовані механізми довготривалої валідації ЕЦП, не обмеженої у часі.

[1] ISO/IEC 21320-1:2015 Information technology – Document Container File – Part 1: Core (Інформаційні технології. Файл контейнера документа. Частина 1: Зміст)

Перевірка електронних документів. Відповідно до вимог [21] “процедура перевірки електронного документа полягає у перевірці наявності всіх його обов’язкових реквізитів та його цілісності шляхом перевірки та підтвердження кваліфікованого електронного підпису та/або печатки”.

В ETSI EN 319 102-1:2016 [25] визначено процедури для створення цифрових підписів та встановлення факту технічної валідності цифрового підпису (тобто перевірки юридичного статусу підпису). Крім того, в цьому стандарті описано концептуальну модель валідації підпису. Ця модель описує як застосування валідації підпису (signature validation application, SVA) отримує цифровий підпис та інші вхідні дані та виконує валідацію у відповідності з політикою валідації підпису, яка складається з сукупності обмежень валідації. SVA має виводити індикатор стану та звіт про валідацію, в якому містяться деталі технічної валідації кожного з застосованих обмежень, які можуть бути актуальними при інтерпретації результатів.

Валідація підпису (signature validation) – процес верифікації та підтвердження того, що підпис валідний

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

Обмеження (підпису) ((signature) constraints) – абстрактне формулювання правил, значень, діапазонів і результатів обчислень, згідно з якими цифровий підпис може пройти валідацію

Дані створення підпису (signature creation data) – унікальні дані, такі як коди або приватні криптографічні ключі, які використовуються підписувачем для створення значення цифрового підпису

Валідація завжди починається з процесу валідації підпису, що забезпечує довготривалу доступність та цілісність матеріалу валідації. Одним з перших етапів цього процесу є запуск процесу для підписів з часом та підписів з матеріалами для довгострокової перевірки, які знову запустять процес для базових підписів. Фактично, валідація виконується за життєвим циклом підпису і оцінює стан підпису на основі процесу валідації для першого класу підпису цього життєвого циклу (базовий підпис). Якщо цей процес не призводить до остаточного висновку про валідацію (позитивну чи негативну), то валідацію можна зупинити. Однак, можливо, цей клас підпису не містить інформацію, необхідну для остаточного висновку. У цьому випадку валідація продовжується процесом валідації для наступного посиленого класу підписів (підпис з часом, підпис із матеріалами для довгострокової валідації, підпис, що забезпечує довготривалу доступність та цілісність матеріалу валідації), доки не буде можливим отримати остаточний висновок або відсутні процеси валідації для наступного класу посилених підписів. Результат валідації останнього процесу валідації підпису, є остаточним результатом валідації підпису (який може бути невизначеним через відсутність інформації).

Для того, щоб завершити валідацію одного з класів підписів, застосовуються кілька складових частин валідації (формат підпису, валідність сертифікату підписування, криптографічна верифікація тощо). Позначення стану кожної окремої складової частини валідації може бути одним з наступних: PASSED, FAILED або INDETERMINATE.

Стан повної валідації одного з класів підпису в контексті визначеної політики валідації підпису має бути таким:

– TOTAL-PASSED – криптографічні перевірки підпису (включаючи перевірки гешей окремих об'єктів даних, які було підписано непрямим чином), а також всі перевірки, передбачені політикою валідації підпису, здійснено успішно.

– TOTAL-FAILED – криптографічні перевірки підпису не вдалися (включно з перевірками гешей окремих об'єктів даних, підписаних непрямим чином), або доведено, що генерація підпису відбувалася після анулювання сертифіката підписання або тому, що підпис не відповідає одному з базових стандартів у тій мірі, в якій складова частина криптографічної верифікації не може обробити його.

– INDETERMINATE – результати проведених перевірок не дозволяють встановити, що підпис TOTAL-PASSED або TOTAL-FAILED.

Індикація основного стану може супроводжуватись додатковою інформацією.

Якщо SVA повертає TOTAL-PASSED для певного підпису, то цей підпис необхідно розглядати як технічно валідний відповідно до обмежень валідації.

Якщо SVA повертає TOTAL-FAILED, підпис не можна вважати технічно валідним.

Якщо SVA повертає INDETERMINATE і якщо докладна інформація вказує, що результат може змінитися при повторному виконанні алгоритму перевірки, то можна повторити валідацію на основі додаткової інформації або пізніше у часі [25].

Обмін електронними документами. У сучасному світі синонім безпечного обміну електронними повідомленнями – це послуги електронної реєстрованої доставки. Що це таке?

Регламент eIDAS [4, 5] встановлює принцип, відповідно до якого електронний документ не можна позбавити юридичної сили лише на тій підставі, що він знаходиться в електронному вигляді.

Це положення також визначає **послугу електронної реєстрованої доставки** (надалі – послуга eDelivery), як “послугу, що дозволяє передавати дані між третіми сторонами за допомогою електронних засобів та надає докази, пов'язані з обробкою переданих даних, включаючи доказ відправлення та отримання даних, які захищають передані дані від ризику втрати, крадіжки, пошкодження або будь-яких несанкціонованих змін” (ст. 3.36).

На практиці дані, на які посилається це визначення, при передачі за допомогою такої послуги eDelivery від відправника одержувачу можуть бути будь-якого типу, включаючи структуровані та не структуровані електронні документи (відразу створені в електронній формі або дематеріалізовані документи). Засоби передачі можуть бути будь-якого типу, включаючи, але не обмежуючись електронною поштою.

Дані, на які посилається це визначення, при передачі за допомогою такої послуги eDelivery від відправника отримувачу зазвичай називаються **повідомленням** [26].

В [27] зазначено, що послуга eDelivery надається одним провайдером послуг електронної реєстрованої доставки ERDSP. Провайдери ERDSP можуть співпрацювати при передачі даних від відправника одержувачу, якщо вони підписані на різних провайдерів ERDSP. В якості такого провайдера може виступати провайдер довірчих послуг, визначений в Регламенті (ЄС) № 910/2014 [4].

Служба ERDS надає докази щодо подій, які відбуваються під час передачі даних між сторонами (наприклад, докази того, що дані доставлені одержувачу), подібно до відомих фізичних поштових служб для паперових документів, таких як «реєстрована електронна пошта» та/або «повернення отримання». Ці докази можна використовувати для доведення третім сторонам, а також, за необхідності, у судовому розгляді, що транзакція мала місце в той самий час і між тими сторонами, які зазначені в доказах. Юридичні вимоги до служби ERDS та докази, які вона потребує для підтримки, можуть відрізнятися в різних галузях.

Служба електронної реєстрованої доставки (Electronic Registered Delivery Service, ERDS) – це електронна служба, яка передає дані між відправником та одержувачами за допомогою електронних засобів та надає докази стосовно обробки переданих даних, включаючи доказ відправлення та отримання даних, а також захищає дані, що передаються, від ризику втрати, крадіжки, пошкодження або будь-яких несанкціонованих змін

Провайдер послуг електронної реєстрованої доставки (Electronic Registered Delivery Service Provider, ERDSP) – організація, яка надає послуги електронної реєстрованої доставки

Доказ ERDS – це підтвердження, надане ERDS про те, що конкретна подія, пов'язана з процесом передачі певних даних між відправником та одержувачем (наприклад, подання повідомлення, доставка повідомлення, відмова від повідомлення), сталася в певний час. Документи ERDS можуть бути негайно доставлені відправнику/одержувачу або зберігатися в сховищі для подальшого доступу зацікавленими сторонами. Застосовується практика реалізації доказів ERDS у вигляді даних, підписаних цифровим підписом.

Безпечна і надійна доставка одержувачу вимагає однозначної ідентифікації одержувача (наприклад, для забезпечення юридичної відповідальності), навіть якщо у деяких випадках його ідентичність не розкривається одержувачу. Унікальної ідентифікації можна досягти за допомогою одного унікального ідентифікатора або набору атрибутів, які однозначно ідентифікують відправника або одержувача. Важливою метою є підтримка передачі ERDS між відправниками та одержувачами, які є фізичними або юридичними особами; проте в принципі будь-який однозначно ідентифікований об'єкт (система, послуга, функція тощо), який можна адресувати через ERDS, може виступати в ролі відправника або одержувача. В [27] також описано делегування, тобто здатність відправника або одержувача делегувати іншій сутності повноваження діяти від її імені. Служба ERDS може покладатися на сторонні, довірені сторони для автентифікації [27].

Послугу eDelivery можуть використовувати всі види суб'єктів, що бажають безпечно обмінюватися електронними документами, такими як державні адміністрації, бізнес-організації та громадяни. При цьому можливі різні типи передачі повідомлень, які можуть отримати вигоду від eDelivery, наприклад, адміністрація адміністрації (A2A), адміністрація для бізнесу (A2A), клієнт клієнту (C2C).

Кваліфікована послуга eDelivery означає послугу електронної реєстрованої доставки, яка:

– надається кваліфікованими постачальниками довірчих послуг, тобто організаціями, що перебувають під національним наглядом, а їх відповідність вимогам регулярно перевіряється акредитованим, довіреним суб'єктом, так званим органом з оцінки відповідності;

– забезпечує високий рівень довіри щодо ідентифікації відправника;

– забезпечує ідентифікацію адресата перед доставкою;

– захищає відправлення та отримання даних, використовуючи вдосконалений електронний підпис або печатку кваліфікованого постачальника довірчих послуг у такий спосіб, щоб було можливо виявити всі зміни даних;

– захищає дату і час відправлення та отримання з використанням кваліфікованих електронних штемпелів часу;

– відповідає іншим потенційним стандартам, які Комісія вважає релевантними.

Реєстрована електронна пошта є загально прийнятою реалізацією eDelivery, хоча існують більш специфічні послуги eDelivery, такі як доставка податкової декларації або eInvoicing, що використовують різні типи повідомлень і канали зв'язку [26].

Архівне зберігання електронних документів. Документи, що відпрацювали всі необхідні етапи, або знищуються, або переміщаються в архів для централізованого зберігання. За вимогою документи за допомогою функції пошуку можна запитати та вилучити з архіву. Архівне зберігання електронних документів може передбачати середньострокове або довготривале (довічне) зберігання електронних документів.

Задача середньострокового та довготривалого зберігання зумовлена вимогами чинного законодавства зберігати первинні електронні документи (ПЕД) як мінімум 3 роки. Але згідно з [2] і регламентами Акредитованих центрів сертифікації ключів (АЦСК) [28] ЕЦП видається терміном до двох років[2] (крім сертифікатів АЦСК та сертифікатів серверів позначки часу, термін дії яких може досягати п’яти років), тому ПЕД втрачає правочинність мінімум через день, а максимум через рік-два [19].

Для вирішення проблеми довготривалого зберігання еДок, необхідно застосовувати відповідні процедури створення та валідації цифрових підписів, описані в ETSI EN 319 102-1:2016 [25]. Відповідно до визначеної в цьому стандарті моделі створення підпису метою створення підпису є генерація підпису, що охоплює документ підписувача (Signer's Document, SD), сертифікат підписування або посилання на нього, а також атрибути підпису, що підтримують підпис, його інтерпретацію та призначення. В цьому процесі використовуються такі інформаційні об'єкти:

– обмеження створення підпису, сукупність яких контролює процес створення підпису;

– документ підписувача SD – це документ, для якого створюється підпис і з яким він асоціюється;

– подання документу підписувача (SDR), яке використовується для обчислення підпису як подання SD;

– атрибути підписів – це частина інформації, яка підтримує підпис AdES, його інтерпретацію та призначення, і яка може бути охоплена підписом разом з SD. Множина

[2] Стандарти захисту вказують на те, що електронний підпис має створюватися із застосуванням стійких до злому алгоритмів. Перш за все, це вимога стосується підбору ключа або можливості впливу на нього за допомогою програмних або апаратних засобів. Саме цими факторами обумовлені терміни, на які АЦСК видають сертифікати ключів, бо лише на цей строк можна гарантувати стійкість до злому сучасних криптографічних алгоритмів.

атрибутів, що входять до складу підпису, визначається політикою створення підпису або, при посиленні підпису, застосовується політика посилення підпису, яка також може враховувати специфіку різних форматів. Зокрема, атрибути підписів можуть включати ідентифікатор сертифікату підписування, ідентифікатор політики підпису, репозиторій політики підписів, заявлений час підписання тощо;

– дані, що підлягають підписанню DTBS (Data To Be Signed) – мають бути побудовані на основі інформаційних об'єктів, охоплених підписом, а саме документів SD або SDR та атрибутів підпису, обрані для підписання разом з документом SD;

– дані, які підлягають підписанню (форматовані) DTBSF (Data To Be Signed (Formatted)) – створюється з об'єктів DTBS шляхом їх форматування та розміщення у правильній послідовності для процесу підписання.

– подання даних для підписання DTBSR (Data To Be Signed Representation) – DTBSF гешуються відповідно до геш-алгоритму, зазначеному в криптографічному наборі, результатом цього процесу є подання DTBSR, яке потім використовується для створення підпису;

– підпис – створюється з DTBSR, до якого застосовується алгоритм підпису, вказаний у криптографічному наборі, результатом цього процесу є значення підпису.

– підписаний об'єкт даних SDO (Signed Data Object) – створюється шляхом одержання значення підпису та його форматування відповідно до типу SDO. Об'єкт SDO має містити значення підпису, підписані атрибути та може містити документи SD або SDR та/або додаткові допоміжні непідписані атрибути.

– дані валідації – додаткові дані, необхідні для валідації. Ці додаткові дані називаються даними валідації, є результатом процесу посилення підпису та включають сертифікати відкритих ключів PKC (Public Key Certificate), інформацію про статус анулювання для кожного PKC (списки відкликаних сертифікатів CRL (Certificate Revocation List) або відомості про статус сертифікатів OCSP (Online Certificate Status Protocol)) та застосовані до підпису підтвердження часу.

На рис. 3.2 показана структура підпису, спільна для всіх класів підписів, визначених в [25] і описаних нижче. Він складається з документу підписувача та підписаних атрибутів, обидва з яких є вхідними даними для обчислення значення підпису, самого значення підпису та будь-яких не підписаних атрибутів, що входять до підпису.

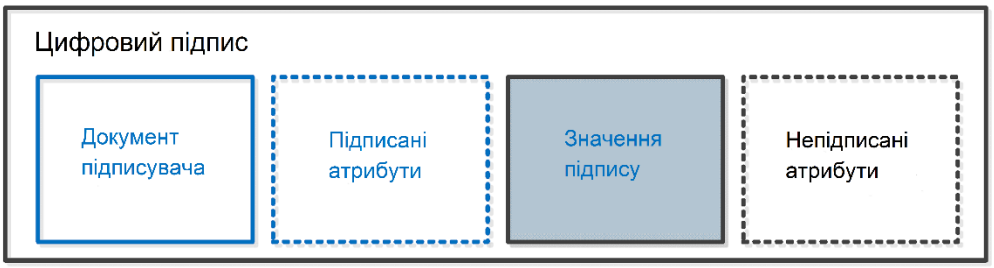

Рисунок 3.2 – Цифровий підпис

На рис. 3.3 відображено життєвий цикл підпису. Більшість підписів використовують лише деякі етапи життєвого циклу. На рисунку етапи життєвого циклу визначаються як класи підписів, які мають загальні властивості, визначені в цьому стандарті. Процес створення екземпляру класу підпису на основі підпису іншого класу який відповідає

вимогам цього життєвого циклу називається посилення підпису та керується політикою посилення підпису.

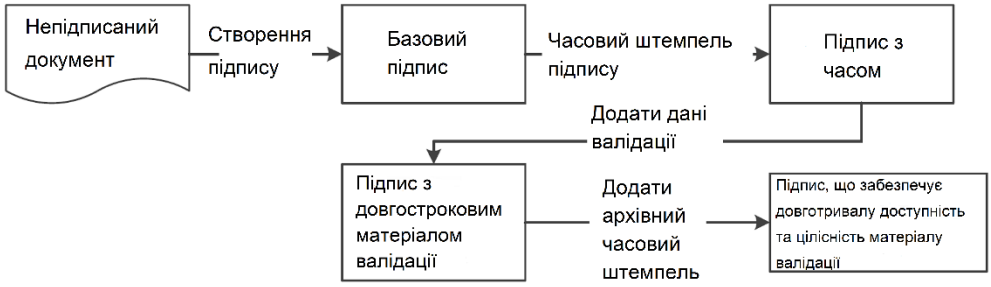

Рисунок 3.3 – Життєвий цикл підпису

Кожен з наведених нижче класів підписів відповідає змістовній комбінації атрибутів, доданих до підпису, з метою покращення можливості валідації підпису в майбутньому, коли відповідний сертифікат або будь-який інший матеріал, необхідний для успішної валідації, може закінчитися, бути анульованим або використані алгоритми вже недостатньо сильні, щоб бути надійними.

Базовий підпис – це підпис, який може пройти валідацію, якщо відповідні сертифікати не анульовані або не закінчуються.

На рис. 3.4 показані етапи створення базового підпису.

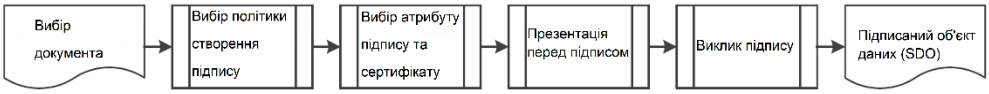

Рисунок 3.4 – Створення базового підпису

Результатом процесу створення базового підпису є SDO, який повинен містити:

- значення підпису;
- посилання або копію сертифіката підписування як підписаний атрибут;
- будь-які опціональні підписані або непідписані атрибути (наприклад, ідентифікатор політики підпису).

Базовий підпис призначений для запобігання атакам простої заміни та перевидачі сертифікату. Базовий підпис вказує на сертифікат, який треба використовувати для верифікації підпису.

На рис. 3.5 наведено базовий підпис.

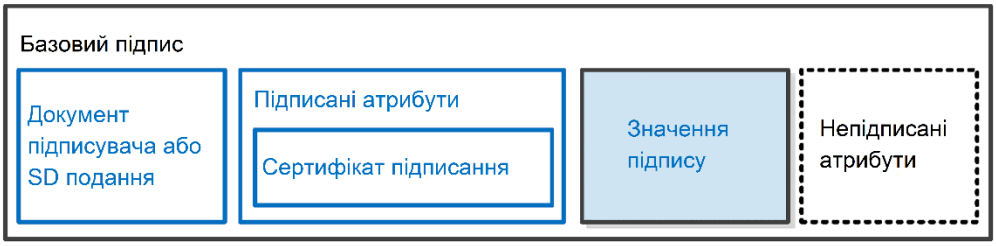

Рисунок 3.5 – Базовий підпис

Підпис з часом – це підпис, який підтверджує, що підпис вже існував у визначений момент часу (рис. 3.6). Його можна використати для валідації підпису, якщо після створення підпису сертифікат було скасовано.

Час забезпечується токеном часового штемпеля для підпису в якості непідписаної властивості, яка додана до базового підпису в результаті посилення підпису.

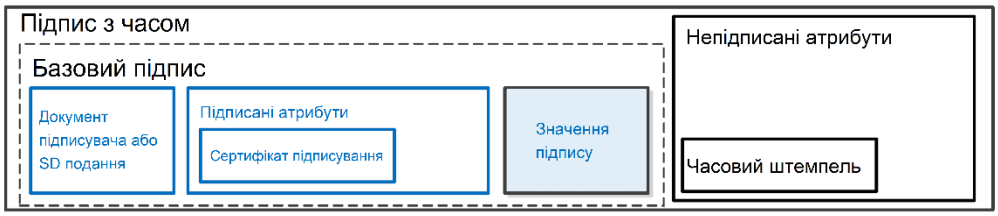

Рисунок 3.6 – Підпис з часом

Підпис з довгостроковим матеріалом валідації – це підпис, що забезпечує тривалий доступ до матеріалів валідації шляхом включення всього матеріалу або посилання на матеріал, необхідний для валідації підпису.

Поки алгоритм валідації може оцінити валідність підпису з часом, його підпис можна посилити до підпису з матеріалом для довгострокової валідації шляхом додавання непідписаних атрибутів. Це посилення підпису можна виконати або за допомогою застосування для створення підпису (Signature Creation Application, SCA), або третьою стороною, або верифікатором, що використовує SVA.

Алгоритм валідації підпису може оцінювати валідність підпису з часом лише за умови, що дані валідації, необхідні для валідації підпису, доступні для верифікаторів в режимі онлайн. У випадку, якщо немає впевненості, що дані валідації, необхідні для валідації підпису, як і раніше будуть доступні в режимі онлайн для верифікаторів або що деякі верифікатори не можуть отримати доступ до цих даних, то необхідно помістити ці дані всередину підпису.

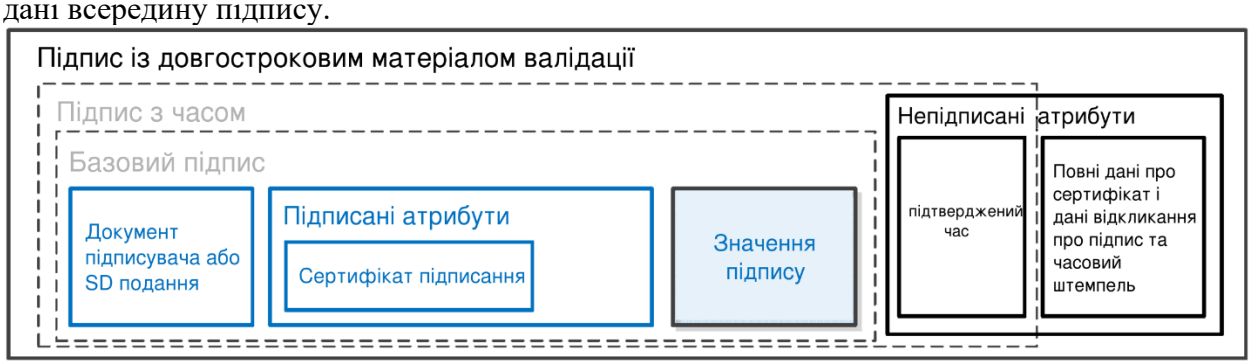

Рисунок 3.7 – Підпис з довгостроковим матеріалом валідації

Підпис з довгостроковим матеріалом валідації (рис. 3.7) містить дані валідації, які необхідні для верифікації підпису після завершення дії сертифікату підписування, зокрема, щоб визначити статус відкликання всіх сертифікатів кінцевого об'єкта (сертифікат підписування, сертифікати одиниць часових штемпелів, сертифікати атрибутів тощо), що містяться в підписі.

Може бути більше елементів, ніж це необхідно, також може бути менше елементів, ніж необхідно, якщо очікується, що одержувачі мають альтернативний спосіб отримання відсутніх елементів.

Підпис, що забезпечує довготривалу доступність та цілісність матеріалу валідації (рис. 3.8), спрямований на довготривалу доступність та цілісність матеріалу перевірки цифрових підписів у довгостроковій перспективі і може допомогти провести валідацію підпису за межами багатьох подій, що обмежують його валідність (наприклад,

слабкість використовуваних криптографічних алгоритмів або закінчення терміну дії даних валідації).

Підписи можна перевірити після завершення терміну дії або скасування сертифікатів, а також у випадках, коли безпека використовуваних алгоритмів стає сумнівною, або розміри використовуваних ключів вже не відповідають сучасним вимогам.

Перш ніж алгоритми, ключі та інші криптографічні дані, використані під час створення підпису, стануть слабкими, а криптографічні функції – вразливими, або сертифікати, що підтримують попередні твердження часу, закінчаться або будуть скасовані, документ підписувача, підпис, а також будь-які атрибути, що містяться в підписі з матеріалом для довгострокової валідації, необхідно захистити шляхом застосування одного або кількох тверджень часу. Підтвердження часу зв'язує дані з певним часом, формуючи докази того, що ці дані існували на даний момент часу. Подібні додаткові твердження часу додаються до підпису як непідписаний атрибут з метою забезпечення довгострокової доступності та цілісності матеріалу валідації і тому називаються **атрибутами довгострокової доступності та цілісності матеріалу валідації**. Створення тверджень часу слід повторювати задовго до того, як захист, наданий попереднім твердженням часу, стане слабким, тому для цього необхідно використовувати сильніші алгоритми або ключі більшої довжини, ніж ті, що використовувалися в оригінальних підписах або попередніх твердженнях часу.

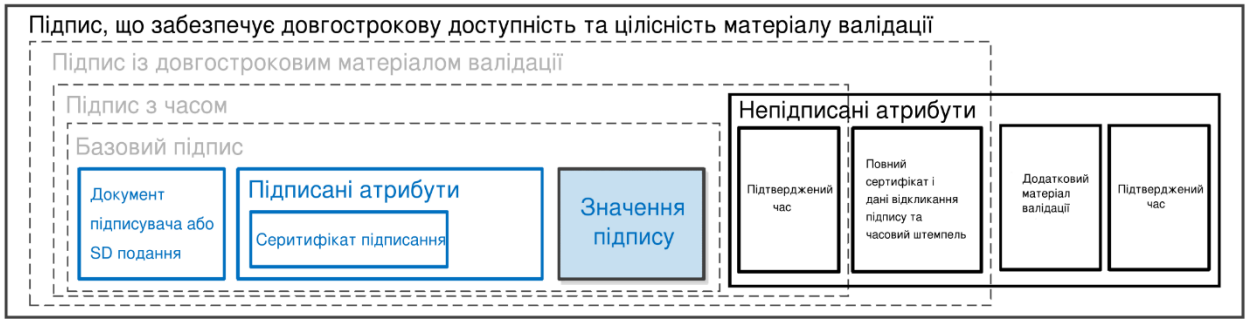

Рисунок 3.8 – Підпис, що забезпечує довгострокову доступність та цілісність матеріалу валідації

Якщо процес повторюється, можуть існувати декілька екземплярів тверджень часу. На рис. 3.9 показаний приклад підпису, в якому застосовано два твердження часу [25].

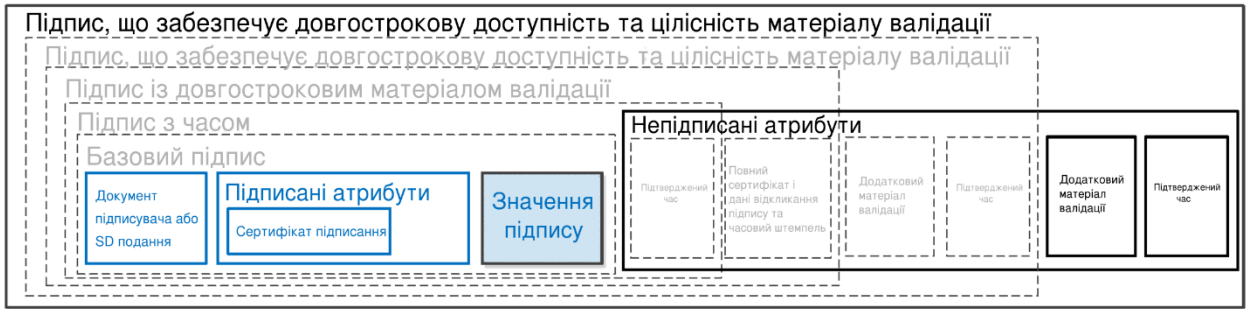

Рисунок 3.9 – Підпис, що забезпечує довгострокову доступність та цілісність матеріалу валідації після повторення

Відображення електронних довірчих послуг на етапі життєвого циклу еДок проілюстровано на рис. 3.10. у овальних блоках показано, які довірчі послуги використовуються на відповідних етапах життєвого циклу електронного документу.

Практичне застосування електронних довірчих послуг для проходження життєвого циклу еДок проілюстровано двома практичними роботами, виконуваними в рамках даного курсу в частині створення електронного документа та його перевірки.

Рисунок 3.10 – Відображення електронних довірчих послуг на етапі життєвого циклу еДок

Огляд наявних засобів для створення еДок на ринку України

На сьогодні на ринку доступні наступні засоби створення електронних документів:

– онлайн сервіс створення кваліфікованого електронного підпису на електронні документи Державного підприємства "Національні інформаційні системи" – https://ca.informjust.ua/;

– Акредитований центр сертифікації ключів інформаційно-довідкового департаменту ДФС – https://www.acskidd.gov.ua/verify;

– Інтегрована система електронної ідентифікації – https://id.gov.ua/sign.

– Безкоштовна система створення електронних документів – http://edoc.link;

Також, на ринку присутні комерційні системи електронного документообігу, зокрема document.online, Вчасно (vchasno.ua), dealssign.com.ua та інші.

Література

1. Закон України “Про електронні документи та електронний документообіг” [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15
2. Закон України “Про електронні довірчі послуги” [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19
3. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093
4. Regulation (EU) No 910/2014 of the european parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Електронний ресурс] – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
5. Learn about eIDAS – https://ec.europa.eu/digital-single-market/en/learn-about-eidas
6. Chris Allen, Steve Marshall. Digital Signatures For Dummies ®, Cryptomathic Special Edition. – John Wiley & Sons, Ltd., The Atrium, Southern Gate, 2017. – 73 p.
7. United Nations e-Government Survey 2018. Gearing e-Government to Support Transformation Towards Sustainable and Resilient Societies [Електронний ресурс] – Режим доступу: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf
8. Публічні IT-ініціативи в Україні. Електронна ідентифікація/аутентифікація [Електронний ресурс] – Режим доступу: http://e-gov.com.ua/e-identification.html
9. eID-карты постараются сделать максимально удобными для пользователей [Електронний ресурс] – Режим доступу: https://rus.lsm.lv/statja/novosti/obschestvo/eid-karti-postarayutsja-sdelat-maksimalno-udobnimi-dlja-polzovateley.a256823/
10. Mobile Connect forCross-Border Digital Services. Lessons Learned from the eIDAS Pilot [Електронний ресурс] – Режим доступу: https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-FINAL-web.pdf
11. Без черг і чиновників: послуги, які українці можуть отримати онлайн [Електронний ресурс] – Режим доступу: https://ukr.segodnya.ua/ukraine/bez-ocheredey-i-chinovnikov-uslugi-kotorye-ukraincy-mogut-poluchit-onlayn-1113992.html
12. Запис до лікаря онлайн: як запрацювало нововведення в українських лікарнях [Електронний ресурс] – Режим доступу: https://ukr.segodnya.ua/ukraine/zapis-k-vrachu-onlayn-kak-zarabotalo-novovvedenie-v-bolnicah-1106807.html
13. Концепція розвитку електронного урядування в Україні [Електронний ресурс] – Режим доступу: https://www.kmu.gov.ua/ua/npas/250287124
14. Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/617-2018-%D1%80
15. Запуск Mobile ID: в Україні впроваджують новий сервіс онлайн-ідентифікації [Електронний ресурс] – Режим доступу: https://ukr.segodnya.ua/ukraine/zapusk-

mobile-id-chto-nuzhno-znat-o-novom-servise-onlayn-identifikacii-ukraincev-1105812.html
16. Мобільні сервіси електронної ідентифікації [Електронний ресурс] – Режим доступу: https://www.apteka.ua/article/484559
17. Digital Single Market. eIDAS for SMEs [Електронний ресурс] – Режим доступу: https://ec.europa.eu/digital-single-market/en/eidas-smes?fbclid=IwAR0Fmvdd1fwfIv-50lIuUoUe4yr3Mk0qh948mzOLNrt-92gb7OZ0h4IPkUg
18. М.Б. Величкевич, Н.В. Мітрофан, Н.Е. Кунанець «Електронний документообіг, тенденції та перспективи» // Вісник «Національного університету “львівська політехніка” «Інформаційні системи та мережі»» № 689
19. Мелащенко А.О., Перевозчикова О.Л., Скарлат О.С. «Формат довгострокового зберігання електронних документів». // Компьютерная математика. – 2011. – № 1. – С. 106–115
20. ISO 32000-1:2008 Document management – Portable document format – Part 1: PDF 1.7 [Електронний ресурс] – Режим доступу: https://www.iso.org/standard/51502.html
21. ISO 19005-1:2005 Document management - Electronic document file format for long-term preservation [Електронний ресурс] – Режим доступу: Part 1: Use of PDF 1.4 (PDF/A-1) – https://www.iso.org/standard/38920.html
22. Перелік форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1422-14#n4
23. Вимоги до форматів даних електронного документообігу в органах державної влади [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/z1309-18?fbclid=IwAR1sEYerNXI9y_GyIYkOvuuIUAgG7exUf47po2tdB4FHCmPmCz6rqewWudM#n17
24. ДСТУ ETSI EN 319 162-1:201_ (ETSI EN 319 162-1:2016, IDT) Електронні підписи та інфраструктури (ESI). Контейнери асоційованих підписів (ASiC). Частина 1: Складові частини та базові контейнери ASiC
25. ДСТУ ETSI EN 319 102-1:201_ (ETSI EN 319 102-1:2016, IDT) Електронні підписи та інфраструктури (ESI). Процедури, які використовуються для створення та валідації цифрових підписів ADES. Частина 1: Створення та валідація
26. Security guidelines on the appropriate use of qualified electronic registered delivery services Guidance for users. VERSION 2.0, FINAL, DECEMBER 2016 - European Union Agency For Network And Information Security [Електронний ресурс] – Режим доступу: file:///C:/Users/user/AppData/Local/Temp/WP2016-3-2-16-Relying-Parties-QDel.pdf
27. ДСТУ ETSI EN 319 522-1:201_ (ETSI EN 319 522-1:2018, IDT) Електронні підписи та інфраструктури (ESI). Служби електронної реєстрованої доставки. Частина 1. Структура та архітектура
28. Регламент АЦСК ООО "Центр сертификации ключей "Украина" [Електронний ресурс] – Режим доступу: https://uakey.com.ua/index.php?num_text=7380